Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2205

(05/2011)

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

Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques

Recommandation UIT-T Y.2205

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 de transmission par paquets	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

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

Recommandation UIT-T Y.2205

Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques

Résumé

La Recommandation UIT-T Y.2205 contient des considérations techniques qui peuvent être appliquées dans les réseaux de prochaine génération (NGN, *next generation network*) pour la prise en charge des télécommunications d'urgence (ET, *emergency telecommunications*) et énonce les principes techniques qui sous-tendent cette prise en charge.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2205	2008-09-12	13
2.0	ITU-T Y.2205	2011-05-20	13

Mots clés

Architecture, alerte avancée (EW), NGN, qualité de service, service de télécommunications d'urgence (ETS), télécommunications à traitement préférentiel, télécommunications d'urgence, télécommunications pour les secours en cas de catastrophe (TDR), télécommunications prioritaires.

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

Introduction

La Recommandation UIT-T Y.1271 contient les spécifications et capacités de réseau pour les télécommunications d'urgence. Suivant l'exemple des autorités qui coordonnent les secours en cas de catastrophe en utilisant les réseaux publics, la mise en place de systèmes de télécommunications prioritaires découlant de ces spécifications peut conduire à la création de nouveaux mécanismes et à l'interfonctionnement/la réutilisation de mécanismes existants. Les télécommunications d'urgence doivent bénéficier d'un traitement préférentiel par rapport aux services normaux sur les réseaux publics. L'expression "télécommunications bénéficiant d'un traitement préférentiel" est utilisée dans certaines Recommandations UIT-T pour désigner les services devant faire l'objet d'un traitement préférentiel. On considère que le service des télécommunications d'urgence est une catégorie de service appelant un traitement préférentiel. Les expressions "télécommunications bénéficiant d'un traitement préférentiel" et "télécommunications d'urgence" sont employées indifféremment.

Les systèmes de classement des télécommunications par ordre de priorité utilisés dans les situations d'urgence ne sont pas nouveaux; les réseaux à commutation de circuits prennent en charge des systèmes de ce type depuis des années, essentiellement pour les appels vocaux (par exemple [UIT-T E.106]). Toutefois, il faut adapter les méthodes techniques utilisées pour prendre en charge ces spécifications sous-jacentes pour les télécommunications d'urgence dans l'environnement NGN. En effet, les méthodes traditionnelles de priorité utilisées dans les réseaux à commutation de circuits ne s'appliquent pas nécessairement dans les NGN en raison des différences intrinsèques qui existent entre les télécommunications à commutation de circuits et les télécommunications à commutation par paquets.

La Recommandation UIT-T Y.1271 présente les spécifications et capacités en général et définit des termes abstraits, de manière indépendante de la technologie.

Etant donné que les NGN utilisent la technologie de commutation par paquets, qui est fondamentalement différente de la technologie de commutation de circuits, il est nécessaire d'examiner les problèmes techniques et les solutions qui peuvent être utilisées pour mettre en place des capacités de télécommunications d'urgence dans les NGN.

La présente Recommandation contient des considérations techniques qui peuvent être appliquées dans les NGN pour la prise en charge des télécommunications d'urgence et énonce les principes sous-jacents.

Recommandation UIT-T Y.2205

Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques

1 Domaine d'application

La présente Recommandation contient des considérations techniques qui peuvent être appliquées dans les réseaux de prochaine génération (NGN, *next generation network*) pour la prise en charge des télécommunications d'urgence (ET, *emergency telecommunications*) et énonce les principes techniques qui sous-tendent cette prise en charge. Elle énonce des spécifications et des capacités pour les télécommunications d'urgence qui viennent compléter celles qui sont énoncées dans [UIT-T Y.2201] dans le contexte des NGN (définis dans [UIT-T Y.2001] et décrits plus en détail dans [UIT-T Y.2011]).

Les télécommunications d'urgence (y compris la prise en charge de certains aspects de l'alerte avancée (voir la Figure 1)) comprennent:

- les télécommunications d'urgence d'individu à autorité, par exemple les appels destinés à des fournisseurs de services d'urgence;
- les télécommunications d'urgence entre autorités;
- les télécommunications d'urgence d'autorité à individu, par exemple des services de notification collective.

L'Appendice I contient des informations supplémentaires sur les catégories de télécommunications d'urgence susmentionnées.

Certaines spécifications et capacités sont également présentées concernant l'alerte avancée. Les capacités de télécommunications d'urgence d'individu à autorité ne sont pas prises en considération et n'entrent pas dans le cadre de la présente Recommandation.

Les moyens techniques décrits ici pourraient aussi, pour certains, être utilisés pour les télécommunications d'urgence d'individu à autorité ou entre individus, mais ces catégories ne sont pas prises en considération dans la présente Recommandation.

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.

2.1 UIT-T

[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 G.808.1] Recommandation UIT-T G.808.1 (2010), *Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux*.

[UIT-T G.841] Recommandation UIT-T G.841 (1998), *Types et caractéristiques des architectures de protection des réseaux à hiérarchie numérique synchrone*.

[UIT-T G.842] Recommandation UIT-T G.842 (1997), *Interfonctionnement des architectures de protection des réseaux à hiérarchie numérique synchrone*.

[UIT-T G.873.1] Recommandation UIT-T G.873.1 (2006), *Réseau de transport optique: protection linéaire*.

[UIT-T G.983.1] Recommandation UIT-T G.983.1 (2005), *Systèmes d'accès optique à large bande basés sur les réseaux optiques passifs*.

[UIT-T G.8031] Recommandation UIT-T G.8031/Y.1342 (2009), *Commutation de protection linéaire Ethernet*.

[UIT-T G.8032] Recommandation UIT-T G.8032/Y.1344 (2010), *Commutation de protection annulaire Ethernet*.

[UIT-T G.8131] Recommandation UIT-T G.8131/Y.1382 (2007), *Commutation de protection linéaire pour les réseaux MPLS de transport (T-MPLS)*.

[UIT-T H.248.1] Recommandation UIT-T H.248.1 (2005), *Protocole de commande de passerelle: version 3*.

[UIT-T H.248.81] Recommandation UIT-T H.248.81 (2011), *Protocole de commande de passerelle: lignes directrices relatives à l'utilisation de l'indicateur d'appel et de l'indicateur de priorité du plan international de priorité en période de crise (IEPS) dans les profils UIT-T H.248*.

[UIT-T H.323] Recommandation UIT-T H.323 (2009), *Systèmes de communication multimédia en mode paquet*.

[UIT-T H.460.4] Recommandation UIT-T H.460.4 (2007), *Désignation de la priorité des appels et identification du pays/réseau international d'origine des appels prioritaires H.323*.

[UIT-T I.630] Recommandation UIT-T I.630 (1999), *Commutation de protection ATM*.

[UIT-T J.260] Recommandation UIT-T J.260 (2005), *Prescriptions relatives aux communications à traitement préférentiel sur les réseaux IPCablecom*.

[UIT-T J.261] Recommandation UIT-T J.261 (2009), *Cadre applicable à la mise en oeuvre des télécommunications à traitement préférentiel sur les réseaux IPCablecom et IPCablecom2*.

[UIT-T J.262] Recommandation UIT-T J.262 (2009), *Spécifications relatives à l'authentification pour les télécommunications à traitement préférentiel sur les réseaux IPCablecom2*.

[UIT-T J.263] Recommandation UIT-T J.263 (2009), *Spécifications relatives à la priorité pour les télécommunications à traitement préférentiel sur les réseaux IPCablecom2*.

[UIT-T Q.812] Recommandation UIT-T Q.812 (2004), *Profils des protocoles des couches supérieures pour les interfaces Q et X*.

[UIT-T Q.1741.6] Recommandation UIT-T Q.1741.6 (2009), *Références IMT-2000 à la version 8 du réseau central UMTS issu du GSM*.

[UIT-T Q.3303.3] Recommandation UIT-T Q.3303.3 (2008), *Protocole de contrôle des ressources N° 3 – Protocoles à l'interface Rw entre une entité physique de décision de politique (PD-PE) et une entité physique d'application de politique (PE-PE): protocole Diameter.*

[UIT-T Q.3321.1] Recommandation UIT-T Q.3321.1 (2010), *Protocole de contrôle des ressources N° 1 version 2 – Protocole à l'interface Rs entre les entités de commande de service et l'entité physique de décision de politique.*

[UIT-T Q-Sup.57] Supplément 57 aux Recommandations UIT-T de la série Q (2008), *Spécifications de signalisation pour la prise en charge du service de télécommunications d'urgence (ETS) dans les réseaux IP*.

[UIT-T X.660] Recommandation UIT-T X.660 (2008) | ISO/CEI 9834-1:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – Procédures opérationnelles des organismes d'enregistrement de l'OSI: procédures générales et arcs sommitaux de l'arborescence des identificateurs internationaux d'objet.*

[UIT-T X.674] Recommandation UIT-T X.674 (2011), *Procédures d'enregistrement d'arcs d'identificateur d'objet en matière d'alerte.*

[UIT-T X.1303] Recommandation UIT-T X.1303 (2007), *Protocole d'alerte commun (CAP 1.1).*

[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.1720] Recommandation UIT-T Y.1720 (2006), *Commutation de protection pour les réseaux MPLS.*

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

[UIT-T Y.2011] Recommandation UIT-T Y.2011 (2004), *Principes généraux et modèle de référence général pour les réseaux de prochaine génération*.

[UIT-T Y.2012] Recommandation UIT-T Y.2012 (2010), *Prescriptions et architecture fonctionnelles du réseau 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.2171] Recommandation UIT-T Y.2171 (2006), *Niveaux de priorité de contrôle des admissions dans les réseaux de prochaine génération (NGN).*

[UIT-T Y.2172] Recommandation UIT-T Y.2172 (2007), *Niveaux de priorité pour le rétablissement de service dans les réseaux de prochaine génération.*

[UIT-T Y.2201] Recommandation UIT-T Y.2201 (2009), *Spécifications et capacités des réseaux de prochaine génération de l'UIT-T.*

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

[UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation dans les réseaux de prochaine génération de version 1*.

[UIT-T Y.2704] Recommandation UIT-T Y.2704 (2010), *Mécanismes et procédures de sécurité des réseaux NGN*.

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

[UIT-T Y.2721] Recommandation UIT-T Y.2721 (2010), *Spécifications et cas d'utilisation de la gestion d'identité dans les NGN*.

[UIT-T Y.2722] Recommandation UIT-T Y.2722 (2011), *Mécanismes de gestion d'identité dans les réseaux de prochaine génération*.

2.2 IETF

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[IETF RFC 3168] IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*.

[IETF RFC 3246] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior).*

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 3312] IETF RFC 3312 (2012), *Integration of Resource Management and Session Initiation Protocol (SIP).*

[IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[IETF RFC 4340] IETF RFC 4340 (2006), *Datagram Congestion Control Protocol (DCCP).*

[IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP).*

[IETF RFC 4542] IETF RFC 4542 (2006), *Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite.*

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

[IETF RFC 5865] IETF RFC 5865 (2010), *A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic.*

2.3 ETSI

[ETSI TS 183 017] ETSI TS 183 017 V3.2.1 (2010), TISPAN *Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification.*

2.4 Broadband Forum

[BBF TR-058] Broadband Forum TR-058 (2003), *Multi-Service Architecture and Framework Requirements*.

[BBF TR-059] Broadband Forum TR-059 (2003), *DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services*.

[BBF TR-101] Broadband Forum TR-101 (2011), *Migration to Ethernet-Based DSL Aggregation.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 alerte [UIT-T X.674]: message d'avertissement ou d'alarme concernant l'imminence d'un danger ou d'un problème.

3.1.2 centre d'alerte [UIT-T X.674]: entité nationale, régionale ou internationale chargée de la gestion des alertes.

3.1.3 service de télécommunications d'urgence (ETS, *emergency telecommunications service*) [UIT-T E.107]: service national offrant des télécommunications prioritaires aux utilisateurs autorisés en cas de catastrophe et de situation d'urgence.

3.1.4 réseau de prochaine génération (NGN, *next generation network*) [UIT-T Y.2001]: réseau en mode paquet, en mesure d'assurer des services de télécommunication et d'utiliser de multiples technologies de transport à large bande à qualité de service imposée et dans lequel les fonctions liées aux services sont indépendantes des technologies sous-jacentes liées au transport. Il assure le libre accès des utilisateurs aux réseaux et aux services ou fournisseurs de services concurrents de leur choix. Il prend en charge la mobilité généralisée qui permet la fourniture cohérente et ubiquitaire des services aux utilisateurs.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 télécommunications d'urgence (ET, *emergency telecommunications*): tout service associé à une urgence qui nécessite un traitement spécial de la part du NGN par rapport aux autres services. Les télécommunications d'urgence comprennent les services de sécurité du public et les services d'urgence autorisés par les pouvoirs publics.

3.2.2 télécommunications à traitement préférentiel: catégorie de service pour lequel il est possible d'accéder en priorité aux ressources d'un réseau et/ou de les utiliser en priorité.

3.2.3 télécommunications pour les secours en cas de catastrophe (TDR, *telecommunications for disaster relief*): capacité de télécommunications internationales et nationales pour les secours en cas de catastrophe, utilisant des installations de réseau partagées internationales permanentes déjà en place et opérationnelles, des installations de réseau temporaires qui sont fournies spécifiquement pour les télécommunications TDR, ou une combinaison des deux.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

AAA authentification, autorisation et comptabilité (*authentication, authorization and accounting*)

AF fonction d'application (*application function*)

ANMS système de gestion des noeuds d'accès (*access node management system*)

APS commutation de protection automatique (*automatic protection switching*)

AQM gestion active des files d'attente (*active queue management*)

ASN réseau de service d'accès (*access service network*)

ASN.1 notation de syntaxe abstraite numéro un (*abstract syntax notation one*)

BNG passerelle de réseau à large bande (*broadband network gateway*)

BS station de base (*base station*)

CAC contrôle d'admission d'appel (*call admission control*)

CAP protocole d'alerte commun (*common alerting protocol*)

CPE équipement des locaux d'abonné (*customer premises equipment*)

DCCP protocole de gestion des encombrements de données (*data congestion control protocol*)

DoS déni de service (*denial of service*)

DSCP point de code des services différenciés (*differentiated services code points*)

DSLAM multiplexeur de lignes d'abonné numérique (*digital subscriber line access multiplexer*)

EAS système d'alerte en cas d'urgence (*emergency alert system*)

ECN notification d'encombrement explicite (*explicit congestion notification*)

EF transmission express (*expedited forwarding*)

E-MTA adaptateur multiterminal intégré (*embedded multi-terminal adapter*)

ENI mise en œuvre nationale du service ETS (*ETS national implementation*)

ET télécommunications d'urgence (*emergency telecommunications*)

ETH réseau de couche Ethernet (*Ethernet layer network*)

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

EW alerte avancée (*early warning*)

GETS service de télécommunications d'urgence de l'Etat (*government emergency telecommunications service*)

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

IP protocole Internet (*Internet protocol*)

LAN réseau local (*local area network*)

LSP conduit commuté avec étiquette (*label switched path*)

MDF répartiteur principal (*main distribution frame*)

MMPS service de priorité multimédia (*multimedia priority service*)

MPS service de priorité multimédia (*multimedia priority service*)

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

MS section de multiplexage (*multiplex section*)

NID dispositif d'interface avec le réseau (*network interface device*)

NOAA National Oceanic and Atmospheric Administration

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

ODUk unité de données de canal optique (*optical channel data unit k*)

OLT terminaison de ligne optique (*optical line termination*)

OMCI interface de gestion et de commande de terminaison de réseau optique (*ONT management and control interface*)

ONT terminaison de réseau optique (*optical network termination*)

ONU/SIPC stratégie internationale des Nations Unies pour la prévention des catastrophes

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

P-CSC-FE entité fonctionnelle proxy de contrôle de session d'appel (*proxy call session control functional entity*)

PCC commande de la politique et de la taxation (*policy and charging control*)

PDP point de décision de politique (*policy decision point*)

PEP point d'application des politiques (*policy enforcement point*)

PF fonction de politique (*policy function*)

PHB comportement par saut (*per hop behaviour*)

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

PON réseau optique passif (*passive optical network*)

POTS service téléphonique ordinaire (*plain old telephone service*)

PSAP point de réponse de sécurité publique (*public safety answering point)*

QoS qualité de service (*quality of service*)

RACF fonction de contrôle des ressources et d'admission (*resource and admission control function*)

RMTP réseau mobile terrestre public

RNIS réseau numérique à intégration de services

RPH en-tête de priorité de ressource (*resource priority header*)

RSVP protocole de réservation de ressources (*resource reservation protocol*)

RTPC réseau téléphonique public commuté

SAME codage de message de zone spécifique (*specific area message encoding*)

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

SDH hiérarchie numérique synchrone (*synchronous digital hierarchy*)

SIP protocole d'ouverture de session (*session initiation protocol*)

SLA accord de niveau de service (*service level agreement*)

SNC connexion de sous-réseau (*subnetwork connection*)

SNCP protection de la connexion de sous-réseau (*subnetwork connection protection*)

SS7 système de signalisation N° 7 (*signalling system No. 7*)

TCP protocole de commande de transmission (*transmission control protocol*)

TDM multiplexage temporel (*time division multiplexing*)

TDR télécommunications pour les secours en cas de catastrophe (*telecommunications for disaster relief*)

T-MPLS réseau MPLS de transport (*transport MPLS*)

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

UE équipement d'utilisateur (*user equipment*)

USI interface de service universelle (*universal services interface*)

VC canal virtuel (*virtual channel*)

VLAN réseau local virtuel (*virtual LAN*)

VoIP téléphonie IP (*voice over IP*)

VP conduit virtuel (*virtual path*)

W-CDMA accès multiple par répartition en code à large bande (*wideband code division multiple access*)

WPS service prioritaire sans fil (*wireless priority service*)

xDSL toute variante de ligne d'abonné numérique (*any variant of digital subscriber line*)

XML langage de balisage extensible (*eXtensible markup language*)

XSD définition de schéma XML (*XML schema definition*)

5 Description des télécommunications d'urgence (ET) et de l'alerte avancée

5.1 Généralités

La présente Recommandation utilise les termes suivants:

- Télécommunications d'urgence ET
- Service de télécommunications d'urgence ETS
- Télécommunications pour les secours en cas de catastrophe TDR
- Alerte avancée EW

Il est essentiel de définir et comprendre les différents emplois de ces termes, à savoir:

- ET: Terme cadre désignant tout service associé à une urgence qui nécessite un traitement spécial de la part du NGN par rapport aux autres services.
- ETS: Terme employé comme défini dans [UIT-T E.107].
- TDR: Terme générique désignant une capacité de télécommunications utilisée pour les secours en cas de catastrophe.
- EW: Terme générique désignant tous les types de systèmes, capacités et services d'alerte avancée.

Une arborescence avec les télécommunications d'urgence comme racine pour toutes les activités permet de représenter l'emploi des termes et les relations entre eux (voir la Figure 1 ci-dessous).

Comme indiqué dans l'introduction, certaines Recommandations UIT-T, en particulier celles de la série J.26x, utilisent l'expression "télécommunications bénéficiant d'un traitement préférentiel" pour inclure les services qui nécessitent un traitement particulier par rapport à d'autres services. Sauf dans le contexte des Recommandations UIT-T de la série J.26x, il n'est pas fait mention, dans la présente Recommandation, de l'expression "télécommunications bénéficiant d'un traitement préférentiel". L'expression "télécommunications bénéficiant d'un traitement préférentiel" dans les Recommandations UIT-T de la série J.26x comprend les télécommunications ETS, TDR et EW.

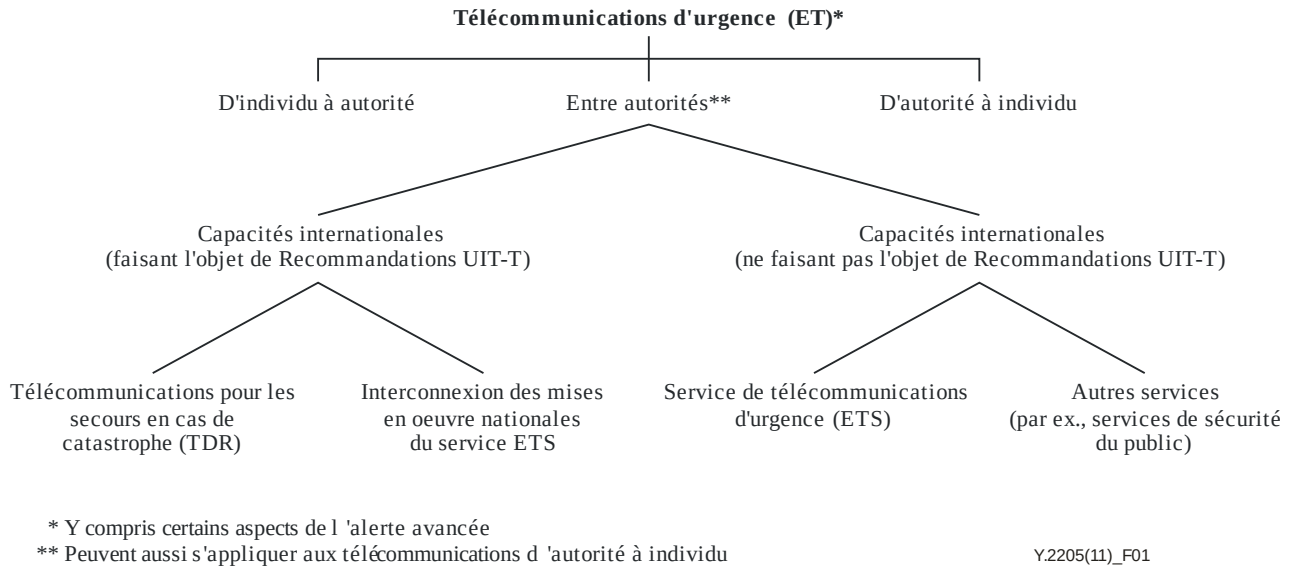


Figure 1 – Cadre des relations terminologiques pour les télécommunications d'urgence

5.2 Télécommunications d'urgence

Les télécommunications d'urgence (ET) désignent tout service associé à une urgence qui nécessite un traitement spécial de la part du NGN par rapport aux autres services. Elles comprennent les services de sécurité du public et les services d'urgence autorisés par les pouvoirs publics. On donne ci-après des exemples de services entrant dans le cadre des télécommunications d'urgence:

1) Télécommunications pour les secours en cas de catastrophe (TDR)

   Il s'agit d'une capacité de télécommunications internationales et nationales pour les secours en cas de catastrophe, utilisant des installations de réseau partagées internationales permanentes déjà en place et opérationnelles, des installations de réseau temporaires qui sont fournies spécifiquement pour les télécommunications TDR, ou une combinaison des deux.

2) Service de télécommunications d'urgence (ETS)

   Il s'agit d'un service national offrant des télécommunications prioritaires aux utilisateurs autorisés en cas de catastrophe et de situation d'urgence. Le service ETS est décrit dans [UIT-T E.107], qui donne des indications concernant l'interconnexion de mises en œuvre nationales du service ETS (ENI) (entre autorités).

3) Services de sécurité du public et services d'urgence nationaux/régionaux/locaux

   Parmi les télécommunications d'urgence figurent aussi les services de sécurité du public et les services d'urgence nationaux, régionaux, locaux. Il s'agit de services spécialisés pour la sécurité du public et les situations d'urgence nationales, régionales, locales. Ces services d'urgence, dont la portée est nationale, régionale ou locale, font l'objet d'une normalisation nationale ou régionale.

5.3 Alerte avancée

Dans un Rapport de septembre 2006 [b-UN Global Survey] adressé au Secrétaire général de l'Organisation des Nations Unies et portant sur une "Etude mondiale des systèmes d'alerte avancée", la Stratégie internationale des Nations Unies pour la prévention des catastrophes (ONU/SIPC) définit l'alerte avancée comme "la fourniture, par des institutions identifiées, d'informations efficaces en temps utile permettant aux individus exposés à un danger de prendre des mesures pour éliminer ou réduire le risque les concernant et se préparer à réagir efficacement". Ce rapport des Nations Unies évalue les capacités, les lacunes et les possibilités dans l'optique d'élaborer un système mondial complet d'alerte avancée pour tous les risques naturels.

6 Considérations générales concernant les télécommunications d'urgence et l'alerte avancée

Avant l'élaboration de [UIT-T Y.1271], les spécifications des capacités de télécommunications d'urgence se rapportaient essentiellement aux réseaux à commutation de circuits tels que le réseau téléphonique public commuté (RTPC).

Ces spécifications étaient basées sur certaines caractéristiques des réseaux à commutation de circuits, dont elles tiraient parti. Par exemple:

- contrôle d'admission utilisant un couplage étroit entre les ressources de signalisation et les ressources médias;
- fourniture à un débit binaire constant de l'ensemble du trafic média nécessitant une largeur de bande uniforme;
- largeur de bande réservée pour chaque flux;
- séparation du trafic de commande et du trafic de données.

On ne retrouve pas nécessairement ces caractéristiques dans les réseaux actuels à commutation par paquets offrant un service au mieux (best-effort):

- Les réseaux à commutation par paquets ont tendance à reposer sur un partage des ressources et sur l'utilisation de files d'attente pour faciliter la prise en charge du trafic par salves – combinaison généralement réalisée sous forme de service au mieux.
- Le contrôle d'admission peut être difficile – de nombreuses applications ne signalent pas leurs besoins de largeur de bande, et la signalisation et les médias sont découplés.
- Les applications et services ont des besoins de largeur de bande variables et peuvent envoyer des données en utilisant des débits ajustés dynamiquement.
- Différents flux de paquets utilisent en partage une largeur de bande multiplexée statistiquement.
- Il se peut que le trafic de contrôle des ressources et le trafic de données utilisent en partage les mêmes ressources du réseau.

Dans les NGN à commutation par paquets, il peut toujours y avoir une concurrence entre les paquets concernant la largeur de bande disponible, sauf si des mesures spéciales sont appliquées. Au niveau transport proprement dit, les paquets ne peuvent pas facilement être refusés ou faire l'objet d'un contrôle de flux. Par ailleurs, l'ingénierie du trafic d'un réseau par paquets est très différente de celle d'un réseau à commutation de circuits en ce qui concerne les approches standards acceptées universellement. Un "flux" donné de paquets peut être affecté par d'autres flux de paquets utilisant une ressource partagée, sauf si les mesures spéciales disponibles dans un NGN sont utilisées convenablement. En revanche, la séparation entre service et transport dans un NGN peut être utile pour mettre en place des capacités d'urgence plus souples et plus diverses.

Ces conditions signifient que la mise en place de capacités de télécommunications d'urgence n'est pas complètement immédiate, évidente ou simple, et que la transposition à partir des réseaux à commutation de circuits n'est pas simple. D'autres différences entres les réseaux à commutation de circuits et les réseaux à commutation par paquets ainsi qu'entre les différentes technologies de transmission par paquets auront une incidence sur la mise en œuvre des diverses spécifications énoncées dans [UIT-T Y.1271].

Par conséquent, la présente Recommandation a pour objet d'indiquer quelles caractéristiques et quels mécanismes d'un NGN peuvent être utilisés pour faciliter la prise en charge des spécifications des télécommunications d'urgence et de certains aspects de l'alerte avancée. Toutefois, lorsqu'on examine les protocoles, les mécanismes et l'appui aux télécommunications d'urgence, il convient d'éviter d'ajouter des fonctionnalités ou des spécifications car, même si elles sont utiles, elles risquent de se traduire par une complexité accrue, sans pour autant apporter des avantages notables.

Il faut donc veiller à tenir compte des frais encourus lors de la consommation de ressources ainsi que d'autres conséquences avant d'ajouter, par exemple, de nouvelles fonctionnalités en matière de "priorité".

7 Fonctionnalités et capacités requises d'une manière générale

Les fonctionnalités et capacités requises incluent celles qui sont spécifiées dans [UIT-T Y.1271] et [UIT-T Y.2201] pour les NGN, ainsi que celles qui ont été identifiées dans le cadre de l'Etude mondiale des Nations Unies sur les systèmes d'alerte avancée en rapport avec le développement des NGN [b-UN Global Survey].

7.1 Télécommunications d'urgence

Le Tableau 1 énumère les fonctionnalités et capacités requises pour les télécommunications d'urgence.

Tableau 1 – Liste des fonctionnalités et capacités requises pour les télécommunications d'urgence

Télécommunications d'urgence Fonctionnalités et capacités requises
Traitement prioritaire amélioré
Réseaux sécurisés
Confidentialité de l'emplacement
Capacité de rétablissement
Connectivité du réseau
Interopérabilité
Mobilité
Couverture ubiquitaire
Capacité de survie/durabilité
Transmission en temps réel pour prendre en charge: téléphonie/texte en temps réel et vidéo/imagerie (en cas de disponibilité de largeur de bande)
Transmission pas en temps réel pour prendre en charge: messages/flux pas en temps réel (audio/vidéo)
Largeur de bande modulable
Fiabilité/disponibilité

Le but est de garantir avec un niveau élevé de confiance et de probabilité que des services de télécommunications critiques pourront être offerts de façon fiable aux utilisateurs autorisés, par exemple ceux qui participent aux télécommunications d'urgence. [UIT-T Y.1271] définit les "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".

En ce qui concerne la vidéo et l'imagerie, il convient de prendre en considération la disponibilité de largeur de bande (par exemple, une forme de ressource).

On peut classer les fonctions de réseau propres aux télécommunications d'urgence dans les catégories suivantes: invocation de service, authentification et autorisation, traitement prioritaire de bout en bout, interconnexion de réseaux et interfonctionnement de protocoles.

Une invocation de service concerne l'interaction entre l'utilisateur et l'élément utilisateur (par exemple un téléphone) et le réseau, et contient des renseignements indiquant qu'une demande de service de télécommunications d'urgence est adressée au réseau du fournisseur de services. Il existe différentes méthodes, notamment les modalités d'abonnement, permettant de reconnaître la demande. Les renseignements relatifs à l'abonnement sont utilisés pour autoriser certaines demandes de service.

L'authentification et l'autorisation sont effectuées par le fournisseur de services, pour autoriser l'utilisateur à avoir accès aux services de télécommunications d'urgence invoqués, ou pour refuser cet accès. L'autorisation proprement dite est censée être accordée au niveau du réseau central.

Le traitement prioritaire de bout en bout est un ensemble de fonctionnalités utilisées par le ou les réseaux pour établir et maintenir le service avec une forte probabilité entre le réseau d'origine et le réseau de terminaison, y compris les réseaux de transit éventuels. Le traitement prioritaire subsiste en cas d'invocation de service visant à libérer le service. Le traitement prioritaire est inclus dans la commande d'admission et l'attribution des ressources réseau, et dans le transport des paquets de signalisation et de support média par les éléments de réseau prenant en charge le service.

L'interconnexion de réseaux et l'interfonctionnement de protocoles sont nécessaires pour prendre en charge le traitement prioritaire de bout en bout pour le transport et la signalisation de médias qui traversent plusieurs réseaux appartenant à des fournisseurs de services différents et utilisant des techniques différentes. A titre d'exemple, les niveaux de priorité peuvent varier en fonction de la technique utilisée dans les réseaux multiples et il peut être nécessaire de prévoir une mise en correspondance entre un niveau défini dans une technique et un autre niveau.

7.2 Alerte avancée

Les systèmes d'alerte avancée ont besoin d'un système de communication efficace qui doit être fiable et résistant. Les objectifs des systèmes d'alerte avancée dans le contexte des NGN en tant que systèmes de communication sont notamment les suivants:

- avoir des capacités qui fonctionnent en permanence et être opérationnels, robustes et disponibles chaque minute de chaque jour;
- disposer des capacités de télécommunication nécessaires pour transmettre des données en temps réel (par exemple, des données sismiques et des données sur le niveau de la mer);
- être fondés sur des normes adoptées à l'échelle internationale;
- garantir l'intégrité des systèmes d'alerte avancée et l'intégrité ainsi que l'authenticité des messages (c'est-à-dire que seuls des messages autorisés sont envoyés);
- fournir des messages d'alerte uniquement à ceux qui risquent d'être affectés par une catastrophe imminente et éviter les messages non ciblés ou inutiles (par exemple, messages envoyés aux mauvaises personnes et/ou messages qui ne contiennent pas d'informations viables utiles).

Afin de fournir des messages d'alerte uniquement à ceux qui risquent d'être affectés par une catastrophe imminente, les systèmes d'alerte avancée peuvent avoir des objectifs relatifs au filtrage des messages de manière à viser:

- un certain groupe d'utilisateurs;
- certaines régions, etc.;

(par exemple, une forme de "diffusion cellulaire").

8 Directives et spécifications générales en matière de sécurité

8.1 Directives générales

Les éléments, systèmes, ressources, données et services réseau, utilisés pour les télécommunications d'urgence, peuvent faire l'objet de cyberattaques. L'intégrité, la confidentialité et la disponibilité des télécommunications d'urgence, notamment en cas d'attaque, dépendront des services et pratiques de sécurité mis en œuvre dans le NGN et des capacités de sécurité (par exemple, fonctions d'authentification et d'autorisation des utilisateurs) mises en œuvre dans le cadre du service d'application pour les télécommunications d'urgence. Pour planifier la sécurité des télécommunications d'urgence, il convient d'appliquer les lignes directrices générales suivantes (liste non exhaustive):

- Tous les aspects des télécommunications d'urgence, y compris la signalisation et la commande, le support/les médias ainsi que les données liées à la gestion et d'autres informations (par exemple, informations de profil d'utilisateur), doivent être protégés contre les menaces visant la sécurité des télécommunications d'urgence, menaces qui peuvent intervenir dans diverses couches (par exemple, transport, commande de service ou prise en charge de service) et dans les différents segments de réseau (réseau d'accès, réseau central et interfaces d'interconnexion).
- Etablissement et application de politiques et de pratiques de sécurité qui sont propres aux services de télécommunications d'urgence. Il convient d'identifier et de mettre en œuvre des capacités de protection contre diverses menaces de sécurité. Il convient en particulier d'identifier et de mettre en œuvre, pour les télécommunications d'urgence, des capacités de protection et des pratiques de sécurité qui complètent celles qui sont nécessaires pour les services d'application généraux. Il s'agit notamment d'établir et d'appliquer des politiques de sécurité pour protéger les données de gestion et les informations stockées (par exemple, informations de profil d'utilisateur) liées aux télécommunications d'urgence.
- Implémentation et utilisation de procédures d'authentification et d'autorisation des utilisateurs, dispositifs ou combinaisons utilisateur et dispositif afin d'assurer une protection contre l'accès non autorisé aux services, ressources et informations (par exemple informations d'utilisateur présentes dans les serveurs d'authentification et dans les systèmes de gestion) associés aux télécommunications d'urgence. Par exemple, des fonctions d'authentification et d'autorisation devraient être mises en œuvre pour éviter que des ressources réservées aux télécommunications d'urgence soient utilisées par des utilisateurs non autorisés et éviter ainsi les attaques par déni de service (DoS) et les autres types d'attaque.
- Pour les communications qui traversent plusieurs domaines de fournisseur de réseau, chaque fournisseur de réseau doit assurer la sécurité dans son domaine de manière à ce que les communications de bout en bout puissent être sécurisées. Comme les télécommunications d'urgence peuvent faire intervenir des communications qui traversent différents domaines de fournisseur de réseau nationaux et internationaux (pays et administrations), il faut établir et mettre en œuvre une politique de sécurité, des relations de confiance, des méthodes et des procédures d'identification du trafic de télécommunications d'urgence, de gestion d'identité et d'authentification des utilisateurs et des réseaux sur plusieurs domaines administratifs de réseau.

On trouvera des renseignements complémentaires dans [b-ATIS-1000010].

8.2 Spécifications générales

Les recommandations relatives à la sécurité figurant dans [UIT-T Y.2701], [UIT-T Y.2702] et [UIT-T Y.2704] et les recommandations relatives à la gestion d'identité (IdM) figurant dans [UIT-T Y.2720], [UIT-T Y.2721] et [UIT-T Y.2722] se rapportent à la sécurité des télécommunications d'urgence.

8.2.1 Contrôle d'accès

L'accès aux télécommunications d'urgence et aux ressources associées est réservé aux utilisateurs autorisés. Il faut empêcher tout accès non autorisé, par exemple par des intrus se faisant passer pour des utilisateurs autorisés.

8.2.2 Authentification

Il est nécessaire de prévoir des mécanismes et des capacités permettant d'authentifier et d'autoriser l'accès d'un utilisateur, d'un dispositif ou d'une combinaison utilisateur et dispositif de télécommunications d'urgence, selon le cas, compte tenu de la politique[1] et du niveau de garantie pour un service spécifique (par exemple téléphonie, données, vidéo) aux fins de la protection de la sécurité.

8.2.3 Confidentialité

Il est nécessaire de protéger la confidentialité des télécommunications d'urgence et des informations concernant l'utilisateur final, notamment en ce qui concerne le trafic de signalisation, de commande et de support, les informations relatives à l'utilisateur final (par exemple celles concernant l'identité, l'abonnement et le lieu) et l'activité, s'il y a lieu.

8.2.4 Sécurité des communications

Il est nécessaire de protéger les télécommunications d'urgence contre les intrusions (par exemple prévention des interceptions illicites, du piratage ou de la répétition de messages de signalisation ou du trafic support).

8.2.5 Intégrité des données

Il est nécessaire de protéger l'intégrité des télécommunications d'urgence (en assurant par exemple une protection contre la modification, la suppression, la création ou la répétition non autorisées), ce qui englobe la protection de l'intégrité des informations sur les télécommunications d'urgence et des données de configuration (par exemple, marquage prioritaire, informations prioritaires stockées dans les fonctions de décision politique, niveau de priorité de l'utilisateur, etc.).

8.2.6 Disponibilité

Il faut protéger la disponibilité des télécommunications d'urgence et, plus particulièrement, protéger les télécommunications d'urgence et les ressources associées contre le déni de service (DoS) et autres formes d'attaque.

9 Mécanismes et capacités pour la prise en charge des télécommunications d'urgence dans les NGN

9.1 Généralités

La séparation entre la commande de service/application et le transport, qui permet aux services d'application et aux services de transport d'être offerts séparément et d'évoluer de façon indépendante, est une caractéristique essentielle des NGN. Cette séparation est représentée par deux

[1] Dans ce contexte, on entend par politique toutes les politiques applicables, par exemple celles résultant de décisions du fournisseur de réseau NGN, de prescriptions réglementaires ou d'autres règles édictées par les gouvernements.

strates fonctionnelles distinctes. Les fonctions de transport résident dans la strate de transport et les fonctions de commande de service associées aux applications, comme la téléphonie, résident dans la strate des services. D'une manière générale, chaque strate aura son propre ensemble de rôles, d'acteurs et de domaines administratifs (voir [UIT-T Y.110]). Les rôles intervenant dans la fourniture de service(s) sont indépendants de ceux qui interviennent dans la fourniture de la connectivité de transport. Chaque strate peut être traitée séparément du point de vue technique. Les fonctions de contrôle des ressources et d'admission (RACF, *resource and admission control function*) constituent l'arbitre entre ces strates pour la réservation (et la négociation) liée à la qualité de service dans l'architecture NGN. [UIT-T Y.2111] décrit l'architecture et les spécifications des fonctions de contrôle des ressources et d'admission dans les réseaux de prochaine génération, les technologies de transport dans les réseaux d'accès et dans les réseaux centraux pouvant être diverses et les domaines pouvant être multiples. Les décisions de la fonction RACF liées à la qualité de service sont basées sur des accords SLA, la priorité de service, les profils d'utilisateur, les règles adoptées par l'opérateur de réseau et la disponibilité des ressources à la fois dans les réseaux d'accès et dans les réseaux centraux. Il faut identifier les utilisateurs des télécommunications d'urgence et leur donner la priorité pour le contrôle d'admission par la fonction RACF une fois qu'ils sont authentifiés et autorisés.

Si on veut que le trafic de télécommunications d'urgence puisse être distingué du trafic normal dans le NGN, il faut prévoir des étiquettes appropriées, également appelées marqueurs. Dans ce contexte, on emploie le terme de marquage (de trafic).

Dans l'architecture des protocoles NGN multicouches (strate de transport et strate des services) de périphérie à périphérie (segments de réseau d'accès et de réseau central), les étiquettes peuvent exister sous diverses formes dans les différentes couches de protocole à la fois verticalement (interactions entre différentes couches de protocole) et horizontalement (interactions entre éléments de réseau en communication). Les étiquettes peuvent être incluses dans les paquets de signalisation et/ou dans l'en-tête d'un paquet de données pour identifier et marquer les appels ou les sessions de télécommunications d'urgence. Les étiquettes utilisées pour identifier et marquer les appels ou les sessions et/ou le trafic de télécommunications d'urgence dépendent du protocole. Pour réaliser un traitement spécialisé (par exemple prioritaire ou préférentiel) de bout en bout pour tous les aspects de l'appel ou de la session de télécommunications d'urgence (commande d'appel ou de session, trafic support et gestion), une correspondance et un interfonctionnement appropriés entre les étiquettes utilisées dans les différents protocoles sont nécessaires. Par exemple, l'information d'en-tête de priorité de ressource SIP utilisée dans la couche de commande pour identifier l'appel ou la session prioritaire peut être mise en correspondance avec les codes DiffServ (DSCP) appropriés pour marquer le trafic de télécommunications d'urgence dans la couche de réseau IP. De même, les codes DiffServ (DSCP) au niveau de la couche 3 peuvent être mis en correspondance avec les paramètres de priorité Ethernet ou VLAN spécifiques au niveau de la couche 2 dans le protocole de transport. Le protocole SIP est défini dans [IETF RFC 3261] et dans ses mises à jour [b-IETF RFC 3265], [b-IETF RFC 3853], [b-IETF RFC 4320], [b-IETF RFC 4916], [b-IETF RFC 4032] et [b-IETF RFC 5027].

Dans la strate des services, les services ont tendance à utiliser un certain ensemble désigné de protocoles. Par conséquent, les techniques pouvant être utilisées pour les différents services de télécommunications d'urgence dépendront des services considérés et des capacités des protocoles particuliers liés aux services en question.

Dans la strate de transport, on peut utiliser le protocole Internet (IP). La version IP utilisée peut varier d'un fournisseur à l'autre et il peut être nécessaire d'adapter la connectivité de bout en bout à différentes versions, en utilisant par exemple la tunnellisation d'une version dans une autre. Toutefois, cela ne devrait pas avoir d'incidence sur le transport des informations relatives aux services de télécommunications d'urgence.

De plus, les protocoles utilisés dans les infrastructures d'accès locales (dernier kilomètre) peuvent être différents de ceux utilisés dans les infrastructures centrales. Les infrastructures d'accès locales peuvent être filaires (accès fixe), sans fil, ou utiliser une combinaison de ces deux technologies.

Ainsi, un trajet de bout en bout donné pour un appel ou une session de télécommunications d'urgence peut traverser des technologies de transport très diverses.

Des paragraphes ultérieurs décrivent les diverses caractéristiques et capacités des différentes technologies qui peuvent être utilisées pour faciliter la mise en œuvre des spécifications des télécommunications d'urgence.

Comme la strate de transport peut utiliser le protocole IP et un certain nombre de protocoles associés, tels que TCP ou UDP définis par l'IETF, il est prudent d'utiliser les capacités applicables définies par l'IETF pour la prise en charge des télécommunications d'urgence. Ces capacités sont examinées dans des paragraphes ultérieurs.

Il est important de faire une distinction entre les spécifications (RFC) élaborées par l'IETF et leur déploiement dans l'Internet et dans le contexte d'un NGN. Dans les deux cas, les spécifications réellement utilisées dépendront de ce que le fournisseur concerné aura déployé. Toutefois, comme l'Internet ne relève pas de la compétence de l'UIT-T, aucune hypothèse ne peut être faite sur la qualité de service ou les capacités des trajets basés sur l'Internet, comme cela est expliqué dans [b-IETF RFC 4190][2]. En revanche, les spécifications relatives aux télécommunications d'urgence internationales dans les NGN basés sur IP relèvent de la compétence de l'UIT-T, qui peut proposer des spécifications plus strictes dans des Recommandations UIT-T à utiliser par les fournisseurs NGN.

[IETF RFC 4542] décrit des solutions possibles pour le "service Internet prioritaire en cas d'urgence". Un grand nombre des concepts qui y sont présentés s'appliquent au service ETS dans le contexte des NGN.

Dans un NGN, dans lequel la strate des services et la strate de transport sont indépendantes, les facteurs suivants ont une incidence sur le succès d'une télécommunication d'urgence:

i) identification et marquage du trafic de télécommunications d'urgence;

ii) politique de contrôle d'admission;

iii) politique d'attribution de largeur de bande;

iv) authentification et autorisation des utilisateurs légitimes des télécommunications d'urgence.

9.1.1 Traitement prioritaire

D'une manière générale, le traitement prioritaire est fondamental pour la fourniture de télécommunications d'urgence, qui par définition doivent être considérées comme étant plus importantes que les services de télécommunication ordinaires. Lorsque les services ordinaires utilisent la grande majorité des ressources de réseau, qui sont limitées, les télécommunications d'urgence doivent lutter pour obtenir une part de ces ressources, ce qui peut avoir un effet négatif sur ces télécommunications. Il faut donc concevoir un moyen permettant de traiter prioritairement les télécommunications d'urgence par rapport aux services de télécommunication ordinaires. Il s'agit essentiellement:

a) de reconnaître les utilisateurs autorisés des télécommunications d'urgence;

b) d'accorder la priorité de service aux utilisateurs autorisés des télécommunications d'urgence.

---

[2] Conformément à [b-IETF RFC 4190]:
"Au cours de l'évolution de l'Internet, le service par défaut a toujours été et est toujours le service au mieux", et
"les communications ETS entre domaines ne devraient pas reposer sur une prise en charge ubiquitaire ni même étendue le long du trajet entre les points d'extrémité".

Dans l'architecture NGN en couches définie dans [UIT-T Y.2012], l'indicateur de priorité envoyé par les fonctions de commande de service (SCF, *service control functions*) aux fonctions de contrôle des ressources et d'admission devrait pouvoir indiquer des niveaux de priorité associés aux utilisateurs pour pouvoir mettre en œuvre différentes politiques et distinguer plusieurs types d'applications prioritaires. Par exemple, on pourrait accorder au personnel hospitalier un niveau de priorité inférieur à celui accordé aux coordonnateurs des secours en cas d'urgence critique.

9.1.2 Identification, authentification et autorisation, et contrôle d'accès

Il faut éviter l'accès non autorisé aux services et ressources de télécommunications d'urgence, par exemple, par des intrus se faisant passer pour des utilisateurs autorisés. Il faut donc prendre en charge des mécanismes et des capacités permettant d'authentifier et d'autoriser l'accès des utilisateurs, dispositifs ou combinaisons utilisateur et dispositif des télécommunications d'urgence, selon le cas, compte tenu de la politique applicable au service concerné (par exemple ETS ou TDR).

Il est nécessaire d'identifier les demandes d'appel ou de session de télécommunications d'urgence (par exemple, par des numéros ou des profils d'utilisateur ou d'abonnement spéciaux). Les fournisseurs NGN devraient procéder rapidement à l'authentification des utilisateurs autorisés des télécommunications d'urgence. Il faut utiliser des mécanismes et des méthodes spécifiques d'authentification et d'autorisation, compte tenu de la politique applicable au service concerné des télécommunications d'urgence (par exemple, utilisation d'un numéro d'identification personnel (PIN) et de profils d'utilisateur et d'abonnement).

Parmi les approches relatives à l'authentification et à l'autorisation pour le service ETS, qui sont décrites dans l'Appendice II de [UIT-T Y.2702], figurent:

a) L'utilisation d'un numéro d'identification personnel (PIN, *personal identification number*): dans cette approche, on utilise un numéro PIN pour authentifier et autoriser l'utilisateur. On identifie donc l'utilisateur et non le dispositif d'utilisateur. Par conséquent, cette approche est en principe utilisée dans les cas où l'utilisateur est autorisé à invoquer le service ETS depuis n'importe quel dispositif.

b) L'utilisation d'un profil de service/abonnement: dans cette approche, on indique dans le profil de service du terminal d'utilisateur l'abonnement au service ETS. Le terminal d'utilisateur est authentifié et le profil de service de l'utilisateur est identifié dans le cadre de la procédure normale d'enregistrement du fournisseur NGN (à savoir le fournisseur du service ETS). Lorsque l'utilisateur lance une demande, une comparaison avec le profil de service de l'utilisateur permet de déterminer si l'utilisateur est autorisé à utiliser le service ETS. La demande de service ETS est accordée si l'abonnement au service ETS est validé pour le terminal d'utilisateur.

c) L'utilisation d'une combinaison numéro PIN et profil de service: des approches combinant les méthodes reposant sur le numéro PIN et sur le profil de service peuvent aussi être utilisées pour authentifier à la fois l'utilisateur et le dispositif d'utilisateur afin d'offrir des niveaux plus élevés de garantie.

d) L'utilisation de jetons de sécurité spéciaux et de capacités biométriques: outre les approches décrites ci-dessus, on peut utiliser des approches plus complexes reposant sur des jetons de sécurité spéciaux et sur des capacités biométriques pour authentifier et autoriser les utilisateurs ETS et les terminaux afin d'offrir un niveau plus élevé d'attestation d'identité.

Une fois que l'utilisateur, le dispositif d'utilisateur ou la combinaison utilisateur et dispositif est authentifié et autorisé, compte tenu de la politique applicable, l'appel ou la session de télécommunications d'urgence doit être marqué et indiqué en aval vers les réseaux suivants, et la priorité doit être accordée à tous les aspects de l'appel/de la session de télécommunications d'urgence, la signalisation/commande, le trafic support et toute gestion applicable.

Il faut aussi prendre en considération l'authentification et l'autorisation pour le transfert et la réception des appels ou des sessions de télécommunications d'urgence entre fournisseurs NGN, compte tenu d'un environnement multifournisseurs et de la séparation entre commande de service et transport. L'authentification et l'autorisation des fournisseurs NGN pour le transfert et la réception des appels/sessions et du trafic de télécommunications d'urgence devraient s'appuyer sur les accords SLA et sur la politique applicable.

On peut s'appuyer sur les fonctionnalités de gestion IdM ([UIT-T Y.2720], [UIT-T Y.2721] et [UIT-T Y.2722]) pour renforcer la confiance dans les informations d'identité relatives aux applications des télécommunications d'urgence. L'Appendice III de [UIT-T Y.2721] donne des exemples de cas d'utilisation de fonctionnalités IdM relatives au service ETS, qui décrivent la manière d'utiliser les fonctionnalités IdM pour prendre en charge des applications ETS et qui portent sur les questions suivantes:

- garantie d'authentification utilisant la combinaison dispositif et utilisateur (par exemple corrélation de l'authentification de l'utilisateur et du dispositif);
- amélioration de l'authentification des utilisateurs ETS pour les services prioritaires de prochaine génération (par exemple utilisation de jetons, de certificats numériques, de la reconnaissance vocale et de la biométrie);
- authentification de la partie appelée et des sources de communication de données (par exemple, garantie de messages et de sources de données);
- identification et authentification des fournisseurs de services dans un environnement multifournisseurs (par exemple, identification des fournisseurs d'accès, de contenu et de services réseau);
- accès unique et interruption unique (par exemple, accès à des applications multiples sans qu'il soit nécessaire de fournir des justificatifs d'identité à titre individuel pour chaque application).

9.1.3 Considérations relatives au contrôle d'admission pour une probabilité d'admission plus élevée

La fonction de contrôle des ressources et d'admission (RACF) a notamment pour rôle d'assurer un contrôle de la qualité de service afin de procéder à une admission et à une réservation de ressources si le fournisseur de services le souhaite. A cet égard, lorsque les demandes de service émanant des utilisateurs sont nombreuses, il faudra peut-être en refuser certaines. Si ces refus n'ont pas lieu, le NGN ne pourra peut-être pas garantir entièrement la qualité de service dans les situations d'urgence. Les processus de la fonction RACF liés à la qualité de service font intervenir une autorisation basée sur les profils d'utilisateur, des accords SLA, des règles propres à l'opérateur, la priorité de service et la disponibilité des ressources de transport dans les réseaux d'accès et dans les réseaux centraux. Dans la présente Recommandation, on suppose que la fonction RACF devrait pouvoir classer les demandes de service par ordre de priorité en utilisant la priorité de service. (Un réseau qui ne fait que refuser des demandes autorisées en cas d'encombrement temporaire offre un service de qualité médiocre aux clients si ceux-ci sont contraints de resoumettre leurs demandes de façon répétée.) On suppose donc, dans la présente Recommandation, que la priorité de service est un facteur essentiel à prendre en compte dans la méthode de programmation de la file d'attente d'attribution des ressources/la décision générale d'admission. Des mécanismes permettant d'assurer cette fonctionnalité sont examinés ci-dessous.

La fonction RACF doit avant tout traiter les demandes autorisées de qualité de service en utilisant les profils d'utilisateur et la priorité. En particulier, le contrôle d'admission doit utiliser les informations de priorité de service pour gérer la priorité. Diverses méthodes peuvent être utilisées pour la prise en compte de la priorité de service dans le contrôle d'admission basé sur les ressources.

Une méthode possible consiste à fixer un seuil d'admission plus élevé pour le trafic des télécommunications d'urgence, ce qui permet d'admettre davantage de demandes prioritaires lorsque des demandes normales sont refusées. Cette méthode permet en fait d'augmenter temporairement l'utilisation des ressources de réseau. Toutefois, étant donné que les ressources NGN sont nombreuses et que, dans un intervalle de temps sensible, certaines ressources seront progressivement libérées (par exemple, à mesure que des sessions se terminent), le système reviendra à sa capacité de trafic journalière opérationnelle prévue. En outre, dans l'hypothèse où la quantité de trafic prioritaire est relativement faible et où les réseaux fonctionnent rarement, voire jamais, à leur pleine capacité de 100 pour cent, le seuil d'admission plus élevé pour le trafic prioritaire ne devrait pas poser de problème en ce qui concerne la qualité de fonctionnement générale du réseau ou la qualité de service pour le trafic normal.

Il existe des systèmes de contrôle d'admission basé sur la réservation qui n'autorisent une demande de service que lorsque la demande de largeur de bande nécessaire a abouti. Dans ce cas, la méthode utilisée pour les mécanismes de programmation devrait tenir compte en premier lieu de la priorité de service.

Enfin, d'autres mécanismes possibles contournent les mécanismes de contrôle d'admission (par exemple, trafic prioritaire contournant la fonction RACF). Un exemple de tel mécanisme est actuellement en cours de description au sein de l'IETF.

9.1.3.1 Contrôle d'admission d'appel

Le contrôle d'admission d'appel (CAC, *call admission control*) est un ensemble de mesures et de dispositions prises par le réseau pendant la phase d'établissement d'appel ou de session afin d'accepter ou de rejeter un service, compte tenu de la qualité de fonctionnement demandée et des critères de priorité, et de la disponibilité des ressources nécessaires.

Dans un RTPC/RNIS classique, le contrôle d'admission d'appel consiste simplement à accorder ou non un circuit sur la base de l'autorisation. De plus, l'attribution d'un circuit suppose, par définition, qu'un trajet ayant la largeur de bande nécessaire soit disponible. Compte tenu de la disponibilité des informations d'état du réseau concernant le statut des différents circuits (canaux dans la bande vocale), un RTPC/RNIS peut:

a) dévier les appels d'urgence sur des trajets spécifiquement réservés au trafic d'urgence (si de tels trajets sont disponibles);

b) attendre qu'un circuit soit disponible (mise en file d'attente).

Comme il n'existe pas de trajets individuels ni d'informations d'état des circuits dans les réseaux IP, l'authentification et l'autorisation à l'entrée du réseau ne suffisent pas à garantir la disponibilité d'un trajet de bout en bout ou d'une largeur de bande de bout en bout suffisante pour un appel ou une session donné. Dans un réseau IP, un élément de réseau entrant n'a pas ou peu d'informations sur les conditions de réseau qui prévalent en dehors de son domaine. Par conséquent, le contrôle CAC dans un élément de réseau entrant est insuffisant pour garantir la disponibilité d'un trajet de bout en bout à moins qu'il ne soit complété par d'autres mécanismes.

Autre conséquence: un élément de réseau sortant n'a aucun contrôle ni aucune information sur l'élément de réseau entrant distant susceptible de tenter d'établir un appel ou une session avec lui. Toutefois, dans un RTPC/RNIS, un élément de réseau sortant est en mesure de contrôler un élément de réseau entrant potentiel, tentant d'établir un appel/une session, via les mécanismes de signalisation associés.

[UIT-T Y.2171] définit des niveaux de priorité de contrôle d'admission pour les services de télécommunications cherchant à entrer dans un réseau, notamment pendant des situations d'urgence lorsque les ressources de réseau peuvent être épuisées. En particulier, elle recommande trois niveaux de priorité de contrôle d'admission pour les services cherchant à entrer dans un NGN. Le niveau de priorité 1 (le plus élevé) est recommandé pour les télécommunications d'urgence (y compris le service ETS) dans les NGN. Le trafic ayant ce niveau de priorité est le trafic admis en priorité dans un NGN.

9.2 Strate des services

9.2.1 Généralités

Un service ETS est opérationnel ou en cours de mise au point dans chaque pays, le but étant de pouvoir traiter prioritairement le trafic autorisé lors des opérations de secours en cas d'urgence ou de catastrophe sur le territoire national. Toutefois, il peut arriver une situation de crise dans laquelle il est important qu'un utilisateur ETS d'un pays donné puisse communiquer avec des utilisateurs dans un autre pays. Dans ce cas, il est important qu'un appel ou une session ETS provenant d'un pays donné soit traité de façon prioritaire de bout en bout, autrement dit à la fois dans le pays d'origine et dans le pays de destination. Pour cela, il peut être nécessaire de prévoir une interconnexion de deux mises en œuvre nationales du service ETS via un réseau international qui offre des capacités de traitement prioritaire ou qui achemine la priorité de façon transparente entre les deux pays.

Les paragraphes qui suivent décrivent un certain nombre de mécanismes de protocole utilisés pour signaler et obtenir un traitement prioritaire au niveau de la commande de service dans le contexte d'un NGN par paquets. Ils attirent en outre l'attention sur l'applicabilité spécifique de ces mécanismes au service ETS. Ces capacités de protocole sont nécessaires pour les applications internationales dans le contexte des communications entre mises en œuvre nationales du service ETS via le réseau international (par exemple, interconnexion de deux mises en œuvre nationales du service ETS).

9.2.2 Priorité de ressource SIP

[IETF RFC 4412] ajoute deux champs d'en-tête SIP, à savoir les champs de priorité de ressource et d'acceptation de priorité de ressource, et spécifie les procédures applicables à leur utilisation. Le champ d'en-tête de priorité de ressource peut être utilisé par les agents d'utilisateur SIP, y compris les passerelles et terminaux de réseau téléphonique public commuté (RTPC), et par les serveurs proxy SIP pour influer sur leur traitement des demandes SIP.

Pour donner une équivalence avec certains systèmes existants, on peut prendre en charge la priorité appropriée pour plusieurs systèmes "normalisés" différents en identifiant l'"espace de noms" approprié pour le système considéré et le nombre de niveaux de priorité dans ce système. Les espaces de noms suivants et le nombre associé de niveaux de priorité sont identifiés dans [IETF RFC 4412] pour être utilisés dans le service ETS.

Espace de noms	Niveaux
ets	5
wps	5

Pour désigner tous les appels/toutes les sessions ETS dans les environnements IP, on utilise un espace de noms "ets" avec cinq niveaux de priorité qui acheminent les niveaux d'importance dans la couche application (dans les éléments SIP). Les appels ou sessions ETS entrants se voient attribuer la désignation "ets" dans l'en-tête de priorité de ressource. Les appels ou sessions ETS sont reconnus par la présence de la valeur de l'espace de noms "ets" dans l'en-tête de priorité de ressource du message SIP et se voient accorder la priorité "élevée" pour la réservation/attribution de ressource de sorte qu'un traitement préférentiel puisse être assuré dans la couche transport. Un

espace de noms analogue désigné par "wps" avec cinq niveaux de priorité est disponible pour les attributions d'appel/de session en cas de ressources limitées ou d'encombrement, par exemple pour l'accès radioélectrique aux réseaux sans fil.

9.2.3 Plan IEPS

[UIT-T E.106] décrit les fonctions requises, les caractéristiques, l'accès et la gestion opérationnelle du plan IEPS. Ce plan permet d'interconnecter différentes mises en œuvre nationales de plans de priorité et d'assurer ainsi un traitement préférentiel de bout en bout des appels vocaux et de données à bande étroite autorisés.

[UIT-T E.106] s'applique dans le contexte du RTPC, du RNIS ou du RMTP. Le plan IEPS permet aux utilisateurs autorisés de bénéficier d'un traitement prioritaire pour le service téléphonique international sur les réseaux de télécommunication en mode connexion. Par conséquent, sur la base d'accords bilatéraux ou multilatéraux entre pays/administrations, le plan IEPS peut être utilisé dans un scénario de ce type pour l'interconnexion de mises en œuvre nationales du service ETS.

9.2.4 Protocoles de commande des systèmes UIT-T H.323

Le présent paragraphe indique les protocoles utilisés dans les systèmes UIT-T H.323 pour les télécommunications prioritaires.

[UIT-T H.460.4] spécifie la désignation de priorité d'appel et l'identification du pays/réseau international d'origine de l'appel pour les appels prioritaires UIT-T H.323. Le paramètre de désignation de priorité d'appel UIT-T H.460.4 prend en charge l'indicateur d'appel prioritaire et cinq niveaux de priorité.

[UIT-T H.248.1] définit les protocoles utilisés entre les éléments d'une passerelle multimédia décomposée physiquement, utilisés conformément à l'architecture spécifiée dans [UIT-T H.323]. Pour les services d'urgence autorisés par les pouvoirs publics (par exemple, service ETS), [UIT-T H.248.1] définit l'indicateur d'appel IEPS et l'indicateur de priorité. L'indicateur d'appel IEPS achemine l'indication de priorité entre le contrôleur et la passerelle. L'indicateur de priorité achemine les niveaux de priorité entre le contrôleur et la passerelle, 16 niveaux de priorité étant pris en charge. L'indicateur d'appel IEPS et l'indicateur de priorité satisfont aux exigences liées au service ETS consistant respectivement à indiquer un contexte ETS et à acheminer le niveau de priorité. Pour les services de sécurité du public, [UIT-T H.248.1] définit l'indicateur d'urgence destiné à acheminer l'indication de priorité entre le contrôleur et la passerelle.

[UIT-T H.248.81] énonce les lignes directrices relatives à l'utilisation de l'indicateur d'appel et de l'indicateur de priorité dans les profils UIT-T H.248 des systèmes UIT-T H.323 et NGN pour la prise en charge de services prioritaires (par exemple, le service ETS).

9.2.5 Protocole Diameter (Diamètre)

Le protocole Diameter [IETF RFC 3588] prend en charge l'authentification, l'autorisation et la comptabilité (AAA) pour les fonctions et applications de réseau telles que l'accès au réseau et la mobilité IP.

Les paires attribut-valeur (AVP, *attribute value pair*) ci-après sont censées être utilisées dans le protocole Diameter pour prendre en charge des services prioritaires (par exemple le service ETS):

- Identificateur de service MPS (MPS-Identifier)
- Priorité de réservation (Reservation-Priority)
- Niveau de priorité (Priority-Level) (dans le cadre de la paire AVP de priorité de rétention d'attribution (Allocation Retention Priority (ARP))
- Priorité de session (Session-Priority).

La paire AVP de l'identificateur de service MPS est définie par le 3GPP dans le document [b-3GPP TS 29.214]. L'identificateur de service MPS sert à désigner la demande d'un service prioritaire (par exemple un service ETS/MPS à l'interface Rx). La paire APV de l'identificateur de service MPS contient la variante nationale du nom du service prioritaire.

La paire AVP de priorité de réservation est définie par l'Institut européen des normes de télécommunications (ETSI) dans [ETSI TS 183 017]. [UIT-T Q.3321.1] et [UIT-T Q.3303.3] définissent l'utilisation de la paire AVP de priorité de réservation aux interfaces Rs et Rw de la fonction RACF [UIT-T Y.2111], respectivement, pour la prise en charge de services prioritaires. De même, [b-3GPP TS 29.214] (Commande de la politique et de la taxation au point de référence Rx) et [UIT-T Q.1741.6] définissent la paire AVP de priorité de réservation à l'interface Rx de la commande de la politique et de la taxation (PCC) pour la prise en charge de services prioritaires (par exemple le service ETS). La paire AVP de priorité de réservation prend en charge 16 niveaux de priorité qui peuvent être utilisés pour demander un traitement prioritaire. Les valeurs comprises entre 0 et 15 sont indiquées par ordre croissant de priorité, "15" correspondant à la valeur la plus élevée et "0" à la valeur la plus faible. La paire AVP de priorité de réservation contient la valeur de priorité de l'utilisateur.

La paire AVP de niveau de priorité (dans le cadre de la paire AVP de priorité de rétention de l'attribution (ARP)) est définie par le 3GPP dans [b-3GPP TS 29.212] (Commande de la politique et de la taxation au point de référence Rx) dans [UIT-T Q.1741.6]. Celle-ci définit la paire AVP de niveau de priorité à l'interface Gx de la commande de la politique et de la taxation (PCC) pour la prise en charge de services prioritaires (par exemple le service ETS). La paire AVP de niveau de priorité prend en charge 15 niveaux de priorité qui peuvent être utilisés pour demander un traitement prioritaire. Les valeurs comprises entre 1 et 15 sont indiquées par ordre décroissant de priorité, "1" correspondant à la valeur la plus élevée et "15" à la valeur la plus faible. Les valeurs de priorité comprises entre 1 et 8 sont attribuées pour les services qui sont autorisés à bénéficier d'un traitement prioritaire (par exemple le service ETS ou le service MPS). La valeur de priorité "0" est une valeur de réserve et est considérée comme une erreur logique si elle est reçue. La paire AVP de niveau de priorité contient la valeur de priorité de l'utilisateur.

La paire AVP de priorité de session est définie dans [b-3GPP TS 29.229] (Interfaces Cx et Dx fondées sur le protocole Diameter; précisions relatives au protocole) et dans [UIT-T Q.1741.6]. [b-3GPP TS 29.229] définit l'utilisation de la paire AVP de priorité de session aux interfaces Cx et Dx pour la prise en charge de services prioritaires (par exemple le service ETS). De même, [b-3GPP TS 29.329] (interface Sh fondée sur le protocole Diameter; précisions sur le protocole) et [UIT-T Q.1741.6] définissent l'utilisation de la paire AVP de priorité de session à l'interface Sh pour la prise en charge de services prioritaires. La paire AVP de priorité de session prend en charge 5 niveaux de priorité qui peuvent être utilisés pour demander un traitement prioritaire aux interfaces Cx, Dx et Sh. Les valeurs comprises entre 0 et 4 sont définies pour apparaître par ordre décroissant de priorité, "0" correspondant à la valeur la plus élevée et "4" à la valeur la plus faible.

9.3 Strate de transport

9.3.1 Généralités

La nécessité d'accords spéciaux (par exemple, des accords SLA) pour prendre en charge les télécommunications d'urgence dans un NGN correctement conçu et dimensionné est fondée sur l'hypothèse selon laquelle les ressources de réseau sont insuffisantes par rapport au volume de trafic offert sur le réseau et que, dans ces conditions, le trafic de télécommunications d'urgence risque d'être rejeté ou fortement retardé et/ou perturbé au point d'être inutilisable, voire éliminé. Lorsque le volume de trafic reçu dans le cas d'un modèle de service au mieux ou conçu statistiquement dépasse la capacité d'un élément de réseau de réception donné (par exemple, un routeur IP) et la capacité sortante disponible au niveau de l'élément considéré, la seule possibilité pour cet élément de réseau est d'éliminer le trafic en excès. Autrement dit, le trafic d'urgence serait éliminé au même titre que

le trafic normal sauf si des mesures spéciales de traitement préférentiel sont adoptées (par exemple comme indiqué dans un SLA). Le Forum TM a donné des indications sur la spécification et la gestion des SLA [b-TM Forum GB917] et a notamment examiné les modalités d'application de ces indications aux ETS.

La technique du surapprovisionnement est parfois proposée comme solution. Toutefois, le surapprovisionnement est impossible ou irréalisable dans bien des cas et, surtout, certains types d'urgence peuvent résulter de la destruction ou de la dégradation délibérée ou accidentelle de certaines parties du réseau, ce qui élimine des trajets ou des éléments surapprovisionnés qui auraient pu être normalement disponibles. Le surapprovisionnement présente donc des aspects négatifs. Si on veut qu'un NGN puisse traiter tous les types d'urgences dans des situations difficiles, il faut prévoir un système spécifique de traitement préférentiel du trafic de télécommunications d'urgence.

Les paragraphes qui suivent présentent un certain nombre de mécanismes utilisés pour assurer un traitement prioritaire au niveau du transport dans le contexte d'un NGN par paquets.

9.3.2 Gestion de la largeur de bande au moyen de RSVP

Dans les réseaux IP, un équivalent (approximatif) de l'attribution de largeur de bande basée sur les circuits pourrait être un mécanisme IP d'attribution et de réservation de largeur de bande. Un tel mécanisme existe sous forme de procédure définie par l'IETF dans son protocole de réservation de ressource (RSVP) spécifié dans [IETF RFC 2205] et dans ses mises à jour [b-IETF RFC 2750], [b-IETF RFC 3936] et [b-IETF RFC 4495].

Le paramétrage de gestion des ressources nécessaire pour le protocole d'ouverture de session (SIP) dans la strate des services à utiliser conjointement avec le protocole RSVP (dans la strate de transport) est spécifié dans [IETF RFC 3312]. Ainsi, la signalisation RSVP peut être utilisée avant ou pendant les procédures de signalisation SIP et/ou peut être entrelacée avec ces procédures. Des exemples sont donnés dans l'Appendice A de [IETF RFC 4542]. Toutefois, [IETF RFC 4542] utilise la technique de préemption.

L'IETF définit actuellement des extensions du protocole RSVP qui peuvent être utilisées pour prendre en charge une capacité de priorité d'admission au niveau de la couche réseau. Il spécifie de nouvelles extensions du protocole RSVP pour augmenter la probabilité d'aboutissement des appels sans préemption. On utilise des modèles d'attribution de largeur de bande pour satisfaire à la "priorité d'admission" requise par un réseau de télécommunications d'urgence mettant en œuvre le protocole RSVP. En particulier, ces extensions spécifient deux nouveaux éléments de politique RSVP permettant d'acheminer la priorité d'admission à l'intérieur des messages de signalisation RSVP de sorte que les nœuds RSVP puissent prendre des décisions de contrôle d'admission en fonction de la largeur de bande, compte tenu de la priorité d'admission de l'appel.

9.3.3 Gestion de la mise en file d'attente au moyen de services différenciés

[IETF RFC 4594] présente une mise en correspondance recommandée entre les classes de service et les codes de services différenciés (DSCP, *differentiated services code points*). La Figure 3 de [IETF RFC 4594] contient une table de correspondance qui associe la classe de transmission express aux applications de téléphonie, ce qui permet aux paquets IP de contenir une valeur de code DSCP correspondant à la classe de transmission express.

De plus, [UIT-T Y.1541] recommande que le trafic vocal soit marqué (étiqueté) dans les paquets IP avec le code DSCP correspondant à la transmission express. Les éléments de réseau (routeurs) de la strate de transport qui reçoivent des paquets marqués transmission express garantiront une remise rapide du trafic à temps critique par rapport au trafic qui n'est pas à temps critique en utilisant le comportement de transmission express défini pour le code de transmission express, spécifié dans [IETF RFC 3246].

Toutefois, le code de transmission express est utilisé pour le trafic téléphonique normal. Par conséquent, il reste nécessaire de différencier d'une manière ou d'une autre le trafic téléphonique d'urgence et le trafic téléphonique normal (voir le paragraphe qui suit).

9.3.4 Code DSCP de transmission express pour le trafic ayant fait l'objet d'une admission de capacité

[IETF RFC 5865] définit un code DSCP VOICE-ADMIT pour une classe de trafic qui fait l'objet d'un contrôle CAC strict et comporte le trafic ETS. Cela permet d'avoir un trafic en temps réel conforme au comportement par saut de transmission express basé sur une procédure CAC avec authentification, autorisation et admission de capacité (voir § 9.3.1 et 9.3.2 ci-dessus) par opposition à une classe de trafic en temps réel conforme au comportement par saut de transmission express qui n'a pas fait l'objet d'une admission de capacité.

9.3.5 Notification d'encombrement explicite (ECN, *explicit congestion notification*)

[IETF RFC 3168] définit l'architecture à double couche de la notification ECN comme une architecture qui fonctionne au niveau de la couche réseau (c'est-à-dire le protocole IP) et de la couche transport (par exemple le protocole TCP). Son objectif est de fournir un retour d'information explicite transmis dans les délais à la source de l'encombrement dans le sens aval, avec une perte minimale de paquets, voire aucune perte et, en conséquence, en perturbant le moins possible les flux. Cette information est transmise au moyen de noeuds intermédiaires prenant en charge la gestion active de la mise en file d'attente (AQM), qui marque les paquets avec une notification d'encombrement et les retransmet vers l'aval au lieu d'abandonner le paquet. Le point d'extrémité du flux renvoie alors une indication de retour d'information (c'est-à-dire une notification ECN) vers la source par l'intermédiaire d'un protocole de transport de couche supérieure. [IETF RFC 4340] a étendu la prise en charge de la notification ECN au protocole de commande de l'encombrement des données (DCCP, *data congestion control protocol*).

En cas d'utilisation des protocoles TCP et DCCP, la notification ECN déclenche des algorithmes de temporisation qui sont transparents pour les applications. L'avantage général de cette fonction est que les applications deviennent plus conviviales s'agissant de l'utilisation de l'Internet et réduisent la charge de trafic offerte, ce qui permet à un plus grand nombre d'utilisateurs et d'applications d'utiliser le réseau. Dans ce scénario transparent pour les applications, la notification ECN ne favorise pas particulièrement les utilisateurs du service ETS par rapport au grand public. En revanche, la notification ECN facilite l'utilisation continue des ressources réseau par les utilisateurs du service ETS et le grand public.

Le Groupe de travail sur les réseaux de l'IETF étudie actuellement comment utiliser la notification ECN pour les flux RTP acheminés à l'aide du protocole UDP/IP qui utilisent le protocole RTCP comme mécanisme de retour d'information. La solution consiste à envoyer en retour des marquages d'encombrement ECN à l'expéditeur au moyen du protocole RTCP, à vérifier les fonctionnalités ECN de bout en bout et à indiquer comment commencer à utiliser la notification ECN. Les études menées actuellement par l'IETF visent à ajouter une prise en charge ECN pour les applications en temps réel (par exemple la voix et la vidéo) au moyen des protocoles RTP/RTCP. En pareil cas, la notification de l'encombrement est communiquée aux applications, qui peuvent réagir de différentes manières à cette notification. Il est à prévoir que la réaction par défaut suivra celle des protocoles TCP et DCCP, à savoir que l'application réduit la charge offerte du réseau.

9.4 Accès au NGN

9.4.1 Généralités

Il existe plusieurs méthodes d'accès au NGN qui dépendent de la technologie. Conformément à [UIT-T Y.2012], le réseau d'accès inclut des fonctions qui dépendent de la technologie d'accès, par

exemple pour la technologie W-CDMA et l'accès xDSL. Suivant la technologie utilisée pour accéder aux services NGN, le réseau d'accès inclut des fonctions liées à:

1) l'accès par câble;

2) l'accès xDSL;

3) l'accès sans fil (par exemple, technologies [b-IEEE 802.11] et [b-IEEE 802.16] et accès 3G RAN);

4) l'accès optique.

Pour prendre en charge les télécommunications d'urgence, des accords spéciaux sont également nécessaires dans le segment d'accès au NGN. La nécessité d'accords spéciaux est basée sur l'hypothèse que, tout comme les ressources de réseau central sont limitées, les ressources de réseau d'accès le sont aussi. Par conséquent, suivant le volume de trafic offert au segment de réseau d'accès, le trafic de télécommunications d'urgence peut être affecté (par exemple, rejeté ou fortement retardé et/ou perturbé au point d'être inutilisable, voire éliminé).

Par conséquent, si on veut que le NGN puisse traiter tous les types d'urgences dans des situations difficiles, il faut prévoir un système spécifique de traitement préférentiel du trafic de télécommunications d'urgence dans le segment d'accès au NGN, par exemple des mécanismes et capacités permettant (liste non exhaustive):

- de reconnaître le trafic de télécommunications d'urgence;
- d'assurer un accès prioritaire aux ressources/installations;
- d'assurer un routage prioritaire du trafic de télécommunications d'urgence;
- d'assurer un établissement prioritaire des sessions/appels de télécommunications d'urgence.

Lorsqu'on établit le traitement prioritaire pour des télécommunications d'urgence, il faut tenir compte des aspects suivants: classer ou étiqueter le trafic afin qu'ils bénéficient d'un traitement prioritaire, procéder à une signalisation pour créer le trajet permettant de transporter ce trafic et élaborer des mécanismes, y compris les politiques permettant de prendre en charge la priorité demandée. Certains aspects tels que le choix des mécanismes, des politiques et des implémentations associées ne sont pas normalisés et peuvent être propres à une région.

9.4.2 Accès radioélectrique sans fil

Les réseaux d'accès radioélectrique sans fil doivent prendre en charge des mécanismes et capacités spécifiques pour assurer un traitement prioritaire des appels ou sessions autorisés de télécommunications d'urgence. Pour cela, on peut utiliser des mécanismes et capacités qui dépendent de la technologie, notamment des mécanismes et capacités permettant (liste non exhaustive):

- de reconnaître le trafic de télécommunications d'urgence: identification et marquage des télécommunications d'urgence autorisées;
- d'assurer un accès prioritaire aux ressources/installations: cela facilite la remise d'une demande de télécommunications d'urgence à un NGN lorsque les ressources d'accès disponibles sont peu nombreuses;
- d'assurer un routage prioritaire du trafic de télécommunications d'urgence: il peut s'agir de fonctionnalités comme la mise en file d'attente dans l'attente de ressources disponibles, la dispense de certaines fonctions de gestion de réseau restrictives et la réservation de certaines routes/certains trajets pour les télécommunications d'urgence;
- d'assurer un établissement prioritaire des appels ou sessions de télécommunications d'urgence.

9.4.2.1 Systèmes de télécommunications mobiles universelles (UMTS) et évolution à long terme (LTE)

Le service de priorité et le service de priorité multimédia pour les systèmes 3GPP sont spécifiés dans [b-3GPP TS 22.153]. Le service de priorité et le service de priorité multimédia spécifiés par le 3GPP permettent aux utilisateurs autorisés d'accéder prioritairement aux prochains canaux radioélectriques (trafic vocal ou de données) disponibles avant les autres utilisateurs dans les situations où l'encombrement bloque les tentatives d'appel. Le service de priorité assure la progression d'appel prioritaire et l'aboutissement d'appel afin de prendre en charge un appel prioritaire "de bout en bout" entre deux réseaux mobiles, d'un réseau mobile vers un réseau fixe et d'un réseau fixe vers un réseau mobile. Le service de priorité multimédia assure la progression prioritaire de sessions multimédias et leur aboutissement afin de prendre en charge les sessions multimédias prioritaires "de bout en bout", notamment entre deux réseaux mobiles, d'un réseau mobile vers un réseau fixe et d'un réseau fixe vers un réseau mobile.

Sur la base de [b-3GPP TS 22.153], le 3GPP met actuellement au point un rapport technique d'étape 2 en vue d'apporter des améliorations au service prioritaire multimédia (MPS) [b-3GPP TS 23.854], afin d'identifier les modifications à apporter aux spécifications actuelles 3GPP d'étape 2 (par exemple, [b-3GPP TS 23.401], [b-3GPP TS 23.203], [b-3GPP TS 22.328] et [b-3GPP TS 22.272]), pour la prise en charge du MPS, notamment les aspects liés aux sous-systèmes multimédia IP (IMS) et de commande de la politique et de la taxation (PCC, *policy and charging control*). Ce rapport technique vise à préciser les prescriptions en matière d'architecture et les flux d'appel ou de session pour le MPS. A partir des prescriptions d'étape 2 du 3GPP, les modifications à apporter aux spécifications actuelles d'étape 3 du 3GPP pour prendre en charge le MPS pour les techniques d'accès UMTS et LTE seront précisées.

9.4.2.2 Evolution – Données optimisées (EV-DO)

Comme le 3GPP, le 3GPP2 a spécifié le service prioritaire multimédia (MMPS, *multimedia priority service*) pour les systèmes 3GPP2. La spécification 3GPP2 pour le MMPS est [b-3GPP2 S.R0117-0]. Plusieurs fonctionnalités, telles que la mise à jour des niveaux de priorité du support, sont prévues dans les normes relatives à l'interface réseau des systèmes 3GPP2 et ces fonctionnalités peuvent être utilisées pour fournir un service MMPS. De même, plusieurs fonctionnalités, telles que la mise en file d'attente, sont prévues dans les normes relatives à l'interface radioélectrique des systèmes 3GPP2 et ces fonctionnalités peuvent servir à fournir un service MMPS.

9.4.2.3 Accès au réseau WiMAX

[b-WFM Stage1-r1] définit les prescriptions d'étape 1 applicables au service de télécommunications d'urgence (ETS) sur les réseaux WiMAX pour la version 1.6 sur la base de la norme [b-IEEE 802.16] 2009 relative à l'interface radioélectrique. Le document [b-WFM Stage1-r2] est une amélioration des prescriptions d'étape 1 WiMAX ETS (version 1.6) relative à la version 2.0 pour la prise en charge de la norme [b-IEEE 802.16m] (interface radioélectrique).

[b-WFM Stage2-a1] spécifie pour le service ETS le cadre de la solution réseau WiMAX d'étape 2 pour la version 1.6 en vue de la prise en charge des prescriptions d'étape 1. Ce cadre traite de l'indication de priorité et du traitement prioritaire déclenchés par le réseau pour l'architecture d'authentification, d'autorisation et de comptabilité (AAA). Le cadre ETS fondé sur l'architecture de commande de la politique et de la taxation (PCC) et les mécanismes de priorité déclenchés par l'UE sont en cours de mise au point pour la version 2.0.

[b-WFM Stage3-a1] spécifie les procédures et les messages du réseau WiMAX d'étape 3 pour la version 1.6 prenant en charge l'indication de priorité et le traitement prioritaire sur la base du cadre de la solution d'étape 2. Un champ d'indication de priorité est ajouté au paramètre Descripteur de qualité de service (QoS Descriptor) des messages WiMAX RADIUS et Diameter. Les procédures d'indication de priorité applicables à l'architecture AAA déclenchée par le réseau ainsi que les mécanismes de traitement prioritaire des entités fonctionnelles de la station de base (BS), de la

passerelle ASN et du réseau du service de connectivité (CSN, *connectivity service network*) sont également décrites dans ce document. Les principaux domaines de prise en charge ETS dans le réseau WiMAX sont les suivants:

1) Lors de l'entrée initiale dans le réseau, dans le cas d'un équipement UE associé à un abonnement WiMAX compatible ETS, les indications de priorité associées aux flux de service initiaux pour l'équipement UE sont transmises du serveur de l'architecture d'authentification, d'autorisation et de comptabilité (AAA) vers la passerelle du réseau du service d'accès (ASN, *access service network*) avec la station de base (BS). La station BS applique un traitement prioritaire à l'attribution et à la programmation des ressources pour les flux de service prioritaires.

2) En cas d'invocation de service ETS émanant d'un équipement UE, les indications de priorité associées aux flux de service pour l'équipement UE sont transmises du serveur de la fonction d'application (AF)/fonction AAA/de politique (PF) vers la passerelle ASN avec la station BS. La station BS applique un traitement prioritaire à l'attribution et à la programmation des ressources pour les flux de service prioritaires.

3) En cas de transfert, les indications de priorité associées aux flux de service pour l'équipement UE sont maintenues du serveur de la station BS vers la station BS cible pour le transfert intra-ASN et de la passerelle ASN de rattachement vers la passerelle ASN cible. Les stations BS appliquent un traitement prioritaire à l'attribution et à la programmation des ressources pour tous les flux de service prioritaires pendant la préparation et la mise en œuvre du transfert.

4) En cas de radiorecherche vers un équipement UE en mode repos, l'indication de priorité associée au flux de service est transmise de la passerelle ASN dotée de la fonction itinéraire de données vers le dispositif de commande de radiorecherche d'ancrage puis vers la station BS. La station BS applique un traitement prioritaire à l'attribution et à la programmation des ressources pour les flux de service prioritaires des messages de radiorecherche de radiodiffusion. En réponse à une radiorecherche prioritaire, lorsque l'équipement UE entre dans le réseau, la station BS reconnaît la priorité de l'appel ETS entrant et accorde un traitement prioritaire à l'équipement UE pour la sortie du mode repos et l'adjonction/la modification des flux de service pour l'appel ETS vers l'équipement UE de terminaison.

Les procédures et messages d'étape 3 supplémentaires pour le service ETS en vue de la prise en charge de l'indication de priorité et du traitement prioritaire pour la télémétrie, la création de flux de service et l'interface de service universelle (USI, *universal services interface*) sont en cours de mise au point pour la version 2.0.

9.4.3 Accès fixe

Les réseaux d'accès fixe doivent prendre en charge des mécanismes et capacités spécifiques pour assurer un traitement prioritaire des appels ou sessions autorisés de télécommunications d'urgence. Pour cela, on peut utiliser des mécanismes et capacités propres à une technologie (par exemple, [b-802.1p] avec xDSL, IPCablecom, Packet Cable 2), notamment des mécanismes et capacités permettant (liste non exhaustive):

- de reconnaître le trafic de télécommunications d'urgence: identification et marquage des télécommunications d'urgence autorisées;
- d'assurer un accès prioritaire aux ressources/installations: cela facilite la remise d'une demande de télécommunications d'urgence à un NGN lorsque les ressources d'accès disponibles sont peu nombreuses;
- d'assurer un routage prioritaire du trafic de télécommunications d'urgence: il peut s'agir de fonctionnalités comme la mise en file d'attente dans l'attente de ressources disponibles, la dispense de certaines fonctions de gestion de réseau restrictives et la réservation de certaines routes/certains trajets pour les télécommunications d'urgence;

- d'assurer un établissement prioritaire/préférentiel des sessions ou appels de télécommunications d'urgence.

Les considérations propres aux technologies sont décrites dans les paragraphes qui suivent.

9.4.3.1 Accès au réseau IPCablecom

[UIT-T J.260] définit les prescriptions relatives aux télécommunications à traitement préférentiel sur les réseaux IPCablecom. [UIT-T J.261] définit le cadre permettant d'élaborer les spécifications afin de prendre en charge ces prescriptions sur les réseaux IPCablecom et IPCablecom2. Ce cadre porte sur deux domaines principaux: la priorité et l'authentification. Les autres domaines, tels que la mise en service pour la capacité de rétablissement, sont identifiés pour des révisions futures. Le cadre est défini pour inclure à la fois les aspects communs et les différences résultant des architectures utilisées dans les réseaux IPCablecom et IPCablecom2 (basés sur le sous-système IMS). Les réseaux IPCablecom et IPCablecom2 sont des réseaux en mode paquet possédant les propriétés décrites au § 6, par exemple le partage de ressources et le trafic de commande. Le cadre décrit dans [UIT-T J.261] classe les prescriptions de priorité de [UIT-T J.260] en termes de signalisation, d'étiquetage et de mécanismes.

[UIT-T J.262] définit la spécification permettant de prendre en charge les prescriptions d'authentification dans les réseaux IPCablecom. Des flux sont donnés à titre d'exemple dans [UIT-T J.262] pour indiquer les échanges de messages pour différents scénarios correspondant à l'authentification fondée sur le numéro PIN, l'utilisation de l'en-tête de priorité de ressource SIP: agent utilisateur à l'origine d'un appel VoIP vers un utilisateur du RTPC au moyen d'un numéro PIN, agent utilisateur à l'origine d'un appel VoIP vers un autre agent utilisateur VoIP au moyen d'un numéro PIN et l'authentification fondée sur l'abonnement.

[UIT-T J.263] définit la spécification permettant de prendre en charge la signalisation de priorité pour le traitement préférentiel au moyen de l'en-tête de priorité de ressource SIP [IETF RFC 4412]. Deux options sont prévues dans la spécification: 1) l'agent UA lance la demande contenant l'en-tête de priorité de ressource; 2) à partir des informations figurant dans la demande, l'en-tête de priorité de ressource, avec la valeur du niveau de priorité appropriée, est insérée par l'entité P-CSC-FE. Les valeurs de l'espace de noms et du niveau de priorité à utiliser dans différentes régions figurent dans les annexes de [UIT-T J.263]. Dans certaines régions, il est nécessaire de prendre en charge les valeurs définies dans [IETF RFC 4412]. [UIT-T J.263] décrit également les relations avec les flux de service qui sont créés pendant la mise en service de l'adaptateur multiterminal intégré (E-MTA, *embedded multi-terminal adapter*) au niveau de la couche DOCSIS MAC pour refléter les paramètres de qualité de service requis pour les télécommunications à traitement préférentiel. Aucun mécanisme d'étiquetage n'est identifié pour le transfert de données, étant donné que le protocole RTP ne prévoit pas de marquages pour indiquer la priorité. Les mécanismes d'activation de la priorité permettant de réserver des ressources et d'effectuer la commande d'admission sont pris en charge en établissant des portes dans le cadre de la qualité dynamique de service (DQoS, *dynamic quality of service*) dans les réseaux IPCablecom.

9.4.3.2 Accès au réseau xDSL

L'architecture de référence d'agrégation DSL de type Ethernet est décrite dans [BBF TR-101]. Le contrôle de la politique dans le réseau d'accès DSL est fondé sur les spécifications données dans [BBF TR-058] et [BBF TR-059].

Pour l'essentiel, la méthode permettant de fournir des fonctionnalités ETS dans un réseau d'accès DSL consiste à utiliser les fonctionnalités de qualité de service existantes pour donner la priorité aux appels ou aux sessions ETS. Le serveur de politique/point de décision de politique (PDP) est le seul dispositif "reconnaissant le service" selon cette méthode et définit la priorité appropriée à appliquer aux flux en utilisant les fonctionnalités de qualité de service existantes de la passerelle du réseau large bande (BNG).

Etant donné que par nature il n'y a pas de blocage avec le dispositif d'interface réseau (NID, *network interface device*) et le répartiteur principal (MDF, *main distribution frame*), aucune fonction ETS n'est requise dans ces éléments de réseau. La largeur de bande est mise à disposition et est fixe entre le dispositif NID et le multiplexeur de lignes d'abonnés numériques (DSLAM, *digital subscriber line access multiplexer*) et le multiplexeur DSLAM est également conçu de manière à ne pas créer de blocage. En conséquence, la méthode retenue consiste à utiliser les fonctionnalités de qualité de service de la passerelle du réseau large bande (BNG) pour contrôler les flux de données acheminés par l'intermédiaire du multiplexeur DSLAM pour veiller à ce que le trafic n'encombre pas le multiplexeur DSLAM.

La fonction d'agrégation d'Ethernet est conçue pour transporter la totalité du trafic entre la passerelle BNG et le multiplexeur DSLAM et constitue donc un autre élément non bloquant.

La passerelle d'accès de l'équipement des locaux d'abonné (CPE) peut ou non reconnaître le service ETS. Si elle reconnaît ce service, la passerelle d'accès peut donner la priorité au trafic ETS pour assurer la transmission dans le réseau d'accès DSL et pour veiller à ce que le multiplexeur DSLAM ne soit pas encombré.

Le serveur de politique/point de décision de politique (PDP) est chargé de fournir la politique appropriée pour acheminer le trafic ETS vers la passerelle BNG. Dans le cas du service ETS, le serveur de politique/point de décision de politique implémente les politiques de contrôle d'admission pour qu'un appel ou une session ETS ait de fortes chances d'aboutir. Les politiques influent sur l'établissement, le maintien et la terminaison de l'appel ou de la session ETS via le réseau d'accès DSL vers le réseau des locaux d'abonné. On suppose que le serveur de politique/point de décision de politique recevra la demande d'appel ou de session ETS en provenance du NGN (par exemple l'entité fonctionnelle proxy de contrôle de session d'appel (P-CSC-FE)). Le serveur de politique/point de décision de politique reconnaîtra la demande avec les informations ETS appropriées et chargera la passerelle BNG d'assurer comme il convient le traitement prioritaire.

La passerelle BNG est chargée d'accorder la priorité au trafic ETS. Elle applique les instructions provenant du serveur de politique/point de décision de politique lors de la réservation et de l'établissement des ressources appropriées pour le traitement d'un appel ou d'une session ETS. Elle applique un traitement prioritaire, y compris le marquage des paquets du support pour le traitement prioritaire aux fins de la transmission vers la passerelle d'accès CPE et vers le réseau régional à large bande.

9.4.3.3 Accès au réseau à fibres optiques (FTTx)

L'architecture de référence du réseau optique passif (PON, *passive optical network*) d'accès par fibres optiques est décrite dans [UIT-T G.983.1]. L'architecture de référence désigne un système de gestion de nœuds d'accès (ANMS, *access node management system*) pour le contrôle de la terminaison des lignes optiques (OLT, *optical line termination*) et de la terminaison des réseaux optiques (ONT, *optical network termination*). Le système ANMS offre la fonctionnalité du point de décision de politique qui est implémentée par les points d'application des politiques (PEP, *policy enforcement point*) situés dans les terminaux OLT et ONT.

Il n'existe actuellement aucun contrôle direct ni aucune application directe des politiques dans le réseau d'accès par fibres optiques. Toutefois, pour assurer le traitement prioritaire ETS de l'établissement d'un appel ou d'une session dans le réseau d'accès par fibres optiques, le système ANMS sera tenu de prendre en charge des fonctions dynamiques de contrôle des politiques. Pour l'essentiel, la méthode permettant de fournir des fonctionnalités ETS dans un réseau d'accès par fibres optiques consiste à utiliser les fonctionnalités de qualité de service existantes pour donner la priorité aux appels ou aux sessions ETS. Le système ANMS (par exemple le serveur de politique) est le seul dispositif "reconnaissant le service ETS" prévu dans cette méthode et définit la priorité appropriée à appliquer aux flux en utilisant les fonctionnalités de qualité de service existantes des

terminaux OLT et ONT. La politique ETS est signalisée sur l'interface Q3 (comme indiqué dans [UIT-T Q.812]) et est reflétée du terminal OLT vers le terminal ONT via l'interface de gestion et de contrôle ONT (OMCI, *ONT management and control interface*).

Le système ANMS est chargé de fournir la politique appropriée pour le trafic ETS vers le terminal OLT. Pour le service ETS, le système ANMS met en œuvre des politiques de contrôle d'admission pour qu'un appel ou une session ETS ait de fortes chances d'aboutir. Les politiques influent sur l'établissement, le maintien et la terminaison de l'appel ou de la session ETS dans le réseau d'accès par fibres optiques. Le système ANMS prend les décisions de politique finales et fournit suffisamment d'informations pour que les terminaux OLT et ONT assurent le fonctionnement du contrôle des ressources pour le service ETS. On suppose que le système ANMS recevra la demande d'appel ou de session ETS en provenance du NGN (par exemple l'entité fonctionnelle proxy de contrôle de session d'appel (P-CSC-FE)). Le système ANMS reconnaîtra la demande avec les informations ETS appropriées et chargera le terminal OLT d'assurer comme il convient le traitement prioritaire.

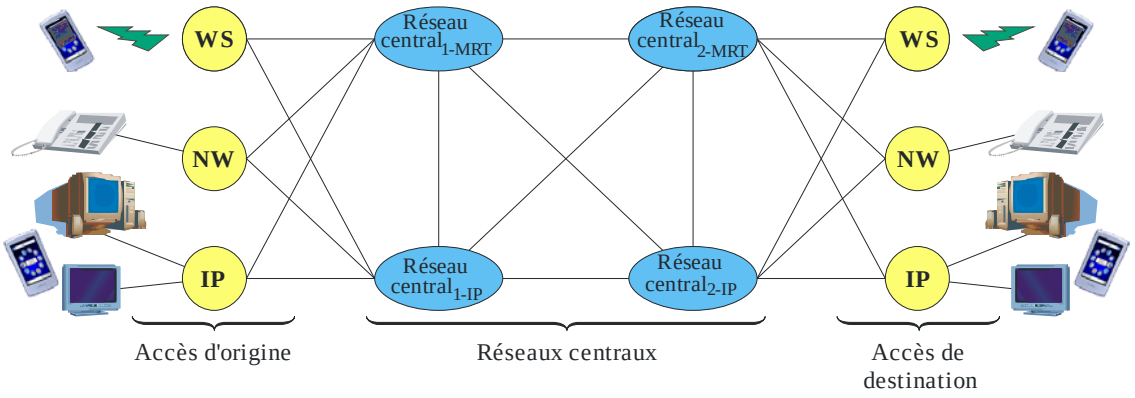
Les terminaux OLT et ONT sont conçus pour transporter la totalité du trafic ETS. Le terminal OLT est chargé d'accorder la priorité au trafic ETS. Le terminal OLT applique les instructions provenant du système ANMS lors de la réservation et de l'établissement des ressources appropriées pour le traitement d'un appel ou d'une session ETS. Il applique un traitement prioritaire, y compris le marquage des paquets de support pour le traitement prioritaire aux fins de la transmission.

10 Prise en charge de bout en bout des télécommunications d'urgence

La Figure 2 représente une matrice d'appel ou de session de bout en bout pour la prise en charge de plusieurs flux d'appels ou de sessions ETS. Elle illustre des appels ou sessions:

- de départ et d'arrivée sur le réseau IP (par exemple réseau câblé et DSL), le réseau d'accès filaire à bande étroite (par exemple le service téléphonique ordinaire) et le réseau d'accès hertzien (par exemple la téléphonie GSM et AMRC);
- transitant par les réseaux IP et les réseaux centraux à commutation de circuits (TDM, *time division multiplexing*).

Pour prendre en charge le service ETS de bout en bout, il faut assurer l'interfonctionnement des informations propres à ce service entre le domaine des technologies IP et d'autres domaines techniques (par exemple les domaines TDM hertziens ou filaires). Pour ce faire, il faut aussi assurer l'interfonctionnement pour l'appel ou la session ETS de bout en bout, qui peut recouper différents domaines technologiques (voir la Figure 2). Ainsi, les informations propres au service ETS (par exemple le marquage d'appels ETS, le niveau de priorité) doivent être signalées de part et d'autre de l'interface réseau-réseau (NNI, *network-to-network interface*) entre les fournisseurs NGN assurant l'interconnexion.



WS Accès hertzien
NW Accès filaire à bande étroite

Y.2205(11)_F02

NOTE – Un réseau central est le réseau d'authentification, un réseau de transit ou les deux.

Figure 2 – Matrice d'appel/de session de bout en bout

Les scénarios d'appel ou de session associés à la Figure 2 sont présentés dans [b-ATIS-10000010]. [b-ATIS-10000010] définit les procédures et les fonctionnalités requises pour prendre en charge le service ETS dans et entre les réseaux du fournisseur de services IP. Les scénarios d'appel ou de session suivants sont possibles sur la base de la matrice indiquée sur la Figure 2:

– Accès d'origine vers le réseau central 1
  - Accès filaire d'origine vers le réseau central IP
  - Accès hertzien d'origine vers le réseau central IP
  - Accès IP d'origine vers le réseau central IP
  - Accès IP d'origine vers le réseau central TDM

– Réseau central 1 vers réseau central 2
  - réseau central TDM vers réseau central IP
  - réseau central IP vers réseau central TDM
  - réseau central IP 1 vers réseau central IP 2

– Réseau central 2 vers accès de destination
  - réseau central IP vers accès de destination filaire
  - réseau central IP vers accès de destination hertzien
  - réseau central IP vers accès de destination IP
  - réseau central TDM vers accès de destination IP.

Pour établir l'appel ou la session ETS, il faut implémenter avec soin les protocoles de signalisation nécessaires qui transmettent les informations requises pour signaler le caractère critique du service ETS. Pour assurer le traitement prioritaire de bout en bout, il est important de prendre en charge la mise en correspondance des informations prioritaires afin de faciliter l'interfonctionnement transparent des protocoles entre les différents protocoles utilisés dans un réseau (par exemple l'interfonctionnement vertical des protocoles entre le contrôle d'appel ou de session et le contrôle de support) ou entre différents types de réseaux (par exemple l'interfonctionnement du contrôle d'appel ou de session entre deux réseaux), y compris le RTPC. De même, il est indispensable de permettre la mise en correspondance des informations prioritaires pour faciliter l'interfonctionnement transparent entre les différents types de transport, c'est-à-dire les types de médias. Sans cet interfonctionnement/cette mise en correspondance, le traitement prioritaire de bout en bout ne pourra peut-être pas être assuré.

L'UIT-T élabore actuellement des indications relatives à la mise en correspondance des attributs du protocole de signalisation requis (informations prioritaires ETS) pour prendre en charge l'établissement et l'admission appropriés du service ETS pour diverses configurations "horizontales" (par exemple ISUP, SIP, UIT-T H.225.0) et "verticales" (par exemple UIT-T H.248.0, Diameter).

[UIT-T Q-Sup.57] présente les prescriptions de signalisation permettant de prendre en charge des fonctionnalités de traitement préférentiel dans des réseaux IP pour le service ETS. On trouvera dans l'Appendice III un exemple de flux d'appel tiré de [UIT-T Q-Sup.57] qui illustre l'authentification et l'établissement réussis d'un appel ou d'une session ETS.

11 Mécanismes et capacités pour la prise en charge de certains aspects de l'alerte avancée dans les NGN

11.1 Généralités

Les systèmes d'alerte avancée peuvent être classés en deux catégories: à distribution sélective ou à extraction sélective.

Dans le modèle de distribution sélective, les participants enregistrent leurs informations de contact (par exemple, une adresse de courrier électronique) auprès d'un service central. Lorsqu'un événement se produit, ces participants enregistrés sont alertés de l'événement, des pointeurs complémentaires pouvant les orienter vers d'autres informations. L'architecture de ce modèle repose essentiellement sur une autorité centrale qui détermine si des informations doivent être diffusées et ce que ces informations entraînent. La force de ce modèle réside dans le fait qu'il prend en charge activement la surveillance des événements, ce qui permet aux utilisateurs de poursuivre normalement leurs tâches et de rester passifs concernant la surveillance des catastrophes ou urgences potentielles.

Le modèle de distribution sélective représente un mécanisme de distribution point à multipoint et il est implémenté au niveau de la strate des services et de la strate de transport (par exemple, multidiffusion).

Contrairement au modèle de distribution sélective, le modèle d'extraction sélective repose sur un échange d'informations de type interrogation-réponse. Dans les deux modèles, les participants doivent s'enregistrer individuellement, mais dans le modèle d'extraction sélective, ce sont les utilisateurs individuels qui sont chargés de la surveillance et de l'obtention des informations. L'avantage de ce système est que les informations ne sont fournies qu'en fonction des besoins ou qu'à la demande.

Succinctement, les systèmes d'alerte utilisent les applications existantes et les capacités sous-jacentes se trouvant dans les réseaux IP. L'ajout d'une distribution sélective ou d'une extraction sélective permet d'adapter ces systèmes aux besoins et attentes des utilisateurs. Les applications de chaque type de système d'alerte peuvent aussi être utilisées parallèlement: le modèle de distribution sélective peut assurer une surveillance et une notification automatiques périodiques et le modèle d'extraction sélective peut être utilisé pour obtenir des informations spécifiques à la demande.

On trouvera des exemples de distribution sélective et d'extraction sélective à l'Appendice II.

11.2 Protocole d'alerte commun

Le présent paragraphe décrit le protocole d'alerte commun (CAP, *common alerting protocol*) spécifié dans [UIT-T X.1303], qui peut être utilisé pour prendre en charge des applications d'alerte avancée. Le protocole CAP utilise le langage de balisage extensible (XML, *extensible markup language*) et fournit des formats d'échange de données types.

[UIT-T X.1303] spécifie un format général pour échanger, sur tout type de réseau, des alertes d'urgence pour tous les risques et des alertes destinées au public. Le protocole CAP permet de

diffuser simultanément un message d'alerte cohérent sur un grand nombre de systèmes d'alerte différents, ce qui augmente l'efficacité de l'alerte tout en simplifiant la tâche d'alerte. Le protocole CAP facilite aussi la détection de scénarios émergents dans les alertes locales de divers types, pouvant par exemple indiquer un acte hostile ou un danger non détecté. Le protocole CAP définit aussi un gabarit pour que les messages d'alerte soient efficaces, basé sur les bonnes pratiques identifiées lors de travaux de recherche universitaires et lors d'expériences menées en grandeur nature.

Le protocole CAP définit un format de message non propriétaire ouvert pour tous les types d'alertes et de notifications. Il ne se rapporte ni à une application ni à une méthode de télécommunication particulière. Le format CAP est compatible avec les nouvelles techniques, par exemple les services web et les services web rapides de l'UIT-T, ainsi qu'avec les formats existants, dont le format SAME (*specific area message encoding*) utilisé pour les radiocommunications météorologiques de la National Oceanic and Atmospheric Administration (NOAA) aux Etats-Unis d'Amérique et le système d'alerte en cas d'urgence (EAS, *emergency alert system*), tout en offrant des capacités améliorées, notamment:

- ciblage géographique souple grâce à des modèles de latitude/longitude et à d'autres représentations géospatiales en trois dimensions;
- messagerie multilingue et multidestinataires;
- heures effectives et expirations en phase ou différées;
- fonctionnalités améliorées de mise à jour et d'annulation de message;
- prise en charge d'un gabarit permettant d'élaborer des messages d'alerte complets et efficaces;
- compatibilité avec la capacité de chiffrement et de signature numériques; et
- prise en charge d'images et de signaux audionumériques.

Le protocole CAP permet de réduire les coûts et la complexité de fonctionnement du fait qu'il n'est pas nécessaire d'avoir de multiples interfaces logicielles personnalisées avec les nombreuses sources d'alerte et les nombreux systèmes de diffusion des alertes pour tous les risques. Des conversions étant possibles entre le format de message CAP et les formats "natifs" de tous les types de technologies de détection et d'alerte, le format de message CAP peut servir de base à un "internet d'alerte" national et international indépendant de la technologie.

Le protocole CAP spécifié dans [UIT-T X.1303] est techniquement équivalent au protocole d'alerte commun V1.1 d'OASIS et est compatible avec ce protocole. OASIS a également défini le protocole CAP V1.2, qui est une mise à jour du protocole CAP V1.1.

[UIT-T X.1303] contient une spécification ASN.1 équivalente permettant un codage binaire compact et l'utilisation d'outils ASN.1 et XSD pour produire et traiter les messages CAP. Cette Recommandation permet aux systèmes existants, par exemple les systèmes UIT-T H.323, de coder, transporter et décoder plus facilement les messages CAP.

11.3 Procédures applicables à l'enregistrement d'arcs d'identificateur d'objet en matière d'alerte

[UIT-T X.674] (Procédures applicables à l'enregistrement d'arcs d'identificateur d'objet en matière d'alerte) traite de l'enregistrement d'arcs d'identificateur d'objet (OID, *object identifier*) permettant d'identifier différents types d'alertes et de centres d'alerte. Elle indique plus particulièrement les procédures à suivre pour l'enregistrement d'arcs permettant d'identifier (tous types d') des alertes et des centres d'alertes sous l'arc d'identificateur d'objet d'alerte {joint-iso-itu-t(2)alerting(49)} conformément à [UIT-T X.660].

[UIT-T X.674] facilite l'attribution et l'utilisation d'identificateurs OID pour identifier les centres d'alerte (par exemple ceux désignés par les Etats Membres de l'Organisation météorologique mondiale (OMM)).

NOTE – L'OMM tient un Registre des autorités compétentes en matière d'alerte, accessible à l'adresse: http://www-db.wmo.int/alerting/authorities.html.

12 Priorité de rétablissement de service

En cas de défaillance ou d'interruption du réseau, les services critiques (par exemple, les services d'urgence) peuvent être interrompus et devront peut-être pouvoir être rétablis avec une plus grande probabilité que les autres services. [UIT-T Y.2172] définit trois niveaux de priorité de rétablissement des services dans les NGN. Elle permet d'utiliser ces catégories de priorité dans les messages de signalisation de sorte qu'un appel ou une session correspondant au service considéré puisse être établi avec la priorité de rétablissement souhaitée, permettant ainsi aux services critiques de pouvoir être rétablis avec une plus grande probabilité que les autres services.

13 Commutation de protection et rétablissement

13.1 Considérations générales

Divers concepts généraux communs à de nombreuses techniques de transport sont décrits dans [UIT-T G.808.1]. Plusieurs questions importantes à prendre en compte pour assurer la protection du trafic de télécommunications d'urgence sont identifiées dans [UIT-T G.808.1].

13.1.1 Protection individuelle

Le concept de protection individuelle s'applique aux situations où il est utile de protéger seulement une partie des signaux de trafic, qui nécessitent un niveau élevé de fiabilité.

13.1.2 Protection de groupe

Une commutation de protection rapide est obtenue par le traitement d'un faisceau logique d'entités de transport comme une seule entité après le commencement des actions de protection.

13.1.3 Types d'architectures

Les types d'architectures suivants sont identifiés dans [UIT-T G.808.1] et sont récapitulés ci-après.

13.1.3.1 Architecture de protection 1+1 (doublée)

Dans le type d'architecture 1+1, une entité de transport en protection est spécialisée comme ressource de secours offerte à l'entité de transport en service.

13.1.3.2 Architecture de protection 1:n (partagée)

Dans le type d'architecture en 1:n, une entité de transport en protection spécialisée est une ressource de secours partagée entre n entités de transport en service.

13.1.3.3 Architecture de protection m:n (multipartagée)

Dans le type d'architecture en m:n, m entités de transport en protection spécialisées se partagent des ressources de secours pour n entités de transport en service, avec normalement $m \leq n$.

13.1.4 Types de commutation

La commutation de protection peut être de l'un des deux types suivants: unidirectionnelle ou bidirectionnelle.

Il convient de noter que tous les types de commutation, sauf la commutation 1+1 unidirectionnelle, nécessitent un canal de communication entre les deux extrémités du domaine protégé; ce canal est appelé canal de commutation automatique de protection (APS, *automatic protection switching*).

Une liste des avantages et inconvénients de l'application de ces types de commutation à tous les cas ci-dessus est reproduite dans [UIT-T G.808.1].

Dans le contexte des télécommunications d'urgence basées sur les réseaux IP, il peut être indiqué d'utiliser la commutation unidirectionnelle, car en général, les trajets dans chaque sens ne sont pas directement associés en raison de la nature unidirectionnelle des trajets/de l'acheminement via les réseaux IP.

13.1.5 Types de fonctionnement

Le fonctionnement en protection peut être de type irréversible ou réversible.

En fonctionnement réversible, le signal de trafic (service) revient toujours à l'entité de transport en service (ou y reste toujours) lorsque l'entité de transport en service s'est rétablie après le défaut.

En fonctionnement irréversible, le signal de trafic (service) ne revient pas à l'entité de transport en service.

Il est indiqué dans [UIT-T G.873.1] que la protection doublée est souvent préconfigurée comme étant irréversible car cette protection est de toute façon entièrement spécialisée: cela évitera l'envoi d'une seconde alerte de "panne aléatoire" du trafic. Il peut, cependant, y avoir des raisons de préconfigurer la protection comme étant réversible (par exemple, de façon que le trafic utilise le sens "court" autour d'un anneau sauf en conditions de défaillance. Certaines politiques d'opérateur imposent également la commutation réversible même en protection doublée.)

13.2 Architectures de protection des réseaux SDH

[UIT-T G.841] fournit les spécifications au niveau équipement qui sont nécessaires pour l'implémentation des différentes options d'architecture de protection de réseaux utilisant la hiérarchie numérique synchrone (SDH, *synchronous digital hierarchy*).

Les entités protégées peuvent être une section de multiplexage SDH unique (par exemple, pour une protection linéaire d'une section de multiplexage), une partie d'un conduit SDH unique de bout en bout (par exemple, pour une protection de connexion de sous-réseau), ou la totalité d'un conduit SDH de bout en bout (par exemple, pour une protection linéaire d'un chemin de conduit de conteneur virtuel de niveau supérieur ou inférieur). Les réalisations physiques de ces architectures de protection peuvent englober des anneaux ou des chaînes linéaires de nœuds. Chaque classification de la protection contient des directives générales concernant les objectifs réseau, l'architecture, les fonctionnalités d'application, les critères de commutation, les protocoles et les algorithmes.

En outre, [UIT-T G.842] contient les spécifications d'interfonctionnement des architectures de protection de réseau. Elle traite en particulier de l'interconnexion à un seul nœud et à deux nœuds entre anneaux de protection partagée de section(s) de multiplexage (MS) et anneaux de protection de connexion de sous-réseau (SNCP, *subnetwork connection protection*) de même type ou de types différents.

13.3 Réseau de transport optique

[UIT-T G.873.1] définit le protocole de commutation de protection automatique (APS, *automatic protection switching*) et l'opération de commutation de protection pour les systèmes de protection linéaire du réseau de transport optique au niveau des unités de données de canal optique (ODUk).

Les systèmes de protection examinés dans [UIT-T G.873.1] sont les suivants:

– protection de connexion de sous-réseau par unité ODUk avec surveillance intrinsèque (1+1, 1:n);

– protection de connexion de sous-réseau par unité ODUk avec surveillance non intrusive (1+1);

– protection de connexion de sous-réseau par unité ODUk avec surveillance de sous-couche (1+1, 1:n).

Dans un certain sens de transmission, la "tête de réseau" du signal protégé est capable de remplir une fonction de dérivation, qui placera une copie d'un signal de trafic normal dans une entité de protection lorsque requis. "L'extrémité distante" remplira une fonction de sélecteur si elle est capable de choisir un signal de trafic normal soit dans son entité de trafic habituelle, ou dans une entité de protection. En transmission dans les deux sens, où les deux sens de transmission sont protégés, les deux extrémités du signal protégé rempliront normalement les deux fonctions de dérivateur et de sélecteur.

13.4 Commutation de protection linéaire Ethernet

[UIT-T G.8031] décrit en détail la commutation de protection des signaux VLAN Ethernet, notamment en ce qui concerne les caractéristiques et les architectures de protection du réseau de couche Ethernet (ETH) et le protocole APS.

Les architectures de commutation de protection 1+1 et 1:1 linéaires à commutation unidirectionnelle ou bidirectionnelle sont définies dans [UIT-T G.8031].

Dans une architecture de commutation de protection 1+1 linéaire, une entité de transport de protection est attribuée à chaque entité de transport de service. Le trafic normal est copié et alimente l'entité de transport de service et l'entité de transport de protection par le biais d'un pont permanent situé à la source du domaine protégé. Le trafic transitant sur ces deux entités est transmis simultanément au puits du domaine protégé, où une sélection est faite sur la base de certains critères prédéterminés, tels qu'une indication de défaut de serveur.

Bien que la sélection se fasse uniquement au puits du domaine protégé dans l'architecture de commutation de protection 1+1 linéaire, la commutation de protection 1+1 bidirectionnelle requiert le protocole de coordination APS de telle sorte que les sélecteurs sélectionnent la même entité dans les deux sens. Par contre, la commutation de protection 1+1 unidirectionnelle ne requiert pas ce protocole.

Dans l'architecture de commutation de protection 1:1 linéaire, l'entité de transport de protection est associée à l'entité de transport de service. Toutefois, le trafic normal est acheminé dans l'entité de transport de service ou dans l'entité de transport de protection à l'aide d'un pont sélecteur situé à la source du domaine protégé. Le sélecteur situé au puits du domaine protégé sélectionne l'entité qui achemine le trafic normal. Le protocole de coordination APS est nécessaire car la source et le puits doivent être coordonnés pour que le point sélecteur à la source et le sélecteur au puits sélectionnent la même entité.

13.5 Commutation de protection linéaire Ethernet

[UIT-T G.8032] définit le protocole de protection automatique (APS) et les mécanismes de commutation de protection concernant les topologies en anneau Ethernet de la couche ETH. On y trouve des précisions sur les caractéristiques de protection des anneaux Ethernet, les architectures et le protocole APS en anneau.

Le protocole de protection défini dans [UIT-T G.8032] permet d'assurer une connectivité protégée point à point, point à multipoint et multipoint à multipoint à l'intérieur de l'anneau ou des anneaux interconnectés, que l'on appelle topologie de "réseau multi-anneaux/échelles".

13.6 Commutation de protection linéaire pour les réseaux MPLS de transport (T-MPLS)

[UIT-T G.8131] donne les spécifications et les mécanismes applicables à la commutation de protection de connexion de sous-réseau (SNC) et de chemin de bout en bout en ce qui concerne les réseaux MPLS de transport (T-MPLS). Elle décrit les types d'architecture de protection de chemin et de protection de connexion SNC, les types de commutation uni et bidirectionnelle, les types de fonctionnement réversible et irréversible. Elle définit le protocole de commutation automatique de protection utilisé pour aligner les deux extrémités du domaine protégé.

[UIT-T G.8131] définit l'architecture 1+1 et l'architecture 1:1. La première fonctionne avec une commutation unidirectionnelle et la seconde avec une commutation bidirectionnelle.

13.7 Commutation de protection APM

[UIT-T I.630] définit les architectures et les mécanismes de commutation de protection au niveau de la couche ATM. Cette architecture est définie par l'étendue et la configuration du domaine protégé. Les ressources de protection sont attribuées à l'avance. Le mécanisme de protection fait intervenir des déclencheurs, des mécanismes de blocage et le protocole de commande de la commutation de protection.

[UIT-T I.630] décrit la protection de VP/VC individuelle et de groupe. La protection de VP/VC individuelle est une technique permettant d'utiliser une seule connexion de réseau ou de sous-réseau pour l'entité active et l'entité de protection. La protection de groupe est une technique avec laquelle un faisceau logique d'une ou plusieurs connexions de réseau ou de sous-réseau est utilisé pour l'entité active et l'entité de protection.

A l'heure actuelle, [UIT-T I.630] décrit la commutation de protection bidirectionnelle 1+1 et 1:1 ainsi que la commutation de protection unidirectionnelle 1+1.

13.8 Commutation de protection pour les réseaux MPLS

[UIT-T Y.1720] indique les prescriptions et les mécanismes relatifs aux fonctionnalités de commutation de protection doublée (1+1), alternée (1:1), partagée entre mailles et 1+1 en mode paquet dans le plan utilisateur pour les réseaux de couche à commutation multiprotocole avec étiquette (MPLS). Le mécanisme défini ici est conçu pour la prise en charge de chemins commutés avec étiquettes (LSP, *label switched path*) point à point de bout en bout.

[UIT-T Y.1720], qui vise à définir les techniques de commutation de protection, explique comme suit la différence entre commutation de protection et reroutage:

- Commutation de protection: cette forme de commutation suppose que le routage soit déterminé d'avance et que les ressources soient préalablement attribuées à un conduit LSP de protection spécialisé avant que la défaillance se produise. La commutation de protection offre donc une bonne assurance que les ressources de réseau voulues pourront être récupérées après la défaillance.
- Reroutage: le reroutage suppose qu'aucun conduit LSP de protection spécialisé ne soit défini et donc que le routage ne soit pas déterminé d'avance et que les ressources ne soient pas non plus attribuées avant que la défaillance se produise. Le reroutage est communément utilisé dans des situations mettant en œuvre des fonctions de routage et de signalisation et dans lesquelles toute "demande de rétablissement de la connexion" soumise à la suite de la défaillance (à l'instigation du réseau ou de l'utilisateur) sera comparée à d'autres types de demande de trafic analogues aux fins de l'obtention de la ressource voulue. Le reroutage n'offre donc aucune garantie que les ressources de réseau voulues pourront être récupérées après la défaillance; en outre, le reroutage est généralement plus lent que la commutation de protection.

La commutation de protection, qui est nécessaire pour assurer un retour rapide à l'exploitation normale après une défaillance, améliore du même coup la fiabilité et la disponibilité de fonctionnement des réseaux MPLS.

La commutation de protection doit répondre aux caractéristiques suivantes:

1) elle doit être appliquée sur toute la longueur d'un conduit LSP;

2) elle doit assurer la protection entre "défaillances du signal" (signaux SF) et "requêtes de commutation manuelle";

3) elle doit permettre d'assurer une protection au niveau de la couche MPLS le plus rapidement possible (sous réserve de la résolution temporelle du mécanisme de détection des dérangements);

4) elle doit offrir un coefficient de protection de 100%, de telle sorte que 100% du trafic actif dégradé soit protégé contre une panne affectant un conduit LSP en service;

5) elle doit permettre, lorsque cela est possible, la prise en charge d'une capacité de trafic supplémentaire.

Appendice I

Catégories de télécommunications d'urgence

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

I.1 Télécommunications d'urgence d'individu à autorité

Une télécommunication d'urgence d'individu à autorité est lancée par un individu utilisant les capacités de télécommunications d'urgence nationales ordinaires pour demander une assistance urgente lors d'une urgence individuelle (personnelle), voire lors d'une situation d'urgence restreinte. Par exemple, certains numéros courts (112, 911, etc.) permettent à un utilisateur individuel de se raccorder à un centre de réponse d'urgence. Le centre envoie alors les intervenants nécessaires (par exemple, police, pompiers, ambulance) au nom de l'appelant. Des informations complémentaires peuvent être signalées automatiquement au centre d'appel, par exemple l'emplacement de l'appelant. Ces informations peuvent permettre de réagir encore plus rapidement car il arrive que les appelants ne puissent pas ou n'aient pas le temps ou la possibilité de fournir eux-mêmes ces informations. Ce type de communication est généralement une communication point à point dans laquelle l'appelant interagit essentiellement avec l'agence de destination. La grande majorité de ces télécommunications concernent des urgences à petite échelle (par exemple, l'incendie d'une maison individuelle) résultant d'événements qui sont pour la plupart non corrélés même si des événements à grande échelle (par exemple, un tremblement de terre) peuvent donner lieu à de nombreuses communications corrélées simultanées. (Le terme individu est pris dans une acception large et désigne toute personne ayant besoin d'une assistance urgente (par exemple, des citoyens, des visiteurs ou d'autres habitants d'un endroit particulier).) Pour les communications entre les personnes qui participent à des télécommunications d'urgence, plusieurs types de média peuvent être utilisés (téléphonie, vidéo, texte en temps réel, messagerie instantanée, etc.).

I.2 Télécommunications d'urgence entre individus

Une télécommunication d'urgence entre individus est lancée par une personne ou un dispositif du grand public ou d'une organisation. Par exemple, pendant et immédiatement après des situations d'urgence, les individus ont fortement envie de communiquer entre eux. Il existe donc une forte demande de télécommunications entre individus alors même que les ressources de télécommunication peuvent être réduites en raison des dommages causés par les situations d'urgence. Tous ces facteurs font que les réseaux de télécommunication peuvent être encombrés.

I.3 Télécommunications d'urgence entre autorités

Une télécommunication d'urgence entre autorités est généralement une communication lancée par un utilisateur autorisé des télécommunications d'urgence (ou son organisation) à destination d'un autre utilisateur autorisé pour:

1) faciliter les opérations de rétablissement urgent (par exemple, en créant des centres de gestion des urgences et des centres administratifs associés pour que les pouvoirs publics ou d'autres organisations puissent apporter une assistance);
2) rétablir une infrastructure communautaire de base (par exemple rétablir l'eau, l'électricité, etc.); et
3) prendre des mesures pour permettre un rétablissement complet à long terme (par exemple, reconstruction de routes, ponts, bâtiments, etc.).

Traditionnellement, les télécommunications d'urgence entre autorités (parfois appelées télécommunications de sécurité du public) utilisant des réseaux publics ont lieu alors même que les ressources de télécommunications sont encombrées en raison de l'augmentation des télécommunications entre individus.

Etant donné que les télécommunications d'urgence entre autorités peuvent contribuer pour beaucoup à faciliter le retour à un état de normalité et à éviter d'autres risques pour les personnes ou les biens, on peut accorder un statut prioritaire à cette catégorie de télécommunications d'urgence par rapport aux autres catégories de télécommunications d'urgence lorsque des urgences sont déclarées ou lorsqu'elles s'intensifient.

I.4 Télécommunications d'urgence d'autorité à individu

Enfin, les télécommunications d'urgence d'autorité à individu (parfois classées dans la catégorie des systèmes d'alerte avancée) concernent généralement des informations provenant d'une source autorisée et destinées au grand public. Il peut s'agir d'informations destinées à une communauté touchée par une catastrophe (par exemple, des instructions de sécurité, des lignes directrices, des conseils, etc.). Une télécommunication particulière est généralement lancée par un utilisateur autorisé à destination de nombreux individus.

Point quelconque à point quelconque: exemple de service ETS à partir d'un emplacement/dispositif quelconque, contactant un autre utilisateur quelconque (ETS ou grand public), une prise en charge prioritaire étant assurée par l'infrastructure des communications. Le service GETS dans le RTPC est un bon exemple, le service prioritaire n'étant pas ubiquitaire et n'étant pas limité à un ensemble sélectif de destinations ou de dispositifs terminaux.

Point à point: dans le contexte des télécommunications d'urgence, cette relation point à point est considérée comme un cas particulier de relation point quelconque à point quelconque. Dans ce cas, les participants sont limités à deux utilisateurs ETS quelconques.

Multipoint à point: ce modèle est par exemple réalisé sous la forme d'une architecture client-serveur du web, dans laquelle un utilisateur quelconque accède à un seul emplacement bien connu pour obtenir des informations. Dans le RTPC, ce modèle est réalisé sous la forme de systèmes 911, 112, etc., dans lesquels les sessions d'une région sont transmises à un seul point de réponse de sécurité publique (PSAP, *public safety answering point*).

Point à multipoint: dans ce modèle, les informations sont envoyées d'une seule source à un ensemble de destinations (utilisateurs finals) choisissant de participer à la diffusion des données. Dans le cas de la radiodiffusion média, la télévision et la radio sont d'excellents exemples étant donné que les destinataires obtiennent uniquement les informations fournies sur le canal qu'ils ont choisi. Dans le modèle de communication de données, on fait la distinction entre la relation point à multipoint et la radiodiffusion car cette dernière implique que tous les nœuds reçoivent le message, qu'ils le choisissent ou non, tandis que la première implique l'appartenance directe à un groupe.

Appendice II

Exemples de scénarios pour les systèmes d'alerte avancée

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

II.1 Modèle de distribution sélective

Le secteur privé et le secteur public offrent tous deux des systèmes d'alerte basés sur le modèle de distribution sélective. Cela étant, la présente Recommandation ne décrit qu'un exemple de modèle de distribution sélective dans le secteur public, à savoir le centre d'informations d'urgence de l'administration locale de Washington D.C. (http://alert.dc.gov/eic/site/default.asp). Les utilisateurs enregistrent leurs informations de contact sous la forme d'une adresse de courrier électronique, d'un pageur ou d'un numéro de téléphone mobile (messagerie textuelle ou messagerie vocale automatique). La messagerie vocale automatique est équivalente au système 911 inversé et tous les citoyens du District de Columbia sont directement enregistrés pour ce service par le biais du commutateur filaire correspondant. En ce qui concerne les adresses de courrier électronique et les pageurs, le service d'alerte n'est pas limité qu'aux résidents de Washington D.C.

II.2 Modèle d'extraction sélective

Le meilleur exemple de modèle d'extraction sélective fonctionnant sur l'Internet est le système I-AM-Alive au Japon (http://www.isoc.org/inet2000/cdproceedings/8l/8l_3.htm, http://www.iaa-alliance.net/en/). Ce système a vu le jour à la suite du tremblement de terre de Kobe en 1995 afin de permettre à la population de déterminer la situation et l'emplacement possible de leurs êtres chers affectés par le tremblement de terre. Il s'agit d'un centre de collecte d'informations permettant aux premiers intervenants de déposer les informations qu'ils ont découvertes. Il s'agit également d'un centre de distribution permettant aux amis et proches de déterminer si des connaissances ont été blessées dans une catastrophe.

Le système I-AM-Alive stocke les informations que les individus et/ou les premiers intervenants fournissent par fax, par téléphone ou sur le web. Ces informations sont ensuite distribuées essentiellement sous la forme de pages web, mais certaines informations peuvent être obtenues à partir de numéros de téléphone connus associés au système.

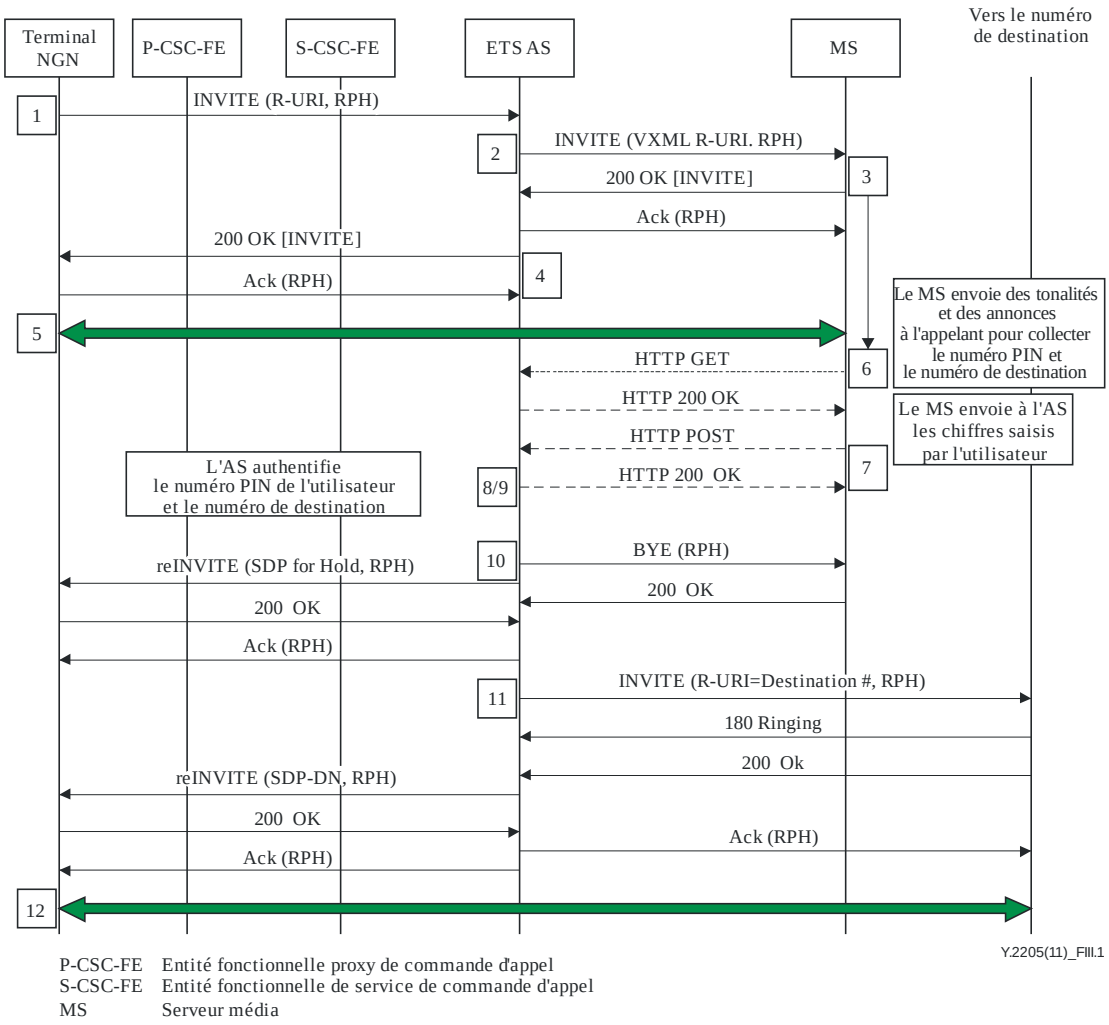
Appendice III

Exemple de flux d'appel/de session pour les NGN

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

Le présent appendice donne un exemple de flux d'appel ou de session ETS tiré de [UIT-T Q.Sup.57] qui est applicable aux NGN. Ce flux d'appel illustre l'établissement réussi d'un d'appel ou d'une session ETS lorsque l'authentification et l'autorisation de l'utilisateur utilisent un numéro PIN.

La Figure III.1 illustre une méthode d'authentification d'utilisateur ETS qui utilise un numéro PIN introduit par l'utilisateur dans un réseau IP. Un serveur de média (MS) est une combinaison d'entité fonctionnelle de contrôle des ressources média/d'entité fonctionnelle de traitement des ressources média (MRC-FE/MRP-FE). Toutes les demandes SIP comprennent un en-tête de priorité de ressource (RPH) [IETF RFC 4412] pour indiquer qu'un traitement prioritaire est requis.



P-CSC-FE Entité fonctionnelle proxy de commande d'appel
S-CSC-FE Entité fonctionnelle de service de commande d'appel
MS Serveur média

Figure III.1 – Etablissement d'un appel ou d'une session ETS au moyen de l'authentification reposant sur un numéro PIN

1) L'appel ou la session est acheminé vers un serveur d'application (AS) ETS, qui lance le processus d'authentification de l'utilisateur.

2) Le serveur d'application ETS envoie un message INVITE au serveur de média (MS) choisi, avec une offre SDP associée à l'appelant. Le message INVITE contient l'URL d'un script VoiceXML, stocké dans le serveur d'application ETS. Le script décrit comment le serveur de média doit interagir avec l'appelant (quelle annonce envoyer, comment collecter les chiffres, le nombre de chiffres à collecter, les temporisations entre les chiffres, etc.).

3) Dès qu'il reçoit le message INVITE, le serveur de média:

- peut envoyer un message 100 Trying au serveur d'application ETS;
- récupère le script VoiceXML directement auprès du serveur d'application ETS en utilisant HTTP et l'URL contenue dans le message INVITE (Le serveur de média envoie un message HTTP GET au serveur d'application et le script VoiceXML est retourné par le serveur d'application ETS dans un message HTTP 200 OK.);
- valide le script;
- formule et envoie un message 200 OK contenant son propre élément SDP au serveur d'application ETS.

4) Le serveur d'application ETS envoie un message 200 OK à l'appelant (terminal NGN), contenant les informations de session qu'il a reçues du serveur de média.

5) A ce stade, la connexion de média est disponible entre le serveur de média et l'appelant.

6) Dès qu'il reçoit l'accusé de réception et le script VXML dans le message HTTP 200 OK, le serveur de média exécute le script VoiceXML. Il envoie une tonalité et collecte les chiffres (numéro PIN) saisis par l'appelant.

7) Le serveur de média envoie ensuite les chiffres collectés directement au serveur d'application ETS en utilisant un message HTTP POST.

8) Dès qu'il reçoit les chiffres collectés, le serveur d'application ETS vérifie si les chiffres reçus (numéro PIN) sont valides.

- Si les chiffres reçus ne sont pas valides (nombre de chiffres reçus ou numéro erroné), le serveur d'application ETS détermine qu'une nouvelle interaction avec l'appelant est nécessaire. Le serveur d'application ETS retourne un message HTTP 200 OK au serveur de média MS avec un nouveau script VoiceXML. Le serveur d'application ETS donne des instructions pour le traitement final.
- Si les chiffres reçus sont valides, le serveur d'application ETS charge le serveur de média d'envoyer l'annonce pour collecter les chiffres (numéro de destination).

9) Le serveur d'application ETS détermine que les chiffres du numéro de destination saisis par l'appelant sont valides.

10) Le serveur d'application ETS libère le serveur de média de l'appel ou de la session avec un message SIP BYE et envoie un message reINVITE à l'appelant, avec un élément SDP pour mettre en attente le média.

11) Le serveur d'application ETS envoie un message INVITE à la partie de destination. Dès qu'il reçoit le message 200 OK (réponse), le serveur d'application ETS envoie à l'appelant un message reINVITE avec l'élément SDP associé à la destination.

12) Un trajet de média est établi entre l'appelant et le numéro de destination, le trajet de la commande d'appel passant par le serveur d'application ETS d'authentification.

Bibliographie

[b-UIT-T Q-Sup.62] Recommandations UIT-T de la série Q – Supplément 62 (2011), *Aperçu des travaux des organisations de normalisation et d'autres organisations sur le service de télécommunications d'urgence*.

[b-UN Global Survey] Stratégie internationale des Nations Unies pour la prévention des catastrophes (2006), Rapport final portant sur une "*Etude mondiale des systèmes d'alerte avancée*". <http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf>

[b-ATIS 1000010] ATIS-1000010.2006, *Support of Emergency Telecommunications Service (ETS) in IP Networks*.

[b-IEEE 802.11] IEEE Std 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between system – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IEEE 802.16] IEEE Std 802.16-2009, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems*.

[b-IEEE 802.16m] IEEE Std 802.16m-2011, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems, Amendment 3: Advanced Air Interface*.

[b-IEEE 802.1p] IEEE Std 802.1D-2004, *IEEE Standard for Local and metropolitan area networks; Media Access Control (MAC) Bridges*.

[b-3GPP TR 23.854] 3GPP TR 23.854 (en vigueur), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancements for Multimedia Priority Service (Release 10)*.

[b-3GPP TS 22.153] 3GPP TS 22.153 (06/2008), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia priority service (Release 8)*.

[b-3GPP TS 23.203] 3GPP TS 23.203 (en vigueur), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture (Release 10)*.

[b-3GPP TS 23.272] 3GPP TS 23.272 (en vigueur), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Circuit Switched (CS) Fallback in Evolved Packet System (EPS); Stage 2 (Release 10)*.

[b-3GPP TS 23.328] 3GPP TS 23.228 (en vigueur), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 10)*.

[b-3GPP TS 23.401] 3GPP TS 23.401 (en vigueur), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 10)*.

[b-3GPP TS 29.212] 3GPP TS 29.212, version 9 6.1 (2011-04), *Universal Mobile Telecommunications System (UMTS);* LTE; *Policy and Charging Control over Gx reference point (Release 9).*

[b-3GPP TS 29.214] 3GPP TS 29.214 (en vigueur), *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point (Release 10).*

[b-3GPP TS 29.229] 3GPP TS 29.229, version 9.3.0 (2010-10), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 9).*

[b-3GPP TS 29.329] 3GPP TS 29.329 v9.4.0 (2011-01), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (Release 9).*

[b-3GPP2 S.R0117-0] 3GPP2 S.R0117-0-v1.0 (06/2006), *3rd Generation Partnership Project 2; Multimedia Priority Service (MMPS) for MMD-based Networks – Stage 1 Requirements*.

[b-IETF RFC 2750] IETF RFC 2750 (2000), *RSVP Extensions for Policy Control*.

[b-IETF RFC 3265] IETF RFC 3265 (2002), *Session Initiation Protocol (SIP) – Specific Event Notification*.

[b-IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP).*

[b-IETF RFC 3936] IETF RFC 3936 (2004), *Procedures for Modifying the Resource reSerVation Protocol (RSVP).*

[b-IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.

[b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony*.

[b-IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction*.

[b-IETF RFC 4495] IETF RFC 4495 (2006), *A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow*.

[b-IETF RFC 4916] IETF RFC 4916 (2007), *Connected Identity in Session Initiation Protocol (SIP).*

[b-IETF RFC 5027] IETF RFC 5027 (2007), *Security Preconditions for Session Description Protocol (SDP) Media Streams*.

[b-TM Forum GB917] TM Forum GB917 (en vigueur), *SLA Management Handbook, Release 3.0*.

[b-WFM Stage 1-r1] WiMAX Forum – WFM-T31-122-R016v01 (2009), *Service Provider Working Group (SPWG) ETS Phase 1 Requirements for Release 1.6*.

[b-WFM Stage 1-r2] WiMAX Forum – WFM-T31-122-R020v01 (2009), *SPWG ETS Requirements, Release 2.0*.

[b-WFM Stage 2-a1] WiMAX Forum – WFM-T32-001-R016v01 (2010), *Network Architecture – Architecture Tenets, Reference Model and Reference Points, Base Specification, Release 1.6,) ETS Stage 2 Specification (Section 7.14).*

[b-WFM Stage 3-a1] WiMAX Forum – WFM-T33-001-R016v01 (2010), *Network Architecture – Detailed Protocols and Procedures, Base Specification, Release 1.6, ETS Stage 3 Specification (Section 4.19).*

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, 2012