

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2205

(09/2008)

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 futurs	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999

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

Recommandation UIT-T Y.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.

Source

La Recommandation UIT-T Y.2205 a été approuvée le 12 septembre 2008 par la Commission d'études 13 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Architecture, alerte avancée (EW), NGN, qualité de service, service de télécommunications d'urgence (ETS), 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/>.

© UIT 2009

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

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 1
3	Définitions 3
4	Abréviations et acronymes 3
5	Description des télécommunications d'urgence (ET) et de l'alerte avancée 4
5.1	Généralités 4
5.2	Télécommunications d'urgence 5
5.3	Alerte avancée 6
6	Considérations générales concernant les télécommunications d'urgence et l'alerte avancée 6
7	Fonctionnalités et capacités requises d'une manière générale 7
7.1	Télécommunications d'urgence 7
7.2	Alerte avancée 8
8	Mécanismes et capacités pour la prise en charge des télécommunications d'urgence dans les NGN 8
8.1	Généralités 8
8.2	Strate des services..... 12
8.3	Strate de transport..... 14
8.4	Accès au NGN 15
9	Mécanismes et capacités pour la prise en charge de certains aspects de l'alerte avancée dans les NGN 17
9.1	Généralités 17
9.2	Protocole d'alerte commun (CAP)..... 18
10	Priorité de rétablissement de service 19
11	Sécurité 19
	Appendice I – Catégories de télécommunications d'urgence 21
I.1	Télécommunications d'urgence d'individu à autorité 21
I.2	Télécommunications d'urgence entre individus 21
I.3	Télécommunications d'urgence entre autorités 21
I.4	Télécommunications d'urgence d'autorité à individu 22
	Appendice II – Exemples de scénarios pour les systèmes d'alerte avancée 23
II.1	Modèle de distribution sélective..... 23
II.2	Modèle d'extraction sélective 23
	Bibliographie..... 24

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. 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 la Recommandation [UIT-T Y.2201] dans le contexte des NGN (définis dans la Recommandation [UIT-T Y.2001] et décrits plus en détail dans la Recommandation [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

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T E.106] Recommandation UIT-T E.106 (2003), *Plan international de priorité en période de crise destiné aux opérations de secours en cas de catastrophe*.

[UIT-T E.107] Recommandation UIT-T E.107 (2007), *Service de télécommunications d'urgence (ETS) et cadre d'interconnexion pour applications nationales du service ETS*.

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

- [UIT-T H.323] Recommandation UIT-T H.323, *Systèmes de communication multimédia en mode paquet.*
- [UIT-T H.460.4] Recommandation UIT-T H.460.4, *Désignation de la priorité des appels et identification du pays/réseau international d'origine des appels prioritaires H.323.*
- [UIT-T J.260] Recommandation UIT-T J.260, *Prescriptions relatives aux communications à traitement préférentiel sur les réseaux IPCablecom.*
- [UIT-T X.805] Recommandation UIT-T X.805, *Architecture de sécurité pour les systèmes assurant des communications de bout en bout.*
- [UIT-T X.1303] Recommandation UIT-T X.1303, *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.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 (2006), *Prescriptions fonctionnelles et architecture des réseaux de prochaine génération de version 1.*
- [UIT-T Y.2111] Recommandation UIT-T Y.2111, *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, *Niveaux de priorité pour le rétablissement de service dans les réseaux de prochaine génération.*
- [UIT-T Y.2201] Recommandation UIT-T Y.2201 (2007), *Spécifications des réseaux de prochaine génération de version 1.*
- [UIT-T Y.2701] Recommandation UIT-T Y.2701, *Exigences de sécurité pour les réseaux de prochaine génération de version 1.*
- [IETF RFC 2205] IETF RFC RFC 2205, *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification.*
- [IETF RFC 3246] IETF RFC RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior).*
<<http://www.IETF RFC.org/rfc/rfc3246.txt?number=3246>>
- [IETF RFC 3261] IETF RFC RFC 3261, *SIP: Session Initiation Protocol.*
- [IETF RFC 3312] IETF RFC RFC 3312, *Integration of Resource Management and Session Initiation Protocol (SIP).*
- [IETF RFC 4412] IETF RFC RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP).*

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

[IETF RFC 4594] IETF RFC RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*.
<<http://www.IETF RFC.org/rfc/rfc4594.txt?number=4594>>

3 Définitions

La présente Recommandation utilise les définitions des Recommandations [UIT-T Y.1271], [UIT-T Y.2001], [UIT-T Y.2011] et [UIT-T Y.2201].

3.1 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 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.

3.3 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.

3.4 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:

ASN.1	notation de syntaxe abstraite numéro un (<i>abstract syntax notation one</i>)
CAC	contrôle d'admission d'appel (<i>call admission control</i>)
CAP	protocole d'alerte commun (<i>common alerting protocol</i>)
DoS	déni de service (<i>denial of service</i>)
DSCP	point de code des services différenciés (<i>differentiated services code points</i>)
EAS	système d'alerte en cas d'urgence (<i>emergency alert system</i>)
EF	transmission express (<i>expedited forwarding</i>)
ENI	mise en œuvre nationale du service ETS (<i>ETS national implementation</i>)
ET	télécommunications d'urgence (<i>emergency telecommunications</i>)
ETS	service de télécommunications d'urgence (<i>emergency telecommunications service</i>)
EW	alerte avancée (<i>early warning</i>)
IEPS	plan international de priorité en période de crise (<i>international emergency preference scheme</i>)

IP	protocole Internet (<i>Internet protocol</i>)
MMPS	service de priorité multimédia (<i>multimedia priority service</i>)
NGN	réseau de prochaine génération (<i>next generation network</i>)
NOAA	National Oceanic and Atmospheric Administration
PHB	comportement par saut (<i>per hop behaviour</i>)
PIN	numéro d'identification personnel (<i>personal identification number</i>)
PSAP	point de réponse de sécurité publique (<i>public safety answering point</i>)
RTPC	réseau téléphone public commuté (<i>public switched telephone network</i>)
RACF	fonction de contrôle des ressources et d'admission (<i>resource and admission control function</i>)
RMTP	réseau mobile terrestre public (<i>public land mobile network</i>)
RNIS	réseau numérique à intégration de services (<i>integrated services digital network</i>)
RPH	en-tête de priorité de ressource (<i>resource priority header</i>)
RSVP	protocole de réservation de ressources (<i>resource reservation protocol</i>)
QoS	qualité de service (<i>quality of service</i>)
SAME	codage de message de zone spécifique (<i>specific area message encoding</i>)
SCF	fonction de commande de service (<i>service control function</i>)
SIP	protocole d'ouverture de session (<i>session initiation protocol</i>)
SLA	accord de niveau de service (<i>service level agreement</i>)
SS7	système de signalisation n° 7 (<i>signalling system No. 7</i>)
TCP	protocole de commande de transmission (<i>transmission control protocol</i>)
TDR	télécommunications pour les secours en cas de catastrophe (<i>telecommunications for disaster relief</i>)
UDP	protocole datagramme d'utilisateur (<i>user datagram protocol</i>)
ONU/SIPC	stratégie internationale des Nations Unies pour la prévention des catastrophes
VoIP	téléphonie IP (<i>voice over IP</i>)
W-CDMA	accès multiple par répartition en code à large bande (<i>wideband code division multiple access</i>)
WPS	service prioritaire sans fil (<i>wireless priority service</i>)
xDSL	toute variante de ligne d'abonné numérique (<i>any variant of digital subscriber line</i>)
XML	langage de balisage extensible (<i>eXtensible markup language</i>)
XSD	définition de schéma XML (<i>XML schema definition</i>)

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 la Recommandation [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/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).

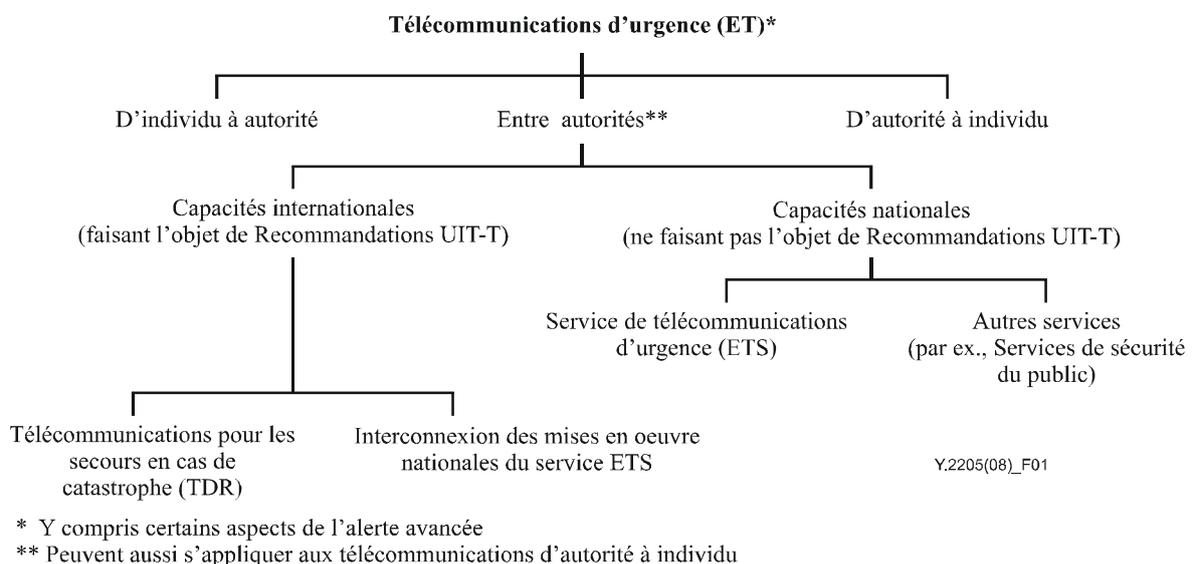


Figure 1 – Cadre des relations terminologiques pour les télécommunications d'urgence

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 la Recommandation [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/locale, font l'objet d'une normalisation nationale/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 la Recommandation [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/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 entre 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 la Recommandation [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.

7 Fonctionnalités et capacités requises d'une manière générale

Les fonctionnalités et capacités requises incluent celles qui sont spécifiées dans les Recommandations [UIT-T Y.1271] et [UIT-T Y.2201] pour les NGN de version 1, 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. La Recommandation [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).

7.2 Alerte avancée

Les objectifs des systèmes d'alerte avancée dans le contexte des NGN sont notamment les suivants:

- avoir des capacités qui fonctionnent en permanence et être opérationnels, robustes et disponibles chaque minute de chaque jour;
- fournir des messages d'alerte uniquement à ceux qui risquent d'être affectés par une catastrophe imminente;
- 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 que seuls des messages autorisés sont envoyés;
- 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).

Parmi les autres objectifs, on peut citer des capacités de filtrage des messages de manière à viser:

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

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

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

8.1 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 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 la Recommandation [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) constituent l'arbitre entre ces strates pour la réservation (et la négociation) liée à la qualité de service dans l'architecture NGN. La Recommandation [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/sessions de télécommunications d'urgence. Les étiquettes utilisées pour identifier et marquer les appels/sessions et/ou le trafic de télécommunications d'urgence dépendent du protocole. Pour réaliser un traitement spécialisé (par exemple prioritaire/préférentiel) de bout en bout pour tous les aspects de l'appel/de la session de télécommunications d'urgence (commande d'appel/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 un appel/une 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 le Document [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 du ou des protocoles particuliers liés aux services en question.

Dans la strate de transport, on peut utiliser le protocole Internet (IP). La composition exacte de la pile de protocoles IP sous-jacents variera probablement d'un fournisseur à l'autre.

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/une session de télécommunications d'urgence peut traverser des technologies de transport très diverses.

Des paragraphes ultérieurs décrivent les diverses caractéristiques et/ou 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 RFC, il est prudent d'utiliser les capacités applicables définies par l'IETF RFC 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 RFC et leur déploiement dans l'Internet et/ou 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 le Document [b-IETF RFC 4190]¹. 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.

Le Document [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.

8.1.1 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.

Dans l'architecture NGN en couches définie dans la Recommandation [UIT-T Y.2012], l'indicateur de priorité envoyé par la fonction de commande de service (SCF) à la fonction de contrôle des ressources et d'admission (RACF) 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.

8.1.2 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).

¹ Conformément au Document [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".

Il est nécessaire d'identifier les demandes d'appel/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). 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/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/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 des accords SLA et sur la politique applicable.

8.1.3 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 service 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). L'utilisation du protocole de réservation de ressource décrit dans le Document [b-IETF RFC RSVP] est un exemple de tel mécanisme.

8.1.3.1 Contrôle d'admission d'appel (CAC)

Le contrôle CAC est un ensemble de mesures/dispositions prises par le réseau pendant la phase d'établissement d'appel/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/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/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.

La Recommandation [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.

8.2 Strate des services

8.2.1 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 les utilisateurs disponibles dans un autre pays. Dans ce cas, il est important qu'un appel/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).

8.2.2 Priorité de ressource SIP

Le Document [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 influencer 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 le Document [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/sessions ETS entrants se voient attribuer la désignation "ets" dans l'en-tête de priorité de ressource. Les appels/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.

8.2.3 Plan IEPS

La Recommandation [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.

La Recommandation [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.

8.2.4 Protocoles de commande des systèmes H.323

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

La Recommandation [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 H.323. Le paramètre de désignation de priorité d'appel H.460.4 prend en charge l'indicateur d'appel prioritaire et cinq niveaux de priorité.

La Recommandation [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 la Recommandation [UIT-T H.323]. Pour les services d'urgence autorisés par les pouvoirs publics (par exemple, service ETS), la Recommandation [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. Pour les services de sécurité du public, la Recommandation [UIT-T H.248.1] définit l'indicateur d'urgence destiné à acheminer l'indication de priorité entre le contrôleur et la passerelle.

8.3 Strate de transport

8.3.1 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 basée sur l'hypothèse que 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/ou 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.

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.

8.3.2 Gestion de la largeur de bande au moyen de RSVP

Dans les réseaux IP, un équivalent (grossier) 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 RFC dans son protocole de réservation de ressource (RSVP) spécifié dans le Document [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 le Document [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 du Document [IETF RFC 4542]. Toutefois, le Document [IETF RFC 4542] utilise la technique de préemption.

Le Document [b-IETF RFC RSVP] spécifie 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, ce document spécifie 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.

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

Le Document [IETF RFC 4594] présente une mise en correspondance recommandée entre les classes de service et les codes de services différenciés (DSCP). La Figure 3 du Document [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, la Recommandation [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 le Document [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).

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

Le Document [b-IETF RFC DSCP] attribue un code DSCP de transmission express pour le trafic ayant fait l'objet d'une admission de capacité. 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 § 8.3.1 et 8.3.2 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.

Il a été proposé de désigner par EF-ADMIT le code demandé et de lui attribuer une valeur appropriée.

8.4 Accès au NGN

8.4.1 Généralités

Il existe plusieurs méthodes d'accès au NGN qui dépendent de la technologie. Conformément à la Recommandation [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 IEEE 802.11 et 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.

8.4.2 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/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 sessions/appels de télécommunications d'urgence.

Par exemple, le 3GPP a spécifié le service de priorité et le service de priorité multimédia pour les systèmes 3GPP. Ces services 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" 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 et le service de priorité multimédia pour les systèmes 3GPP sont spécifiés dans le Document [b-3GPP TS 22.153].

De manière analogue au 3GPP, le 3GPP2 a spécifié le service de priorité multimédia (MMPS) pour les systèmes 3GPP2. Cette spécification figure dans le Document [b-3GPP2 S.R0117-0-v1.0].

8.4.3 Accès fixe

Les réseaux d'accès fixe doivent prendre en charge des mécanismes et capacités spécifiques pour assurer un traitement prioritaire des appels/sessions autorisés de télécommunications d'urgence. Pour cela, on peut utiliser des mécanismes et capacités propres à une technologie (par exemple, 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 des sessions/appels de télécommunications d'urgence.

Par exemple, la Recommandation [UIT-T J.260] définit des prescriptions relatives aux télécommunications prioritaires sur les réseaux IPCablecom. Les principaux aspects considérés peuvent être regroupés en deux domaines: la hiérarchisation des priorités et l'authentification. Ces domaines portent en particulier sur les capacités à prendre en charge sur les réseaux IPCablecom des télécommunications susceptibles de nécessiter un traitement préférentiel (par exemple, TDR et ETS). L'implémentation de méthodes de hiérarchisation des priorités et d'authentification est nécessaire pour la prise en charge de télécommunications prioritaires sur les réseaux IPCablecom.

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

9.1 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 mis en œuvre 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.

9.2 Protocole d'alerte commun (CAP)

Le présent paragraphe décrit le protocole d'alerte commun (CAP) spécifié dans la Recommandation [UIT-T X.1303], qui peut être utilisé pour prendre en charge des applications d'alerte avancée.

La Recommandation [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), 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 la Recommandation [UIT-T X.1303] est techniquement équivalent au protocole d'alerte commun V1.1 d'OASIS et est compatible avec ce protocole. La Recommandation [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 H.323, de coder, transporter et décoder plus facilement les messages CAP.

10 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. La Recommandation [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/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.

11 Sécurité

Les éléments de réseau, systèmes, ressources, données et services 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.
- Mise en œuvre 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/administrations), il faut pouvoir 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.

Pour planifier la sécurité des télécommunications d'urgence, il convient de tenir compte des recommandations formulées dans la Recommandation [UIT-T Y.2701] concernant la sécurité des NGN. Il convient aussi de tenir compte du cadre de sécurité basé sur les dimensions de sécurité suivantes définies dans la Recommandation [UIT-T X.805]:

- Contrôle d'accès
- Authentification
- Non-répudiation
- Confidentialité des données
- Sécurité des communications
- Intégrité des données
- Disponibilité
- Respect de la vie privée.

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 et/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 d'accès à un service public (PSAP).

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>). Ces 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/81/81_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.

Bibliographie

- [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 9)*.
<<http://www.3gpp.org/FTP/Specs/html-info/22153.htm>>
- [b-3GPP2 S.R0117-0-v1.0] 3GPP2 S.R0117-0-v1.0 (06/2006), *3rd Generation Partnership Project 2; Multimedia Priority Service (MMPS) for MMD-based Networks – Stage 1 Requirements*.
<http://www.3gpp2.org/Public_html/specs/S.R0117-0%20v1.0_060714.pdf>
- [b-IETF RFC 2750] IETF RFC 2750 (2000), *RSVP Extensions for Policy Control*.
<<http://www.ietf.org/rfc/rfc2750.txt?number=2750>>
- [b-IETF RFC 3265] IETF RFC 3265 (2002), *(SIP)-Specific Event Notification*.
<<http://www.ietf.org/rfc/rfc3265.txt?number=3265>>
- [b-IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*.
<<http://www.ietf.org/rfc/rfc3853.txt?number=3853>>
- [b-IETF RFC 3936] IETF RFC 3936 (2004), *Procedures for Modifying the Resource reSerVation Protocol (RSVP)*.
<<http://www.ietf.org/rfc/rfc3936.txt?number=3936>>
- [b-IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.
<<http://www.ietf.org/rfc/rfc4032.txt?number=4032>>
- [b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony*.
<<http://www.ietf.org/rfc/rfc4190.txt?number=4190>>
- [b-IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction*.
<<http://www.ietf.org/rfc/rfc4320.txt?number=4320>>
- [b-IETF RFC 4495] IETF RFC 4495 (2006), *A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow*.
<<http://www.ietf.org/rfc/rfc4495.txt?number=4495>>
- [b-IETF RFC 4916] IETF RFC 4916 (2007), *Connected Identity in Session Initiation Protocol*.
<<http://www.ietf.org/rfc/rfc4916.txt?number=4916>>
- [b-IETF RFC 5027] IETF RFC 5027 (2007), *Security Preconditions for Session Description Protocol (SDP) Media Streams*.
<<http://www.ietf.org/rfc/rfc5027.txt?number=5027>>
- [b-IETF RFC DSCP] draft-ietf-tsvwg-admitted-realtime-dscp-00, *DSCP for Capacity-Admitted Traffic*.
- [b-IETF RFC RSVP] draft-ietf-tsvwg-emergency-rsvp, *Resource ReSerVation Protocol (RSVP) Extensions for Emergency Services*.
- [b-UN Global Survey] Stratégie internationale des Nations Unies pour la prévention des catastrophes, Rapport final portant sur une "Etude mondiale des systèmes d'alerte avancée", septembre 2006.
(Référence: <http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf>)

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