

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2205

(09/2008)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA
INFORMACIÓN, ASPECTOS DEL PROTOCOLO
INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Redes de la próxima generación – Aspectos relativos a
los servicios: capacidades y arquitectura de servicios

**Redes de la próxima generación –
Telecomunicaciones de emergencia –
Consideraciones técnicas**

Recomendación UIT-T Y.2205

RECOMENDACIONES UIT-T DE LA SERIE Y
**INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y
 REDES DE LA PRÓXIMA GENERACIÓN**

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes futuras	Y.2600–Y.2699
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.2205

Redes de la próxima generación – Telecomunicaciones de emergencia – Consideraciones técnicas

Resumen

En la Recomendación UIT-T Y.2205 (Y.NGN-ET-Tech) se abordan los aspectos técnicos que pueden incorporarse en las redes de la próxima generación (NGN) para habilitarlas para las telecomunicaciones de emergencia (ET). Se presentan asimismo los principios técnicos necesarios para el soporte de las ET.

Orígenes

La Recomendación UIT-T Y.2205 fue aprobada el 12 de septiembre de 2008 por la Comisión de Estudio 13 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

Palabras clave

Arquitectura, telecomunicaciones prioritarias, telecomunicaciones de emergencia, NGN, calidad de servicio, telecomunicaciones para operaciones de socorro (TDR), servicio de telecomunicaciones de emergencia (ETS), alerta temprana (EW).

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT [ha recibido/no ha recibido] notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2009

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones.....	3
4 Abreviaturas.....	3
5 Descripción de las telecomunicaciones de emergencia (ET, <i>emergency telecommunications</i>) y la alerta temprana	5
5.1 Introducción general.....	5
5.2 Telecomunicaciones de emergencia.....	6
5.3 Alerta temprana	7
6 Consideraciones generales sobre las telecomunicaciones de emergencia y la alerta temprana	7
7 Capacidades y requisitos funcionales generales.....	8
7.1 Telecomunicaciones de emergencia.....	8
7.2 Alerta temprana	9
8 Mecanismos y capacidades para el soporte de las telecomunicaciones de emergencia en las NGN.....	9
8.1 Generalidades	9
8.2 Estrato de servicio	14
8.3 Estrato de transporte.....	15
8.4 Acceso a la NGN.....	17
9 Mecanismos y capacidades que soportan algunos aspectos de la alerta temprana en las NGN.....	18
9.1 Generalidades	18
9.2 Protocolo de alerta común (CAP, <i>common alerting protocol</i>).....	19
10 Prioridad de restauración del servicio.....	20
11 Seguridad.....	20
Apéndice I – Categorías de telecomunicaciones de emergencia	22
I.1 Telecomunicaciones de emergencia individuo-autoridad	22
I.2 Telecomunicaciones de emergencia individuo-individuo.....	22
I.3 Telecomunicaciones de emergencia autoridad-autoridad	22
I.4 Telecomunicaciones de emergencia autoridad-individuo.....	23
Apéndice II – Ejemplos prácticos de sistemas de alerta temprana	24
II.1 Modelo activo.....	24
Bibliografía	25

Introducción

La Recomendación [UIT-T Y.1271] establece los requisitos y capacidades de red para las telecomunicaciones de emergencia. La puesta en marcha de telecomunicaciones prioritarias basadas en esos requisitos, como ejemplifican las autoridades coordinadoras de las operaciones de socorro mediante las redes públicas, puede dar lugar a la creación de nuevos mecanismos y al interfuncionamiento/reutilización de los mecanismos existentes. Las telecomunicaciones de emergencia deben ser prioritarias con respecto a los servicios normales de la red pública. Las telecomunicaciones prioritarias en situaciones de emergencia no son algo nuevo, pues las redes con conmutación de circuitos han soportado sistemas de este tipo durante años, principalmente para las llamadas vocales (por ejemplo, [UIT-T E.106]). No obstante, los métodos técnicos para soportar los requisitos inherentes de las telecomunicaciones de emergencia en el entorno de las NGN están evolucionando. Los métodos de prioridad con conmutación de circuitos tradicionales no se aplican necesariamente en las NGN dadas las diferencias fundamentales que existen entre las telecomunicaciones con conmutación de circuitos y con conmutación de paquetes.

En la Recomendación [UIT-T Y.1271] se describen los requisitos y capacidades en términos generales y abstractos, independientes de la tecnología utilizada.

Dado que las NGN se basan en la tecnología de conmutación de paquetes, fundamentalmente diferente de la conmutación de circuitos, es necesario considerar los problemas técnicos y las posibles soluciones que pueden aportarse para materializar las capacidades de telecomunicaciones de emergencia en las NGN.

En esta Recomendación se abordan los aspectos técnicos que pueden incorporarse en las redes de la próxima generación (NGN) para habilitarlas para las telecomunicaciones de emergencia, así como los principios inherentes que se han de tener en cuenta.

Recomendación UIT-T Y.2205

Redes de la próxima generación – Telecomunicaciones de emergencia – Consideraciones técnicas

1 Alcance

En esta Recomendación se abordan los aspectos técnicos que pueden incorporarse en las redes de la próxima generación (NGN, *next generation networks*) para habilitarlas para las telecomunicaciones de emergencia (ET, *emergency telecommunications*). Además, se presentan los principios técnicos necesarios para el soporte de las ET. Se especifican asimismo requisitos y capacidades de las ET además de los expuestos en [UIT-T Y.2201] en el contexto de las NGN (como se definen en [UIT-T Y.2001] y que también se tratan en [UIT-T Y.2011]).

Las telecomunicaciones de emergencia (incluido el soporte de algunas características de alerta temprana (véase la figura 1)) comprenden:

- las telecomunicaciones de emergencia individuo-autoridad, por ejemplo, llamadas a los servicios de emergencias;
- las telecomunicaciones de emergencia autoridad-autoridad;
- las telecomunicaciones de emergencia autoridad-individuo, por ejemplo, los servicios de notificación comunitarios.

En el apéndice I puede encontrarse más información sobre las categorías expuestas de ET.

Se especifican también algunos requisitos y capacidades necesarios para la alerta temprana. No se tratan en esta Recomendación, y quedan fuera de su alcance, las capacidades de telecomunicaciones de emergencia individuo-autoridad.

Algunos de los medios técnicos aquí descritos pueden también utilizarse para las telecomunicaciones de emergencia individuo-autoridad o individuo-individuo, aunque no se aborden tales categorías en esta Recomendación.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y otras referencias son objeto de revisión, por lo que se alienta a los usuarios de esta Recomendación a que utilicen la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

- [UIT-T E.106] Recomendación UIT-T E.106 (2003), *Plan internacional de preferencias en situaciones de emergencia para actuaciones frente a desastres.*
- [UIT-T E.107] Recomendación UIT-T E.107 (2007), *Servicio de telecomunicaciones en caso de emergencia (STE) y marco de interconexión para la implantación nacional de STE.*
- [UIT-T H.248.1] Recomendación UIT-T H.248.1, *Protocolo de control de las pasarelas: Versión 3.*
- [UIT-T H.323] Recomendación UIT-T H.323 (2006), *Sistemas de comunicación multimedios basados en paquetes.*

- [UIT-T H.460.4] Recomendación UIT-T H.460.4, *Designación de prioridades llamada e identificación la red nacional/internacional de origen de llamada para llamadas prioritarias H.323.*
- [UIT-T J.260] Recomendación UIT-T J.260, *Requisitos aplicables a las telecomunicaciones preferentes en redes IPCablecom.*
- [UIT-T X.805] Recomendación UIT-T X.805, *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.*
- [UIT-T X.1303] Recomendación UIT-T X.1303, *Protocolo de alerta común (CAP 1.1).*
- [UIT-T Y.110] Recomendación UIT-T Y.110 (1998), *Principios y marco de la infraestructura mundial de la información.*
- [UIT-T Y.1271] Recomendación UIT-T Y.1271 (2004), *Requisitos y capacidades de red generales necesarios para soportar telecomunicaciones de emergencia en redes evolutivas con conmutación de circuitos y conmutación de paquetes.*
- [UIT-T Y.1541] Recomendación UIT-T Y.1541 (2006), *Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet.*
- [UIT-T Y.2001] Recomendación UIT-T Y.2001 (2004), *Visión general de las redes de próxima generación.*
- [UIT-T Y.2011] Recomendación UIT-T Y.2011 (2004), *Principios generales y modelo de referencia general de las redes de próxima generación.*
- [UIT-T Y.2012] Recomendación UIT-T Y.2012 (2006), *Requisitos funcionales y arquitectura de la red de próxima generación.*
- [UIT-T Y.2111] Recomendación UIT-T Y.2111, *Funciones del control de recursos y de admisión en redes de próxima generación.*
- [UIT-T Y.2171] Recomendación UIT-T Y.2171 (2006), *Niveles de prioridad del control de admisión en redes de próxima generación.*
- [UIT-T Y.2172] Recomendación UIT-T Y.2172, *Niveles de prioridad de restablecimiento del servicio en las redes de próxima generación.*
- [UIT-T Y.2201] Recomendación UIT-T Y.2201 (2007), *Requisitos de las redes de próxima generación, versión 1.*
- [UIT-T Y.2701] Recomendación UIT-T Y.2701, *Requisitos de seguridad de la versión 1 de la red de próxima generación.*
- [IETF RFC 2205] IETF RFC 2205, *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification.* <<http://www.ietf.org/rfc/rfc2205.txt?number=2205>>
- [IETF RFC 3246] IETF RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior).* <<http://www.ietf.org/rfc/rfc3246.txt?number=3246>>
- [IETF RFC 3261] IETF RFC 3261, *SIP: Session Initiation Protocol.* <<http://www.ietf.org/rfc/rfc3261.txt?number=3261>>
- [IETF RFC 3312] IETF RFC 3312, *Integration of Resource Management and Session Initiation Protocol (SIP).* <<http://www.ietf.org/rfc/rfc3312.txt?number=3312>>
- [IETF RFC 4412] IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP).* <<http://www.ietf.org/rfc/rfc4412.txt?number=4412>>
- [IETF RFC 4542] IETF RFC 4542, *Implementing an emergency telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite.* <<http://www.ietf.org/rfc/rfc4542.txt?number=4542>>

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

3 Definiciones

En esta Recomendación se emplean las definiciones de [UIT-T Y.1271], [UIT-T Y.2001], [UIT-T Y.2011] y [UIT-T Y.2201].

3.1 telecomunicaciones de emergencia (ET, *emergency telecommunications*): Todo servicio de emergencia que necesita de las NGN un tratamiento especial en comparación con otros servicios. Comprende los servicios de emergencia autorizados por el Estado y los servicios de seguridad pública.

3.2 servicio de telecomunicaciones de emergencia (ETS, *emergency telecommunications service*) [UIT-T E.107]: Servicio nacional que proporciona telecomunicaciones prioritarias a los usuarios autorizados en situaciones de catástrofe y emergencia.

3.3 red de la próxima generación (NGN, *next generation network*) [UIT-T Y.2001]: Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta la movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios.

3.4 telecomunicaciones para operaciones de socorro (TDR, *telecommunications for disaster relief*): Capacidad de telecomunicaciones nacionales e internacionales para las operaciones de socorro. Puede utilizar las redes internacionales permanentes compartidas implantadas y utilizadas, redes temporales creadas específicamente para las TDR o una combinación de ambas.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes abreviaturas:

ASN.1	Notación de sintaxis abstracta uno (<i>abstract syntax notation one</i>)
CAC	Control de admisión de llamada (<i>call admission control</i>)
CAP	Protocolo de alerta común (<i>common alerting protocol</i>)
DoS	Denegación de servicio (<i>denial of service</i>)
DSCP	Puntos de código de servicios diferenciados (<i>diff-serv code point</i>)
EAS	Sistema de alerta de emergencia (<i>emergency alert system</i>)
EF	Retransmisión rápida (<i>expedited forwarding</i>)
EIRD/NU	Estrategia Internacional de las Naciones Unidas de Reducción de Desastres
ENI	Implementación nacional del ETS (<i>ETS national implementation</i>)
ET	Telecomunicaciones de emergencia (<i>emergency telecommunications</i>)
ETS	Servicio de telecomunicaciones de emergencia (<i>emergency telecommunications service</i>)
EW	Alerta temprana (<i>early warning</i>)
IEPS	Plan Internacional de Preferencias en Situaciones de Emergencia (<i>international emergency preference scheme</i>)
IP	Protocolo Internet (<i>Internet protocol</i>)

MMPS	Servicio de prioridad multimedios (<i>multimedia priority service</i>)
NGN	Red de la próxima generación (<i>next generation network</i>)
NOAA	Administración Nacional del Océano y la Atmósfera (<i>National Oceanic and Atmospheric Administration</i>)
PHB	Comportamiento por salto (<i>per hop behaviour</i>)
PIN	Número de identificación personal (<i>personal identification number</i>)
PSAP	Punto de acceso de servicio público (<i>public service access point</i>)
QoS	Calidad de servicio (<i>quality of service</i>)
RACF	Función de control de recursos y admisión (<i>resource and admission control function</i>)
RDSI	Red digital de servicios integrados
RMTP	Red móvil terrestre pública
RPH	Encabezamiento de prioridad de recursos (<i>resource priority header</i>)
RSVP	Protocolo de reserva de recursos (<i>resource ReSerVation protocol</i>)
RTPC	Red telefónica pública conmutada
SAME	Codificación de mensajes específica de la zona (<i>specific area message encoding</i>)
SCF	Función de control de servicio (<i>service control function</i>)
SIP	Protocolo de inicio de sesión (<i>session initiation protocol</i>)
SLA	Acuerdo de nivel de servicio (<i>service level agreement</i>)
SS7	Sistema de señalización N° 7 (<i>signalling system No. 7</i>)
TCP	Protolo de central de transmisión (<i>transmission control protocol</i>)
TDR	Telecomunicaciones para operaciones de socorro (<i>telecommunications for disaster relief</i>)
UDP	Protocolo de datagrama de usuario (<i>user datagram protocol</i>)
VoIP	Voz sobre IP (<i>voice over IP</i>)
W-CDMA	Acceso múltiple por división de código de banda amplia (<i>wideband code division multiple access</i>)
WPS	Servicio de prioridad inalámbrico (<i>wireless priority service</i>)
xDSL	Cualquier variante de línea de abonado digital (<i>any variant of digital subscriber line</i>)
XML	Lenguaje de marcación extensible (<i>eXtensible markup language</i>)
XSD	Definición de esquema XML (<i>XML schema definition</i>)

5 Descripción de las telecomunicaciones de emergencia (ET, *emergency telecommunications*) y la alerta temprana

5.1 Introducción general

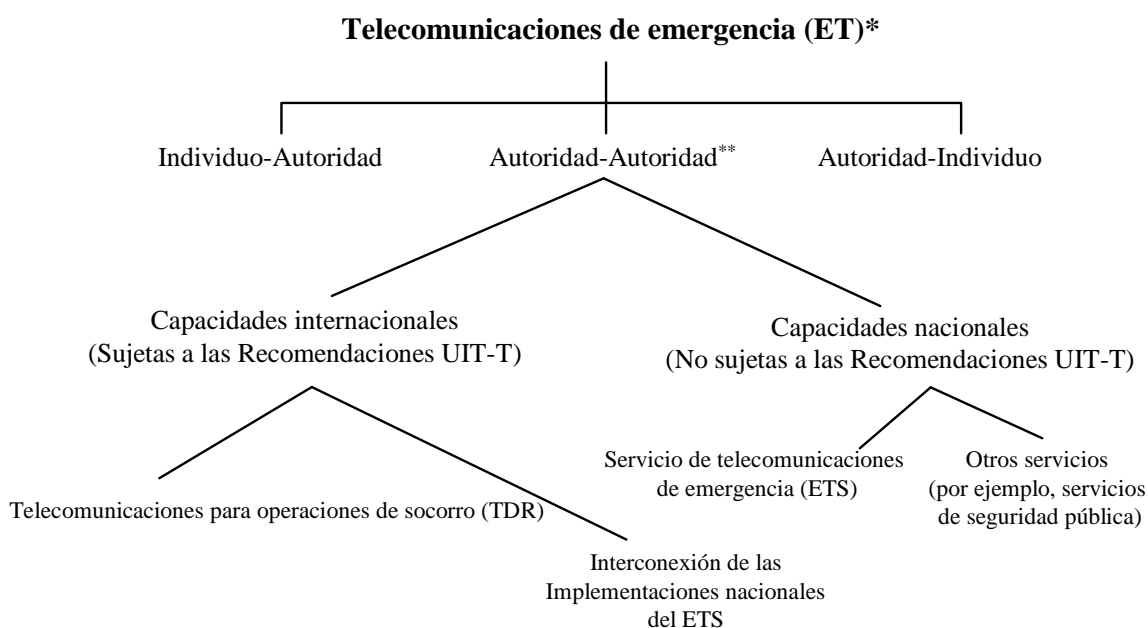
En esta Recomendación se emplean los siguientes términos:

- telecomunicaciones de emergencia ET (*emergency telecommunications*)
- servicio de telecomunicaciones de emergencia ETS (*emergency telecommunications service*)
- telecomunicaciones para operaciones de socorro TDR (*telecommunications for disaster relief*)
- alerta temprana EW (*early warning*)

Es fundamental que la distinción entre estos términos esté consensuada y se entienda claramente, por ello, los términos mencionados se utilizan de la siguiente manera:

- ET Término general para todos los servicios de emergencia que han de recibir de las NGN un tratamiento especial en comparación con otros servicios.
- ETS Este término se utiliza tal y como se define en [UIT-T E.107].
- TDR Término genérico para una capacidad de telecomunicaciones empleada a fin de llevar a cabo operaciones de socorro.
- EW Término genérico para todos los tipos de sistemas/capacidades/servicios de alerta temprana.

Según esta clasificación, se forma un árbol en el que las ET son las raíces de todas las actividades. En la siguiente figura 1 se muestra la utilización de los términos y las relaciones entre ellos.



* Incluidos algunos aspectos de la alerta temprana

** Puede también aplicarse a las telecomunicaciones autoridad-individuo

Figura 1 – Relaciones terminológicas en el marco de las telecomunicaciones de emergencia

5.2 Telecomunicaciones de emergencia

Las telecomunicaciones de emergencia (ET) son todos los servicios de emergencia que han de recibir un tratamiento especial de las NGN con respecto a otros servicios. Comprenden los servicios de emergencia autorizados por el Estado y los servicios de seguridad pública. A continuación se presentan algunos ejemplos de servicios específicos que pertenecen a la categoría general de las telecomunicaciones de emergencia:

1) *Telecomunicaciones para operaciones de socorro (TDR)*

TDR es una capacidad de telecomunicaciones internacionales y nacionales para llevar a cabo operaciones de socorro. Puede utilizar las redes internacionales permanentes compartidas implantadas y utilizadas, redes temporales creadas específicamente para las TDR o una combinación de ambas.

2) *Servicio de telecomunicaciones de emergencia (ETS)*

El ETS es un servicio nacional que proporciona telecomunicaciones prioritarias a los usuarios autorizados del ETS en caso de catástrofe o en situación de emergencia. Puede encontrarse una descripción del ETS en [UIT-T E.107]. En [ITU-T E.107] se dan orientaciones para permitir las telecomunicaciones entre una implementación nacional del ETS (ENI, *ETS national implementation*) y otras ENI (Autoridad-Autoridad).

3) *Servicios nacionales/regionales/locales de emergencia y servicios de seguridad pública*

Otros ejemplos de ET son los servicios nacionales/regionales/locales de emergencia y los servicios de seguridad pública. Se trata de servicios especializados para las situaciones de emergencia a nivel nacional/regional/local y para la seguridad pública. Estos servicios de

emergencia se reducen al ámbito nacional/regional/local y están sujetos a la normalización nacional/regional.

5.3 Alerta temprana

La Estrategia Internacional de las Naciones Unidas de Reducción de Desastres (EIRD/NU), en su Informe de 2006 al Secretario General de las Naciones Unidas sobre "Estudio mundial sobre los sistemas de alerta temprana", define la alerta temprana como "la comunicación puntual y eficaz de información a través de instituciones identificadas que permite a los individuos expuestos a un peligro adoptar las medidas necesarias para evitar o reducir los riesgos incurridos y preparar una respuesta eficaz". En este Informe de las Naciones Unidas se presenta una evaluación de las capacidades, carencias y oportunidades existentes para construir un sistema de alerta temprana mundial para todos los peligros de la naturaleza.

6 Consideraciones generales sobre las telecomunicaciones de emergencia y la alerta temprana

Antes de que se adoptase la [UIT-T Y.1271], los requisitos de las capacidades de telecomunicaciones de emergencia estaban principalmente relacionados con las redes con conmutación de circuitos, como la red telefónica pública conmutada (RTPC).

Estos requisitos se basaban y aprovechaban de las características de las redes con conmutación de circuitos, como, por ejemplo:

- control de admisión mediante un fuerte acoplamiento entre la señalización y los recursos de medios;
- todo el tráfico de medios necesita una anchura de banda uniforme y una velocidad binaria de entrega constante;
- anchura de banda reservada en función del flujo;
- separación del tráfico de control y de datos.

Estas características no están necesariamente presentes en las actuales redes con conmutación de paquetes sin garantías, donde:

- Las redes con conmutación de paquetes tienden a compartir recursos y emplear la puesta en cola para compensar el tráfico en ráfagas; generando la combinación, por norma general, un servicio sin garantías.
- Puede ser difícil aplicar el control de admisión, pues muchas aplicaciones no indican sus necesidades de anchura de banda y la señalización y los medios no están acoplados.
- Las aplicaciones/servicios tienen necesidades de anchura de banda variables y pueden enviar datos a velocidades ajustadas dinámicamente.
- Los distintos flujos de paquetes comparten la anchura de banda multiplexada estadísticamente.
- El tráfico de control de recursos y de datos pueden compartir los mismos recursos de la red.

En las NGN con conmutación de paquetes, los paquetes pueden entrar en conflicto por la anchura de banda disponible, a menos que se apliquen medidas especiales. En el mero nivel de transporte, no es sencillo rechazar paquetes o controlar su flujo. Además, el diseño del tráfico de una red de paquetes es muy distinto del de una red de circuitos en lo que respecta a los métodos normalizados y universalmente aceptados. Un determinado "flujo" de paquetes puede verse afectado por otros flujos de paquetes que utilizan el mismo recurso, a menos que se adopten las medidas especiales adecuadas y se apliquen en la NGN. Por otro lado, la separación entre el servicio y el transporte en una NGN puede ser beneficiosa para la configuración de capacidades de emergencia diversas y más flexibles.

Estas condiciones se traducen en que la configuración de las capacidades de telecomunicaciones de emergencia no es un mecanismo directo, obvio o simple, ni puede ser una mera transposición de lo que se hace en la conmutación de circuitos. Otras diferencias entre las redes con conmutación de circuitos y con conmutación de paquetes, así como entre diversas tecnologías de paquetes, afectarán a la configuración y cumplimiento de los requisitos especificados en [UIT-T Y.1271].

Por consiguiente, el objetivo de esta Recomendación es indicar qué características y mecanismos de las NGN pueden emplearse para facilitar el cumplimiento de los requisitos de las telecomunicaciones de emergencia y de algunos aspectos de la alerta temprana.

7 Capacidades y requisitos funcionales generales

Las capacidades y requisitos funcionales comprenden los especificados en [UIT-T Y.1271] y [UIT-T Y.2201] para la versión 1 de las NGN, además de los prescritos en el Estudio mundial sobre los sistemas de alerta temprana de las Naciones Unidas pertinentes para el desarrollo de las NGN.

7.1 Telecomunicaciones de emergencia

En el cuadro 1 se enumeran las capacidades y requisitos funcionales de las telecomunicaciones de emergencia.

Cuadro 1 – Lista de capacidades y requisitos funcionales de las telecomunicaciones de emergencia

Capacidades y requisitos funcionales de las telecomunicaciones de emergencia
Tratamiento prioritario mejorado
Redes seguras
Confidencialidad del emplazamiento
Restablecimiento
Conectividad de red
Compatibilidad
Movilidad
Cobertura ubicua
Supervivencia/resistencia
Transmisión en tiempo real con soporte de: voz/texto en tiempo real y vídeo/imágenes (cuando se disponga de la anchura de banda necesaria)
Transmisión en tiempo no real con soporte de: mensajes/difusión en tiempo no real (audio/vídeo)
Anchura de banda adaptable
Fiabilidad/disponibilidad

El objetivo es que haya una gran confianza y probabilidad de que las telecomunicaciones críticas estén disponibles para que los usuarios autorizados, como los que efectúan telecomunicaciones de emergencia, puedan utilizarlas de manera fiable. En [ITU-T Y.1271] pueden encontrarse los "Requisitos y capacidades de red generales necesarios para soportar telecomunicaciones de emergencia en redes evolutivas con conmutación de circuitos y conmutación de paquetes".

Con respecto al vídeo y las imágenes, habrá de tomarse en consideración la disponibilidad de la anchura de banda necesaria (por ejemplo, una forma de recurso).

7.2 Alerta temprana

Algunos de los objetivos de los sistemas de alerta temprana en el contexto de las NGN son:

- Disponer de capacidades en continuo funcionamiento y ser operativos, robustos y estar disponibles las veinticuatro horas del día.
- Transmitir mensajes de alerta únicamente a los posibles afectados por una catástrofe inminente.
- Facilitar las capacidades de telecomunicaciones necesarias para la transmisión en tiempo real (por ejemplo, información de datos sísmicos o sobre el nivel del mar).
- Estar basados en normas internacionalmente acordadas.
- Garantizar el envío únicamente de mensajes autorizados.
- Evitar la generación de mensajes sin destino o innecesarios (por ejemplo, mensajes enviados a destinatarios erróneos y/o mensajes que no contengan información viable de utilidad).

Entre los objetivos también se pueden contar las capacidades para soportar el filtrado de los mensajes de manera que lleguen a:

- Grupos de usuarios.
- Regiones, etc.

Seleccionados (por ejemplo, una forma de "difusión en células")

8 Mecanismos y capacidades para el soporte de las telecomunicaciones de emergencia en las NGN

8.1 Generalidades

La separación del control de servicio/aplicación del transporte, que permite ofrecer separadamente servicios de aplicación y de transporte, y que éstos evolucionen por separado, es la principal característica de las NGN. Esta separación adopta la forma de dos bloques o estratos de funcionalidades diferenciados. Las funciones de transporte residen en el estrato de transporte y las funciones de control de servicio relacionadas con las aplicaciones, como la telefonía, residen en el estrato de servicio. En general, cada estrato tendrá su propio conjunto de funciones, actores y dominios administrativos (véase [UIT-T Y.110]). Las funciones que participan en la configuración del/de los servicio(s) son independientes de las que afectan a la configuración de la conexión de transporte. Desde un punto de vista técnico, cada estrato puede manejarse por separado. Las funciones de control de recursos y admisión (RACF, *resource and admission control functions*) ejercen la función de árbitro entre estos estratos en cuanto a la reserva (y negociación) de calidad de servicio en la arquitectura de la NGN. En [UIT-T Y.2111] se especifican la arquitectura funcional y los requisitos de las funciones de control de recursos y admisión en las redes de la próxima generación, que pueden comprender diversas tecnologías de acceso y transporte núcleo, así como múltiples dominios. Las decisiones de las RACF con respecto a la calidad de servicio se basan en acuerdos de nivel de servicio, prioridad de servicios, perfiles de usuario, políticas del operador de red y disponibilidad de recursos tanto para las redes núcleo y de acceso. Una vez autenticados y autorizados, las RACF han de identificar a los usuarios de telecomunicaciones de emergencia y darles prioridad en el control de admisión.

Si en las NGN ha de diferenciarse el tráfico de telecomunicaciones de emergencia del tráfico normal, será necesario disponer de las convenientes etiquetas distintivas, también conocidas como marcadores. En este contexto se emplea el término marcación (de tráfico).

En la arquitectura de protocolo de la NGN de extremo a extremo (es decir, los segmentos de red núcleo y de acceso) multicapa (es decir, estratos de transporte y servicio), puede haber etiquetas con

diversas formas en las diversas capas del protocolo tanto verticalmente (es decir interacción entre las distintas capas del protocolo) como horizontalmente (es decir, interacción entre elementos de red en comunicación). Las etiquetas pueden transportarse en paquetes de señalización y/o estar incluidas en el encabezamiento del paquete de datos a fin de identificar y marcar las llamadas/sesiones de telecomunicaciones de emergencia. Las etiquetas que se utilizan para identificar y marcar llamadas/sesiones de telecomunicaciones de emergencia y/o el tráfico dependen del protocolo empleado. Para lograr un tratamiento especializado (por ejemplo, prioritario/preferente) de extremo a extremo para todos los aspectos de la llamada/sesión de telecomunicaciones de emergencia (es decir, control de llamada/sesión, tráfico portador y gestión) es necesario que exista una adecuada correspondencia y compatibilidad entre las etiquetas utilizadas en los diferentes protocolos. Por ejemplo, la información de encabezamiento de prioridad de recurso SIP empleada en la capa de control para identificar una llamada/sesión prioritaria ha de poder tener una correspondencia con los correspondientes puntos de código diff-serv (DCSP, *diff-serv code points*) para marcar el tráfico de telecomunicaciones de emergencia en la capa de red IP. Del mismo modo, los puntos de código diff-serv (DCSP) en la capa 3 han de tener una correspondencia con los parámetros prioritarios de la VLAN o Ethernet en la capa 2 del protocolo de transporte. Puede encontrarse la especificación de SIP en [IETF RFC 3261] y sus actualizaciones [b-IETF RFC 3265], [b-IETF RFC 3853], [b-IETF RFC 4320], [b-IETF RFC 4916], [b-IETF RFC 4032] y [b-IETF RFC 5027].

En el estrato de servicio, los servicios tienden a utilizar los protocolos específicos y designados. Por tanto, las técnicas que puedan aprovecharse para los servicios de telecomunicaciones de emergencias específicos variarán en función de cada servicio y de las capacidades de los protocolos propios del servicio en cuestión.

En el estrato de transporte puede utilizarse el protocolo Internet (IP). Es probable que la composición exacta de la pila de protocolo IP subyacente varíe de un proveedor a otro.

Además, los protocolos utilizados en las infraestructuras de acceso locales (último kilómetro) pueden diferir de los de las infraestructuras núcleo. Las infraestructuras de acceso locales pueden ser alámbricas (es decir, acceso fijo), inalámbricas o una combinación de ambas.

Por consiguiente, un determinado trayecto de extremo a extremo para una llamada/sesión de telecomunicaciones de emergencia puede atravesar una amplia gama de tecnologías de transporte.

En las últimas cláusulas se definen las diversas características y/o capacidades de cada tecnología que se pueden aprovechar para facilitar el cumplimiento de los requisitos de las telecomunicaciones de emergencia.

Dado que el estrato de transporte puede utilizar el IP (y otros protocolos conexos), como el TCP o el UDP, definidos por el IETF, es prudente utilizar las capacidades definidas por el IETF aplicables a su utilización a fin de soportar las telecomunicaciones de emergencia del caso. Este punto se desarrolla más adelante.

Es importante distinguir entre las especificaciones (RFC) del IETF y su implantación en Internet y/o en el contexto de las NGN. En ambos casos, las especificaciones reales utilizadas dependerán de lo que cada proveedor haya instalado. No obstante, dado que Internet queda fuera del alcance del UIT-T, no pueden establecerse hipótesis sobre la calidad de servicio o las capacidades de los trayectos de Internet, como se expone en [b-IETF RFC 4190]¹. Por otro lado, sí está dentro del alcance del UIT-T establecer requisitos más estrictos para las telecomunicaciones de emergencia internacionales en las NGN basadas en IP, por lo que pueden proponerse en Recomendaciones del UIT-T para su aplicación por parte de los proveedores de las NGN.

En [IETF RFC 4542] se exponen posibles soluciones para el "Servicio de preferencias de emergencia en Internet". Muchos de los conceptos que se presentan se aplican al ETS en el contexto de las NGN.

En una NGN donde los estratos de servicio y transporte son independientes, los siguientes factores influirán en la consecución con éxito de las telecomunicaciones de emergencia:

- i) identificación y marcación del tráfico de telecomunicaciones de emergencia;
- ii) política de control de admisión;
- iii) política de atribución de anchura de banda;
- iv) autenticación y autorización de usuarios de telecomunicaciones de emergencia certificados.

8.1.1 Tratamiento prioritario

Por norma general, el tratamiento prioritario es fundamental a la hora de efectuar telecomunicaciones de emergencia, que, por definición, han de considerarse más importantes que los servicios de telecomunicaciones ordinarios. Cuando los servicios ordinarios consumen la inmensa mayoría de los recursos finitos de la red, las telecomunicaciones de emergencia se ven forzadas a competir por estos mismos recursos finitos y pueden verse menoscabadas. Por consiguiente, habrán de encontrarse los medios de otorgar un tratamiento prioritario a los servicios de emergencia por oposición a los servicios de telecomunicaciones ordinarios. En principio, esto conlleva:

- a) reconocer a los usuarios de telecomunicaciones de emergencia autorizados;
- b) otorgar a los usuarios de telecomunicaciones de emergencia autorizados la prioridad del servicio.

En la arquitectura de capas de la NGN, como se define en [UIT-T Y.2012], el indicador de prioridad enviado por la función de control de servicio (SCF, *service control function*) a la función de control de recursos y admisión (RACF) ha de poder indicar niveles de prioridad asociados con los usuarios para permitir la aplicación de distintas políticas y la distinción entre múltiples tipos de aplicaciones de prioridad. Por ejemplo, puede otorgarse al personal de un hospital un nivel de prioridad de usuario más bajo que a los coordinadores de operaciones de socorro en caso de emergencia críticos.

¹ En [b-IETF RFC 4190] se dice que:

"Una de las constantes de la evolución de Internet ha sido el soporte sin garantías como modelo de servicio por defecto", y que;

"las comunicaciones ETS entre dominios no deben basarse en el soporte ubicuo, ni siquiera extendido a lo largo del trayecto entre puntos extremos."

8.1.2 Identificación, autenticación y autorización y control de acceso

Es necesario impedir el acceso no autorizado, por ejemplo de intrusos suplantando la identidad de usuarios autorizados, a los servicios y recursos de telecomunicaciones de emergencia. Por tanto, es necesario contar con el soporte de mecanismos y capacidades para autenticar y autorizar el acceso de los usuarios de telecomunicaciones de emergencia, dispositivos, o combinaciones de ambos, según disponga la política específica del servicio (por ejemplo, ETS y TDR).

Es necesario identificar las peticiones de llamada/sesión de telecomunicaciones de emergencia (por ejemplo, mediante marcación especializada, entrada, perfiles de usuario o abono). Los proveedores de la NGN han de acelerar la autenticación y autorización de los usuarios de telecomunicaciones de emergencia. Se necesitan mecanismos y métodos específicos para realizar la autenticación y la autorización en función de la política específica de las telecomunicaciones de emergencia (por ejemplo, utilización de un número de identificación personal (PIN, *personal identification number*), y de los perfiles de usuario y abono). Una vez que el usuario, el dispositivo o una combinación de ambos esté autenticado y autorizado de acuerdo con la política aplicable, es necesario marcar la llamada/sesión de telecomunicaciones de emergencia e indicarlo en el sentido de destino a las redes posteriores. Del mismo modo, una vez autenticado y autorizado, es necesario que todos los aspectos de la llamada sesión de telecomunicaciones de emergencia, señalización/control, tráfico portador y cualquier gestión correspondiente reciban prioridad.

También ha de considerarse la posibilidad de aplicar la autenticación y autorización a la entrega y recepción de llamadas/sesiones de telecomunicaciones de emergencia entre proveedores de NGN, teniendo en cuenta el entorno multiproveedor y la separación entre el control de servicio y el transporte. La autenticación y autorización de proveedores de NGN para la entrega y recepción de llamadas/sesiones de telecomunicaciones de emergencia y del tráfico ha de basarse en los acuerdos de nivel de servicio y en la política aplicable.

8.1.3 Consideraciones sobre el control de admisión para aumentar la probabilidad de admisión

Una de las funciones de la función de control de recursos y admisión (RACF) es soportar el control de la calidad de servicio (QoS, *quality of service*) para incluir la admisión de recursos y la reserva de recursos, si así lo desea el proveedor de servicios. Así, en los momentos de alta demanda de servicios por parte de los usuarios, será necesario denegar algunas peticiones de servicio. De no ocurrir tales denegaciones, es posible que la NGN no pueda garantizar plenamente la calidad de servicio en casos de emergencia. Los procesos relacionados con la QoS conllevan la autorización en función de los perfiles de usuario, los acuerdos de nivel de servicio, las políticas de cada operador, la prioridad de servicio y la disponibilidad de recursos en el acceso y el transporte núcleo. En esta Recomendación se aboga por que la RACF tenga la capacidad de establecer prioridades entre las peticiones de servicio a partir de la prioridad del servicio. (Una red que simplemente deniegue peticiones autorizadas a causa de una congestión momentánea dará un mal servicio a los clientes, si se ven obligados a presentar repetidamente las peticiones.) Por consiguiente, en esta Recomendación se sostiene que la prioridad del servicio es el principal factor que ha de considerar el método de planificación de atribución de recursos en cola/decisión de admisión general. A continuación se tratan los mecanismos que habilitan esta funcionalidad.

Los requisitos de alto nivel de la RACF han de aplicarse a las peticiones autorizadas de QoS utilizando los perfiles de usuario y la prioridad. Uno de los requisitos específicos es que el control de admisión utilice la información de prioridad de servicio para otorgar un trato prioritario. Pueden utilizarse diversos métodos para determinar la prioridad de servicio y controlar la admisión en función de los recursos.

Uno de estos métodos consiste en fijar un nivel umbral de admisión más alto para el tráfico de telecomunicaciones de emergencia, permitiendo así la admisión adicional de las peticiones prioritarias cuando se están denegando las ordinarias. En efecto, con este método se incrementa

temporalmente la utilización de los recursos de la red. No obstante, dada la gran cantidad de recursos de la NGN y que en un intervalo de tiempo apreciable algunos recursos volverán naturalmente a estar disponibles (por ejemplo, cuando se completen otras sesiones), el sistema restaurará su capacidad de tráfico diaria operativa. Además, suponiendo que la cantidad de tráfico prioritario es relativamente pequeña y que las redes nunca, o casi nunca, funcionan al 100% de su capacidad, queda claro que fijar un umbral de admisión más alto para el tráfico prioritario no debería poner en peligro la integridad de la red ni la calidad de servicio de otro tipo de tráfico.

Hay sistemas de control de admisión basados en la reserva que permiten una petición de servicio únicamente cuando se ha aceptado la petición de anchura de banda necesaria. En este caso, los mecanismos de programación han de considerar la prioridad de servicio como factor fundamental.

Por último, también es posible utilizar medios para evitar los mecanismos de control de admisión (por ejemplo, el tráfico prioritario no se somete a la RACF). Ejemplo de ello es el mecanismo del protocolo de reserva de recursos que se describe en [b-IETF RFC RSVP].

8.1.3.1 Control de admisión de llamada (CAC, *call admission control*)

El CAC es un conjunto de acciones/políticas que toma la red en la fase de establecimiento de llamada/sesión para aceptar o rechazar un servicio en función de criterios de calidad de funcionamiento o de prioridad, y de la disponibilidad de los recursos necesarios.

En la RTPC/RDSI tradicional, el control de admisión de llamada simplemente implica que se otorgue o no un circuito en función de la autorización. Además, la atribución de un circuito por definición supone la disponibilidad del trayecto con la anchura de banda necesaria. Gracias a que se dispone de información sobre el estado de la red relativa a cada uno de los circuitos (canales en banda vocal) la RTPC/RDSI puede:

- a) desviar las llamadas de emergencia a trayectos específicamente reservados para el tráfico de emergencia (de haberlos);
- b) esperar que un circuito quede disponible (puesta en cola troncal).

Puesto que las redes IP no disponen de trayectos discretos o de información sobre el estado de los circuitos, la autenticación y la autorización en el ingreso de la red no pueden por sí mismas garantizar la disponibilidad de un trayecto de extremo a extremo o que haya suficiente anchura de banda de extremo a extremo para una determinada llamada/sesión. En una red IP, el elemento de red de ingreso tiene poco o ningún conocimiento de las condiciones en que se encuentra la red fuera de su dominio. Por consiguiente, el CAC en el elemento de red de ingreso no basta para garantizar la disponibilidad de un trayecto de extremo a extremo, a menos que se apliquen además otros mecanismos.

Por otra parte, el elemento de red de egreso no conoce ni tiene control sobre el elemento de red de ingreso distante, que puede estar intentando establecer una llamada/sesión hacia él. No obstante, en una RTPC/RDSI el elemento de red de egreso puede controlar un posible elemento de red de ingreso, que intente establecer una llamada/sesión, gracias a los mecanismos de señalización.

En [UIT-T Y.2171] se especifica la prioridad del control de admisión de los servicios de telecomunicaciones que intenten ingresar en una red en situaciones de emergencia cuando los recursos pueden estar agotados. En concreto, se recomiendan tres niveles de prioridad de control de admisión para los servicios que intenten ingresar en la NGN. El nivel de prioridad 1 (más elevado) está recomendado para las telecomunicaciones de emergencia (incluido el ETS) en la NGN. El tráfico con este nivel de prioridad tiene la más alta prioridad de admisión en la NGN.

8.2 Estrato de servicio

8.2.1 Generalidades

Los países ya tienen o están estableciendo un ETS para otorgar un tratamiento prioritario al tráfico autorizado en auxilio de las operaciones de socorro o en caso de emergencia dentro de las fronteras nacionales. Sin embargo, puede haber situaciones de crisis en que sea importante que un usuario del ETS de un país se comunique con los usuarios de otro país. En este caso, es fundamental que la llamada/sesión de ETS originada en un país reciba un tratamiento prioritario de extremo a extremo, es decir, un tratamiento prioritario en el país de origen y en el de destino. Para ello, se necesitará la interconexión de las dos implementaciones del ETS nacionales a través de una red internacional con capacidades de tratamiento prioritario o que transmita la prioridad de manera transparente entre los dos países.

En las siguientes cláusulas se presentan brevemente una serie de protocolos utilizados para señalar y obtener tratamiento prioritario en el nivel de control de servicio en el contexto de una NGN de paquetes. Se subraya asimismo la aplicabilidad específica de tales protocolos al ETS. Tales capacidades de protocolo se necesitan para las aplicaciones internacionales en el contexto de la comunicación entre implementaciones nacionales del ETS a través de la red internacional (por ejemplo, interconexión de dos implementaciones nacionales del ETS).

8.2.2 Prioridad de recursos SIP

En [IETF RFC 4412] se añaden a SIP dos campos encabezamiento, los campos prioridad de recursos y aceptar prioridad de recursos, y se especifican los procedimientos de utilización. El campo encabezamiento "Prioridad de recursos" pueden utilizarlo los agentes de usuario SIP, incluidas las pasarelas y terminales de la red telefónica pública conmutada (RTPC) y los servidores intermedios SIP para influir en el tratamiento que reciben las peticiones SIP.

A fin de establecer la equivalencia con algunos sistemas existentes, puede acomodarse la prioridad conveniente en diversos sistemas "normalizados" identificando el correspondiente "espacio de nombre" a cada sistema y al número de niveles de prioridad de tal sistema. En [IETF RFC 4412] se identifican los siguientes espacios de nombre y el número de niveles de prioridad asociado para su utilización en el ETS.

Espacio de nombre	Niveles
ets	5
wps	5

Todas las llamadas/sesiones del ETS en entornos IP se designan con un espacio de nombre "ets" con cinco niveles de prioridad que equivalen a niveles de importancia en la capa de aplicación (en los elementos SIP). A las llamadas/sesiones del ETS entrantes se les asigna una designación "ets" en el encabezamiento "Prioridad de recursos". Las llamadas/sesiones del ETS se reconocen por la presencia del espacio de nombre "ets" en el encabezamiento "Prioridad de recursos" en el mensaje SIP y se les concede la prioridad "Alta" para la reserva asignación de recursos de manera que reciban un trato preferente en la capa de transporte. También puede utilizarse el espacio de nombre "wps", acompañado de cinco niveles de prioridad, para la atribución de llamada/sesión cuando los recursos son limitados o están congestionados, como puede ocurrir en el acceso radioeléctrico a las redes inalámbricas.

8.2.3 Plan internacional de preferencias en situaciones de emergencia (IEPS, *international emergency preference scheme*)

En [UIT-T E.106] se describen los requisitos funcionales, las características, el acceso y la gestión operativa del IEPS, que permite la compatibilidad entre las diferentes implementaciones nacionales de los planes de prioridad/preferencias, otorgando así tratamiento preferente de extremo a extremo a las llamadas de voz y datos autorizadas en banda estrecha.

El alcance de [UIT-T E.106] se limita al contexto de la RTPC, la RDSI o la RMTP. El IEPS otorga el tratamiento prioritario del servicio de telefonía internacional para los usuarios autorizados en redes de telecomunicaciones con conexión. Por consiguiente, de acuerdo con los acuerdos bilaterales/multilaterales contraídos entre países/administraciones, el IEPS puede utilizarse en estos casos para la interconexión de implementaciones nacionales del ETS.

8.2.4 Protocolos de control de sistema H.323

En esta cláusula se presentan los protocolos utilizados por el sistema H.323 para el soporte de las telecomunicaciones prioritarias.

En [UIT-T H.460.4] se especifica la designación de prioridad de llamada y la identificación de país/red internacional de origen de una llamada para las llamadas prioritarias H.323. El parámetro designación de prioridad de llamada H.460.4 soporta tanto un indicador de llamada prioritaria como cinco niveles de prioridad.

En [UIT-T H.248.1] se definen los protocolos utilizados entre elementos de una pasarela multimedios físicamente descompuesta, utilizada de conformidad con la arquitectura especificada en [UIT-T H.323]. En el caso de servicios de emergencia autorizados por el gobierno (por ejemplo, ETS), [UIT-T H.248.1] define el indicador de llamada IEPS y el indicador de prioridad. El indicador de llamada IEPS transmite la indicación de prioridad entre el controlador y la pasarela. El indicador de prioridad transmite los niveles de prioridad entre el controlador y la pasarela y el indicador de prioridad H.248 soporta 16 niveles de prioridad. En el caso de los servicios de seguridad pública, [UIT-T H.248.1] define el indicador de emergencia para transmitir la indicación de prioridad entre el controlador y la pasarela.

8.3 Estrato de transporte

8.3.1 Generalidades

Es necesario llegar a acuerdos especiales (por ejemplo, acuerdos de nivel de servicio) para llevar a cabo ET en una NGN adecuadamente diseñada y dimensionada porque se supone que los recursos de red no son suficientes para la cantidad de tráfico que se ofrece a la red y que, en tales condiciones, el tráfico de telecomunicaciones de emergencia podría verse rechazado o muy retrasado y/o interrumpido hasta el punto de ser inviable o descartado. Cuando la cantidad de tráfico que recibe un modelo de servicio diseñado estadísticamente o sin garantías excede la capacidad de un elemento de red receptor dado (por ejemplo, un encaminador IP) y/o la capacidad saliente disponible de ese elemento, el único recurso que queda a dicho elemento es descartar el tráfico excedente, lo que implica que el tráfico de emergencia se descartará al mismo tiempo que el tráfico normal, a menos que se adopten medidas especiales para darle un trato preferente.

La sobreconfiguración es un técnica que, en ocasiones, se propone como solución, aunque puede a veces resultar imposible o inviable y, lo más importante, algunas emergencias puede estar causadas por la destrucción degradación deliberada o accidental de la red y eliminar así los trayectos o elementos sobreconfigurados que normalmente hubiesen estado disponibles. Por tanto, la sobreconfiguración tiene una repercusión negativa. Si una NGN ha de ser capaz de tratar todo tipo de emergencias en circunstancias adversas, será necesario disponer de los medios específicos para dar un tratamiento preferente al tráfico de telecomunicaciones de emergencia.

En las siguientes cláusulas se exponen algunos mecanismos utilizados para conseguir el tratamiento prioritario en el nivel de transporte en el contexto de una NGN de paquetes.

8.3.2 Control de anchura de banda mediante RSVP

Una de las características que puede tener una red IP capaz de establecer una (cierta) equivalencia con la atribución de anchura de banda basada en circuitos es un mecanismo IP para la atribución y reserva de anchura de banda. Este procedimiento está definido por el IETF en su protocolo de reserva de recursos (RSVP, *resource reservation protocol*), especificado en [IETF RFC 2205] y sus actualizaciones [b-IETF RFC 2750], [b-IETF RFC 3936] y [b-IETF RFC 4495].

La parametrización del control de recursos para el protocolo de inicio de sesión (SIP, *sesión initiation protocol*) en el estrato de servicio para utilizarla con el RSVP (en el estrato de transporte) se especifica en [IETF RFC 3312]. Se permite así la señalización RSVP antes, durante y/o intercalada con los procedimientos de señalización SIP. Pueden encontrarse algunos ejemplos en el apéndice A de [IETF RFC 4542]. No obstante, [IETF RFC 4542] utiliza la técnica de la preferencia.

En [b-IETF RFC RSVP] se especifican las extensiones de RSVP que se pueden emplear para soportar una capacidad de prioridad de admisión en la capa de transporte. Se especifican nuevas extensiones de RSVP para aumentar la probabilidad de completar una llamada sin preferencia. Las técnicas de capacidad diseñada, en forma de modelos de atribución de anchura de banda, se emplean para satisfacer la "prioridad de admisión" que necesita una red de telecomunicaciones de emergencia con RSVP. En concreto, en este documento se especifican dos nuevos elementos de política RSVP que permiten que la prioridad de admisión se transmita dentro de los mensajes de señalización RSVP, de manera que los nodos RSVP puedan aplicar las decisiones de control de admisión por anchura de banda selectiva basadas en la prioridad de admisión de llamada.

8.3.3 Control de puesta en cola mediante servicios diferenciados

En [IETF RFC 4594] se muestra la correspondencia recomendada entre clases de servicios y puntos de código de servicios diferenciados (DSCP). En la figura 3 de [IETF RFC 4594] se incluye una tabla de correspondencia que atribuye la clase retransmisión rápida a las aplicaciones de telefonía, lo que permite a los paquetes IP contener un valor DSCP atribuido a la clase retransmisión rápida.

Además, en [UIT-T Y.1541] también se recomienda que se marque (etiqueta) el tráfico vocal en los paquetes IP con el DSCP correspondiente a la EF. Los elementos de red (encaminadores) en estrato de transporte que reciban paquetes marcados EF garantizarán la entrega puntual de tráfico temporalmente crítico, con respecto al tráfico normal, empleando la retransmisión rápida definida para el punto de código EF y especificado en [IETF RFC 3246].

Sin embargo, el código EF se utiliza para el tráfico de telefonía normal, por lo que sigue siendo necesario diferenciar de alguna manera el tráfico de telefonía de emergencia y el tráfico de telefonía normal, como se indica en la siguiente cláusula.

8.3.4 EF DSCP para el tráfico admitido por capacidad

En [b-IETF RFC DSCP] se atribuye un EF DSCP al tráfico admitido por capacidad, lo que permitiría que el tráfico en tiempo real se conforme a la retransmisión rápida por saltos empleando un procedimiento CAC que conlleve autenticación, autorización y admisión de capacidad (véanse las cláusulas 8.3.1 y 8.3.2 anteriores) por oposición a la clase de tráfico en tiempo real conformada a la retransmisión rápida por saltos no sometida a la admisión de capacidad.

Se ha propuesto que el punto de código referido se denomine EF-ADMIT y que se le asigne un valor adecuado.

8.4 Acceso a la NGN

8.4.1 Generalidades

Hay diversas tecnologías de acceso a la NGN. De acuerdo con [UIT-T Y.2012], la red de acceso comprende funciones dependientes de la tecnología de acceso, por ejemplo, para la tecnología W-CDMA y el acceso xDSL. En función de la tecnología utilizada para acceder a los servicios de la NGN, la red de acceso comprende funciones relacionadas con:

- 1) Acceso por cable.
- 2) Acceso xDSL.
- 3) Acceso inalámbrico (por ejemplo, las tecnologías IEEE 802.11 y 802.16 y el acceso 3G RAN).
- 4) Acceso óptico.

Para soportar las telecomunicaciones de emergencia también se necesita aplicar medidas especiales en el segmento de acceso a la NGN. Tales medidas son necesarias puesto que se supone que, del mismo modo que los recursos de la red núcleo son limitados, también lo son los recursos de acceso. Por consiguiente, dependiendo de la cantidad de tráfico que se ofrece al segmento de la red de acceso, las telecomunicaciones de emergencia pueden verse afectadas (por ejemplo, rechazadas o muy retardadas y/o interrumpidas hasta llegar a no ser viables o que se descarten).

Por tanto, si la NGN ha de poder tratar todo tipo de emergencias en circunstancias adversas, es necesario que el segmento de acceso de la NGN disponga de medios específicos para otorgar un trato preferente al tráfico de telecomunicaciones de emergencia, lo que comprende, aunque no únicamente, mecanismos y capacidades para:

- Reconocer el tráfico de telecomunicaciones de emergencia.
- Dar acceso preferente/prioritario a los recursos/instalaciones.
- Realizar un encaminamiento preferente/prioritario del tráfico de telecomunicaciones de emergencia.
- Establecer de manera preferente/prioritaria sesiones/llamadas de telecomunicaciones de emergencia.

8.4.2 Acceso radioeléctrico inalámbrico

Las redes de acceso radioeléctrico inalámbricas han de poder soportar mecanismos y capacidades específicos para otorgar un tratamiento preferente/prioritario a las llamadas/sesiones de telecomunicaciones de emergencia autorizadas. Los mecanismos y capacidades propios de cada tecnología pueden utilizarse para otorgar dicho tratamiento, e incluyen, aunque no únicamente, mecanismos y capacidades para:

- Reconocer el tráfico de telecomunicaciones de emergencia, que comprende la identificación y marcación de las telecomunicaciones de emergencia autorizadas.
- Dar acceso preferente/prioritario a los recursos/instalaciones, lo que facilita la entrega de una petición de telecomunicaciones de emergencia a una NGN cuando los recursos de acceso disponibles son escasos.
- Realizar un encaminamiento preferente/prioritario del tráfico de telecomunicaciones de emergencia, lo que puede comprender características como la puesta en cola para los recursos disponibles, la exención de determinadas funciones de gestión de red restrictivas y la reserva de determinados caminos/trayectos para las telecomunicaciones de emergencia.
- Establecer de manera preferente/prioritaria las sesiones/llamadas de telecomunicaciones de emergencia.

Por ejemplo, el servicio de prioridad especificado para 3GPP y el servicio de prioridad multimedios para estos sistemas. El servicio de prioridad y el servicio de prioridad multimedios permiten a los usuarios autorizados obtener acceso prioritario al siguiente canal radioeléctrico (tráfico vocal o de datos) disponible antes que otros usuarios en caso de congestión que bloquee los intentos de llamada. El servicio de prioridad soporta la progresión y compleción de llamadas prioritarias a fin de realizar una llamada prioritaria "de extremo a extremo" en redes móvil a móvil, móvil a fijo y fijo a móvil. El servicio de prioridad multimedios soporta la progresión y compleción de sesiones multimedios para realizar sesiones multimedios prioritarias "de extremo a extremo" en redes móvil a móvil, móvil a fijo y fijo a móvil. El servicio de prioridad y el servicio de prioridad multimedios para los sistemas 3GPP se especifican en [b-3GPP TS 22.153].

Al igual que para 3GPP, existe un servicio de prioridad multimedios (MMPS, *multimedia priority service*) especificado para los sistemas 3GPP2, que se especifica en [b-3GPP2 S.R0117-0-v1.0].

8.4.3 Acceso fijo

Las redes de acceso fijo han de soportar mecanismos y capacidades específicos para otorgar un tratamiento preferente/prioritario a las llamadas/sesiones de telecomunicaciones de emergencia autorizadas. Pueden utilizarse mecanismos y capacidades específicos de cada tecnología (por ejemplo, 802.1p con xDSL, IPCablecom, Packet Cable 2) para garantizar este tratamiento preferente/prioritario, que comprende, aunque no únicamente, mecanismos y capacidades para:

- Reconocer el tráfico de telecomunicaciones de emergencia, que incluye la identificación y marcación de las telecomunicaciones de emergencia autorizadas.
- Dar acceso preferente/prioritario a los recursos/instalaciones, facilitando así la entrega de una petición de telecomunicaciones de emergencia a una NGN cuando los recursos de acceso disponibles son escasos.
- Realizar un encaminamiento preferente/prioritario del tráfico de telecomunicaciones de emergencia, que puede comprender características tales como la puesta en cola para los recursos disponibles, la exención de determinadas funciones de gestión de la red restrictivas y la reserva de caminos/trayectos para las telecomunicaciones de emergencia.
- Establecer de manera preferente/prioritaria llamadas/sesiones de telecomunicaciones de emergencia.

Por ejemplo, en [UIT-T J.260] se definen requisitos para las telecomunicaciones preferentes en redes IPCablecom. Los aspectos fundamentales de las telecomunicaciones preferentes en redes IPCablecom definidos en [UIT-T J.260] se agrupan entorno a dos conceptos: establecimiento de prioridades y autenticación. Estos dos conceptos comprenden capacidades para el soporte en IPCablecom de telecomunicaciones que pueden necesitar un trato preferente (por ejemplo TDR y ETS). Es necesario establecer prioridades y efectuar la autenticación para soportar las telecomunicaciones preferentes en las redes IPCablecom.

9 Mecanismos y capacidades que soportan algunos aspectos de la alerta temprana en las NGN

9.1 Generalidades

Los sistemas de alerta utilizados para la alerta temprana pueden clasificarse en modelos activos y pasivos.

El modelo activo se basa en que los participantes registren su información de contacto (por ejemplo una dirección de correo electrónico) ante un servicio central. En caso de emergencia, se alerta a los participantes registrados y posiblemente se les comunica más información sobre lo ocurrido. La característica clave de la arquitectura de este modelo es que la autoridad central determina si la información ha de divulgarse y lo que conlleva. Su fuerza reside en que asume la responsabilidad de

vigilar activamente la ocurrencia de situaciones de emergencia y deja que los usuarios lleven a cabo normalmente sus actividades y no estén encargados de la vigilancia de posibles catástrofes o emergencias.

El modelo activo es un mecanismo de distribución de "uno" a "muchos" y está activado tanto en el estrato de servicio como en el de transporte (por ejemplo, multidifusión).

El modelo pasivo es lo contrario del modelo activo, pues se basa en un intercambio de información en forma de pregunta-respuesta. Si bien ambos modelos requieren el registro de cada participante, el modelo pasivo descarga la responsabilidad de vigilancia y obtención de información en los usuarios. La ventaja de este sistema es que la información sólo se facilita cuando se necesita o solicita.

En resumen, los sistemas de alerta utilizan las aplicaciones existentes y capacidades subyacentes de las redes IP. Que sean activos o pasivos hacen que los sistemas sean más simbióticos con las necesidades y expectativas de los usuarios. Estos sistemas de alerta también pueden utilizarse combinados: el sistema activo puede efectuar una vigilancia y notificación automáticas periódicamente y el modelo pasivo puede emplearse para obtener información específica cuando se necesita.

Pueden encontrarse ejemplos de modelos activos y pasivos en el apéndice II.

9.2 Protocolo de alerta común (CAP, *common alerting protocol*)

En esta cláusula se describe el protocolo de alerta común (CAP) especificado en [UIT-T X.1303] que puede utilizarse para el soporte de aplicaciones de alerta temprana.

En [UIT-T X.1303] se especifica un formato general para el intercambio de alertas de todo tipo de emergencias y de alertas públicas en cualquier red. El CAP permite que un mensaje de alerta coherente se transmita simultáneamente a muy diversos sistemas de alerta, incrementando así su eficacia y simplificando al mismo tiempo la tarea. El CAP facilita asimismo la detección de patrones de emergencia en alertas locales de varios tipos, como las que pueden indicar un peligro indeterminado o un acto hostil. El CAP también dispone de un modelo de mensajes de alerta efectivos basado en las prácticas idóneas determinadas por la investigación y la experiencia real.

El CAP proporciona un formato de mensaje abierto y general para todo tipo de alertas y notificaciones. No se dirige a una aplicación o método de telecomunicaciones en concreto. El formato CAP es compatible con las nuevas técnicas, como los servicios web y los servicios rápidos web del UIT-T, además de con los formatos existentes, incluida la codificación de mensaje específica de la zona (SAME, *specific area message encoding*) utilizado por las Radiocomunicaciones Meteorológicas de la Administración Nacional del Océano y la Atmósfera (NOAA, *National Oceanic and Atmospheric Administration*) de Estados Unidos y por el Sistema de Alerta de Emergencia (EAS, *Emergency Alert System*), al tiempo que ofrece capacidades mejoradas que comprenden:

- determinación geográfica flexible por latitud/longitud y otras representaciones geoespaciales en tres dimensiones;
- mensajería multilingüe y multidestinataria;
- plazos y expiraciones en fases y con retardo efectivo;
- actualización y cancelación de mensajes mejorados;
- modelo para mensajes de alerta efectivos y completos;
- compatibilidad con la encriptación y la firma digitales; y
- capacidad para imágenes y audio digitales.

Con el CAP se reducen los costos y la complejidad operativa al eliminar la necesidad de disponer de numerosas interfaces adaptadas a las diversas fuentes de alerta y sistemas de divulgación que participan en el proceso de alerta. El formato de mensaje CAP puede convertirse desde y hacia los formatos "nativos" de todas las tecnologías de detección y alerta, erigiéndose así como base para el "Internet para alerta" nacional e internacional sea cual sea la tecnología utilizada.

El CAP especificado en [UIT-T X.1303] es técnicamente equivalente y compatible con el protocolo de alerta común OASIS V1.1. En [UIT-T X.1303] se presenta una especificación en ASN.1 equivalente que permite la codificación binaria compacta y la utilización de las herramientas ASN.1 y de definición de esquema XML (XSD, *XML schema definition*) para la generación y procesamiento de mensajes CAP. En [UIT-T X.1303] se permite la utilización de los sistemas existentes, como los sistemas H.323, para codificar, transportar y descodificar más fácilmente los mensajes CAP.

10 Prioridad de restauración del servicio

En caso de fallo o caída de la red, es posible que se interrumpan los servicios críticos (por ejemplo, los servicios de emergencia), que necesitarán una más alta probabilidad de restauración que el resto de servicios. En [UIT-T Y.2172] se especifican tres niveles de prioridad para la restauración de los servicios en las NGN. Se prevé que tal clasificación de prioridad se emplee en los mensajes de señalización de manera que el servicio en cuestión pueda establecer llamadas/sesiones con el grado de prioridad deseado, permitiendo así que los servicios críticos tengan una mayor probabilidad de ser restaurados que los demás servicios.

11 Seguridad

Los elementos de red, sistemas, recursos, datos y servicios utilizados para las telecomunicaciones de emergencia pueden ser objeto de ciberataques. La integridad, confidencialidad y disponibilidad de las telecomunicaciones de emergencia, especialmente cuando estén siendo atacadas, dependerá de los servicios y prácticas de seguridad de las NGN y de las capacidades de seguridad (por ejemplo, funciones de autenticación y autorización de usuarios) que formen parte del servicio de aplicación para las telecomunicaciones de emergencia. A continuación se presenta una lista no exhaustiva de elementos que es necesario tener en cuenta a la hora de planificar la seguridad de las telecomunicaciones de emergencia:

- Todos los aspectos de las telecomunicaciones de emergencia, incluidos la señalización y el control, la portadora/medios y los datos e informaciones relacionados con la gestión (por ejemplo, la información de perfil de usuario) han de estar protegidos contra las amenazas de seguridad. Las telecomunicaciones de emergencia pueden verse amenazadas en las diversas capas (por ejemplo, transporte, control de servicio o soporte de servicio) y en los distintos segmentos de la red (es decir, acceso, red núcleo e interfaces de conexión).
- Establecimiento y aplicación de políticas y prácticas de seguridad específicas para los servicios de telecomunicaciones de emergencia. Habrán de identificarse y ponerse en marcha capacidades de reducción que den protección contra diversas amenazas de seguridad. En concreto, habrán de identificarse y aplicarse al caso de las telecomunicaciones de emergencia capacidades de reducción y prácticas de seguridad más importantes que las necesarias para los servicios de aplicación en general. Esto incluye políticas de seguridad para proteger los datos de gestión y la información almacenada (por ejemplo, información de perfil de usuario) relacionados con las telecomunicaciones de emergencia.
- Implantación y utilización de procedimientos para autenticar y autorizar a los usuarios, los dispositivos, o combinaciones de ambos, para evitar el acceso no autorizado a los servicios, los recursos y la información (por ejemplo, información de usuario en los servidores de autenticación y los sistemas de gestión) asociados con las telecomunicaciones de

emergencia. Por ejemplo, las funciones de autenticación y autorización han de emplearse para evitar que usuarios no autorizados accedan a recursos dedicados a las telecomunicaciones de emergencia a fin de evitar los ataques de denegación de servicio o de otro tipo.

- Cada red será responsable de la seguridad en su dominio en el caso de las comunicaciones que atraviesan diversos dominios de proveedor de red, de manera que se aseguren las comunicaciones de extremo a extremo. Dado que las telecomunicaciones de emergencia pueden conllevar comunicaciones que atraviesan diversos dominios de proveedor de red de redes nacionales e internacionales (es decir, de países/administraciones), la política de seguridad, las relaciones de confianza, los métodos y procedimientos de identificación del tráfico de telecomunicaciones de emergencia, la gestión de identidad y la autenticación de usuarios y redes a través de múltiples dominios administrativos de la red necesitan la implantación y utilización de estas capacidades.

A la hora de planificar la seguridad de las telecomunicaciones de emergencia habrán de tenerse en cuenta las recomendaciones de [UIT-T Y.2701] para la seguridad de las NGN. Además, habrá de considerarse también el marco de seguridad, definido en [UIT-T X.805], basado en las siguientes dimensiones de seguridad:

- Control de acceso.
- Autenticación.
- No repudio.
- Confidencialidad de los datos.
- Seguridad de las comunicaciones.
- Integridad de los datos.
- Disponibilidad.
- Privacidad.

Apéndice I

Categorías de telecomunicaciones de emergencia

(Este apéndice no forma parte integrante de esta Recomendación)

I.1 Telecomunicaciones de emergencia individuo-autoridad

Las telecomunicaciones de emergencia individuo-autoridad las inicia una persona empleando capacidades de telecomunicaciones de emergencia nacionales ordinarias para pedir asistencia de emergencia en caso de emergencia personal o en caso de situación de emergencia de dimensiones reducidas. Por ejemplo, una llamada individuo-autoridad puede consistir en llamar a un número corto (por ejemplo, 112, 911, etc.) que pone al individuo en conexión con un centro de respuesta ante emergencias. Este centro se pondrá en contacto con las entidades correspondientes (por ejemplo, policía, bomberos, ambulancias) en nombre del llamante. Es posible que se señale al centro de llamadas automáticamente otra información, como la ubicación del llamante. Esta información puede propiciar que la reacción sea aún más rápida, pues en ocasiones los llamantes no pueden o no disponen del tiempo o la capacidad de facilitar esta información por sí mismos. Este tipo de comunicación suele ser una conexión uno a uno, donde el iniciador entabla la interacción con el organismo de destino. La amplia mayoría de telecomunicaciones de este tipo se harán en caso de emergencias a pequeña escala (por ejemplo, incendio de la casa de la persona) y estarán originadas por acontecimientos no relacionados unos con otros, aunque es posible que las catástrofes más grandes (por ejemplo, un terremoto), dé como resultado muchas conexiones simultáneas relacionadas. (El término individuo ha de entenderse en sentido amplio y abarcar a toda persona que necesite asistencia de emergencia (por persona se entiende ciudadano, visitante o habitante de un lugar concreto)). Los participantes en las telecomunicaciones de emergencia puede comunicarse mutuamente utilizando múltiples tipos de medios, como la voz, el vídeo el texto en tiempo real y la mensajería instantánea.

I.2 Telecomunicaciones de emergencia individuo-individuo

Las telecomunicaciones de emergencia individuo-individuo las inicia una persona o dispositivo cualesquiera hacia una organización. Por ejemplo, durante e inmediatamente después de una situación de emergencia, las personas sienten una gran necesidad de comunicarse con sus seres queridos. Por consiguiente, hay una gran demanda de telecomunicaciones individuo-individuo al mismo tiempo y los recursos de telecomunicaciones pueden verse reducidos por los daños causados por la catástrofe en cuestión. Si se tienen en cuenta todos estos factores, las redes de telecomunicaciones pueden congestionarse.

I.3 Telecomunicaciones de emergencia autoridad-autoridad

En las telecomunicaciones de emergencia autoridad-autoridad participa un usuario de telecomunicaciones de emergencia autorizado (o su organización) que inicia la comunicación con otro usuario autorizado para:

- 1) facilitar las operaciones de recuperación en caso de emergencia (por ejemplo, creando centros de control de emergencias y los controles administrativos conexos para obtener asistencia del gobierno y/u otras organizaciones);
- 2) restaurar la infraestructura comunitaria esencial (por ejemplo, agua corriente, electricidad, etc.); y
- 3) adoptar las primeras medidas que permitan la recuperación a largo plazo (por ejemplo, reconstrucción de carreteras, puentes, edificios, etc.).

Históricamente, las telecomunicaciones de emergencia autoridad-autoridad (denominadas a veces telecomunicaciones de seguridad pública) a través de las redes públicas suelen darse simultáneamente cuando los recursos de telecomunicaciones están congestionados por un aumento de las telecomunicaciones individuo-individuo.

Dado el inmenso potencial de las telecomunicaciones de emergencia autoridad-autoridad para facilitar la restauración de la normalidad y evitar más riesgos personales o materiales, esta categoría tendrá prioridad sobre las demás categorías de telecomunicaciones de emergencia cuando se declaren estados de emergencia o haya una degradación de la situación.

I.4 Telecomunicaciones de emergencia autoridad-individuo

Por ultimo, las telecomunicaciones de emergencia autoridad-individuo (que, en ocasiones, entran dentro de la categoría de sistemas de telecomunicaciones de alerta (temprana)) suelen conllevar información para el público procedente de una fuente autorizada. El contenido puede ser información dirigida a una comunidad afectada por una catástrofe, y puede ser relativa a la seguridad, instrucciones, orientaciones, consejos, etc. Por norma general, la telecomunicación la inicia un usuario autorizado y está dirigida a muchos individuos receptores.

N-N: por ejemplo, un ETS desde cualquier ubicación/dispositivo que contacta con cualquier otro usuario (ETS o público general) gracias a la preferencia soportada por la infraestructura de telecomunicaciones. El servicio universal de telemedicina de urgencias (GETS) a través de la RTPC es un buen ejemplo de servicio preferente no ubicuo y no restringido a un conjunto selectivo de dispositivos extremos o destinos.

Uno-uno: en el contexto de las telecomunicaciones de emergencia, uno-uno se considera un subconjunto de caso N-N. En este caso, los participantes se reducen a dos usuarios del ETS cualesquiera.

Muchos-uno: una manifestación de este modelo es una arquitectura cliente-servidor de la web, donde cualquier usuario accede a una única ubicación bien conocida para obtener la información. En la RTPC, este modelo se materializa en los sistemas 11, 112, etc., donde las sesiones dentro de una región se reenvían a un único punto de acceso de servicio público (PSAP, *public service access point*).

Uno-muchos: en este modelo, la información se envía desde una fuente a una serie de receptores (usuarios extremos) que quieren participar en la divulgación de los datos. En el caso de los medios de comunicación, la televisión y la radio son excelentes ejemplos, pues los receptores sólo obtienen información a través del canal seleccionado. En el modelo de comunicación de datos, uno-muchos se distingue de la radiocomunicación al implicar esta última que todos los nodos reciben el mensaje, quieran o no, mientras que uno-muchos conlleva que la pertenencia de los miembros a un grupo.

Apéndice II

Ejemplos prácticos de sistemas de alerta temprana

(Este apéndice no forma parte integrante de esta Recomendación)

II.1 Modelo activo

Tanto el sector privado como el público/estatal ofrecen sistemas de alerta basados en el modelo activo. No obstante, esta Recomendación presenta sólo un ejemplo del sector público. Un ejemplo de modelo activo del sector público/estatal es el centro de información de emergencias (<http://alert.dc.gov/eic/site/default.asp>) del gobierno local de Washington D.C. Los usuarios se registran y dan una dirección de contacto, dirección de correo electrónico, número de buscapersonas o de teléfono móvil (para recibir mensajes de texto o mensajes vocales automáticos). La mensajería vocal automática equivale al servicio 911 al revés y todos los ciudadanos del D.C. que dispongan de línea fija están automáticamente registrados para recibir este servicio. El servicio de alerta, al efectuarse por correo electrónico y buscapersonas, no está limitado a los residentes en Washington D.C.

II.2 Modelo pasivo

El mejor ejemplo del modelo pasivo en Internet es el proyecto I-AM-Alive de Japón (http://www.isoc.org/inet2000/cdproceedings/81/81_3.htm, <http://www.iaa-alliance.net/en/>). La idea de I-AM-Alive surgió a partir del terremoto de Kobe de 1995 para permitir a la población determinar la situación y posible emplazamiento de sus seres queridos, afectados por el terremoto. Funciona como un centro de recopilación de información donde los usuarios depositan toda la información conocida. Al mismo tiempo funciona como un centro de distribución donde amigos y parientes pueden saber si alguno de sus conocidos se ha visto afectado por la catástrofe.

El sistema I-AM-Alive utiliza una combinación de datos recibidos por fax, teléfono y la web para almacenar la información comunicada por los particulares y los servicios de socorro. A continuación, la información se divulga principalmente en páginas web y a partir de números de teléfono bien conocidos asociados al sistema.

Bibliografía

- [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] Naciones Unidas/Estrategia Internacional de Reducción de Desastres, Informe Final sobre "*Estudio mundial sobre los sistemas de alerta temprana*", septiembre de 2006. (Referencia: <http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf>)

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación