Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2205

(05/2011)

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 basadas en paquetes	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
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999

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 se especifican los aspectos técnicos que pueden incorporarse, de manera facultativa, en las redes de la próxima generación (NGN) para habilitar las telecomunicaciones de emergencia (ET). Se presentan asimismo los principios técnicos subyacentes para dar soporte a las ET.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T Y.2205	2008-09-12	13
2.0	ITU-T Y.2205	2011-05-20	13

Palabras clave

Alerta temprana (EW), arquitectura, calidad de servicio (QoS), NGN, servicio de telecomunicaciones de emergencia (STE), telecomunicaciones de emergencia, telecomunicaciones para operaciones de socorro (TDR), telecomunicaciones prioritarias.

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 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/.

ÍNDICE

Página

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. Se les debe conferir a las telecomunicaciones de emergencia un trato prioritario con respecto a los servicios normales de la red pública. La expresión telecomunicaciones prioritarias se utiliza en algunas Recomendaciones UIT-T para incluir servicios que exigen un trato prioritario. El servicio de telecomunicaciones de emergencia es una categoría de servicios que se considera necesita trato prioritario. Las expresiones telecomunicaciones prioritarias y telecomunicaciones de emergencia se utilizan indistintamente.

Las telecomunicaciones prioritarias utilizadas en situaciones de emergencia no son nuevas: las redes con conmutación de circuitos admiten dichos sistemas desde hace años, principalmente para llamadas vocales (por ejemplo, [UIT-T E.106]). Sin embargo, los métodos técnicos utilizados para soportar esos requisitos subyacentes de telecomunicaciones de emergencia en el entorno de las NGN van evolucionando. En las NGN no se aplican forzosamente los métodos prioritarios tradicionales con conmutación de circuitos debido a las diferencias inherentes entre las telecomunicaciones con conmutación de circuitos y las telecomunicaciones con conmutación de paquetes.

En la Recomendación [UIT-T Y.1271] se describen los requisitos y capacidades en términos generales y abstractos; dicha Recomendación es neutral desde el punto de vista 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) con el fin de 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 del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

2.1 UIT-T

[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 G.808.1] Recomendación UIT-T G.808.1 (2010), *Conmutación de protección genérica – Protección lineal de camino y de subred*.

[UIT-T G.841] Recomendación UIT-T G.841 (1998), *Tipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona*.

[UIT-T G.842] Recomendación UIT-T G.842 (1997), *Interfuncionamiento de las arquitecturas de protección para redes de la jerarquía digital síncrona*.

[UIT-T G.873.1] Recomendación UIT-T G.873.1 (2006), *Red óptica de transporte: Protección lineal*.

[UIT-T G.983.1] Recomendación UIT-T G.983.1 (2005), *Sistemas de acceso óptico de banda ancha basados en redes ópticas pasivas*.

[UIT-T G.8031] Recomendación UIT-T G.8031/Y.1342 (2009), *Conmutación de protección lineal Ethernet*.

[UIT-T G.8032] Recomendación UIT-T G.8032/Y.1344 (2010), *Conmutación de protección del anillo Ethernet*.

[UIT-T G.8131] Recomendación UIT-T G.8131/Y.1382 (2007), *Conmutación lineal de protección para las redes MPLS de transporte*.

[UIT-T H.248.1] Recomendación UIT-T H.248.1 (2005), *Protocolo de control de las pasarelas: Versión 3*.

[UIT-T H.248.81] Recomendación UIT-T H.248.81 (2011), *Protocolo de control de pasarelas: Directrices sobre la utilización del indicador de llamada e indicador de prioridad del plan internacional de preferencias en situaciones de emergencia (IEPS) en perfiles UIT-T H.248*.

[UIT-T H.323] Recomendación UIT-T H.323 (2009), *Sistemas de comunicación multimedia basados en paquetes.*

[UIT-T H.460.4] Recomendación UIT-T H.460.4 (2007), *Designación de prioridades de llamada e identificación la red nacional/internacional de origen de llamada para llamadas prioritarias H.323*.

[UIT-T I.630] Recomendación UIT-T I.630 (1999), *Conmutación de protección del modo de transferencia asíncrono*.

[UIT-T J.260] Recomendación UIT-T J.260 (2005), *Requisitos aplicables a las telecomunicaciones preferentes en redes IPCablecom*.

[UIT-T J.261] Recomendación UIT-T J.261, (2009), *Marco para la prestación de servicios de telecomunicaciones preferentes en redes IPCablecom e IPCablecom2*.

[UIT-T J.262] Recomendación UIT-T J.262 (2009), *Especificaciones para la autentificación en las telecomunicaciones preferentes por redes IPCablecom2*.

[UIT-T J.263] Recomendación UIT-T J.263 (2009), *Especificación de la prioridad en los servicios de telecomunicaciones preferentes por redes IPCablecom2*.

[UIT-T Q.812] Recomendación UIT-T Q.812 (2004), *Perfiles de protocolo de capa superior para las interfaces Q y X*.

[UIT-T Q.1741.6] Recomendación UIT-T Q.1741.6 (2009), *Referencias de las IMT-2000 a la versión 8 de la red medular del sistema de telecomunicaciones móviles universales derivada del sistema global para comunicaciones móviles*.

[UIT-T Q.3303.3] Recomendación UIT-T Q.3303.3 (2008), *Protocolo de control de recursos N.° 3 – Protocolos en la interfaz Rw entre la entidad física de decisión de política (PD-PE) y la entidad física de cumplimiento de política (PE-PE): Diámetro*.

[UIT-T Q.3321.1] Recomendación UIT-T Q.3321.1 (2010), *Protocolo de control de recursos N.° 1, versión 2 – Protocolo en la interfaz Rs entre las entidades de control de servicio y la entidad física de decisión política.*

[UIT-T Q-Sup.57] Suplemento 57 a las Recomendaciones UIT-T de la serie Q – *Requisitos de señalización para el soporte del servicio de telecomunicaciones de emergencia (ETS) en las redes IP.*

[UIT-T X.660] Recomendación UIT-T X.660 (2008) | ISO/CEI 9834-1:2008, *Tecnología de la información – Interconexión de sistemas abiertos – Procedimientos para la operación de autoridades de registro para interconexión de sistemas abiertos: Procedimientos generales y arcos superiores del árbol de identificadores de objetos*.

[UIT-T X.674] Recomendación UIT-T X.674 (2011), *Procedimientos para el registro de arcos dentro del arco de aviso de identificador de objeto*.

[UIT-T X.1303] Recomendación UIT-T X.1303 (2007), *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.1720] Recomendación UIT-T Y.1720 (2006), *Conmutación de protección para redes con conmutación por etiquetas multiprotocolo*.

[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 y arquitectura funcional de las redes de la próxima generación, versión 1*.

[UIT-T Y.2111] Recomendación UIT-T Y.2111 (2008), *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 de control de admisión en las redes de la próxima generación.*

[UIT-T Y.2172] Recomendación UIT-T Y.2172, (2007), *Niveles de prioridad de restablecimiento del servicio en las redes de próxima generación*.

[UIT-T Y.2201] Recomendación UIT-T Y.2201 (2009), *Requisitos y capacidades de las NGN del UIT-T*.

[UIT-T Y.2701] Recomendación UIT-T Y.2701 (2007), *Requisitos de seguridad para las redes de la próxima generación, Versión 1*.

[UIT-T Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autentificación y autorización para las NGN, Versión 1*.

[UIT-T Y.2704] Recomendación UIT-T Y.2704 (2010), *Mecanismos y procedimientos de seguridad para las NGN*.

[UIT-T Y.2720] Recomendación UIT-T Y.2720 (2009), *Marco general para la gestión de identidades en las redes de la próxima generación*.

[UIT-T Y.2721] Recomendación UIT-T Y.2721 (2010), *Requisitos de la gestión de identidades NGN y ejemplos de utilización*.

[UIT-T Y.2722] Recomendación UIT-T Y.2722 (2011), *Mecanismos de gestión de identidad en las NGN.*

2.2 IETF

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

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

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

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

[IETF RFC 3312] IETF RFC 3312, (2002), *Integration of Resource Management and Session Initiation Protocol (SIP)*.

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

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

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

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

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

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

2.3 ETSI

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

2.4 Broadband Forum

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

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

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

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 alerta (*alert*) [UIT-T X.674]: Mensaje de alerta o alarma respecto de un problema o peligro inminente.

3.1.2 organismo responsable de alertar (*alerting agency*) [UIT-T X.674]: Entidad nacional, regional o internacional responsable de la gestión de alertas.

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

3.1.4 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.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 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.

3.2.2 telecomunicaciones prioritarias (*preferential telecommunications*): Categoría de servicios a los que se les proporciona acceso prioritario a los recursos de la red de telecomunicaciones y/o que utilizan dichos recursos con carácter prioritario.

3.3 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 y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas:

AAA Autentificación, autorización y contabilidad (*authentication, authorization, and accounting*)

AF Función de aplicación (*application function*)

ANMS Sistema de gestión de nodo de acceso (*access node management system*)

APS Conmutación de protección automática (*automatic protection switching*)

AQM Gestión activa de cola (*active queue management*)

ASN Red de servicio de acceso (*access service network*)

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

BNG Pasarela de red de banda ancha (*broadband network gateway*)

BS Estación de base (*base station*)

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

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

CPE Equipo en los locales del cliente (*customer premises equipment*)

DCCP Protocolo de control de gestión de datos (*data congestion control protocol*)

DoS Denegación de servicio (*denial of service*)

DSCP Punto de código de servicio diferenciado (*diff-serv code points*)

DSLAM Multiplexor de acceso de línea de abonado digital (*digital subscriber line access multiplexer*)

EAS Sistema de alerta de emergencia (*emergency alert system*)

ECN Notificación de congestión explícita (*explicit congestion notification*)

EF Retransmisión rápida (*expedited forwarding*)

E-MTA Adaptador multiterminal incorporado (*embedded muti-terminal adapter*)

ENI Implementación nacional del STE (*ETS national implementation*)

ET Telecomunicaciones de emergencia (*emergency telecommunications*)

ETH Red de capa Ethernet (*Ethernet layer network*)

STE Servicio de telecomunicaciones de emergencia (*emergency telecommunications service*)

EW Alerta temprana (*early warning*)

GETS Servicio público de telecomunicaciones de emergencia (*government emergency telecommunications service*)

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

IP Protocolo Internet (*Internet protocol*)

LAN Red de área local (*local area network*)

LSP Trayecto con conmutación por etiquetas (*label switched path*)

MDF Trama de distribución principal (*main distribution frame*)

MMPS Servicio prioritario multimedios (*multimedia priority service*)

MPS Servicio prioritario multimedios (*multimedia priority service*)

MPLS Conmutación por etiquetas multiprotocolo (*multiprotocol label switching*)

MS Sección múltiplex (*multiplex section*)

NGN Red de la próxima generación (*next generation network*)

NID Dispositivo de interfaz de red (*network interface device*)

NOAA Administración Nacional del Océano y la Atmósfera (*National Oceanic and Atmospheric Administration*)

ODUk Unidad de datos k del canal óptico (*optical channel data unit k*)

OLT Terminación de línea óptica (*optical line termination*)

OMCI Interfaz de gestión y control ONT (*ONT management and control interface*)

ONT Terminación de red óptica (*optical network termination*)

OTN Red de transporte óptica (*optical transport network*)

PCC Control de tasación y política (*policy and charging control*)

P-CSC-FE Entidad funcional de control de sesión/llamada apoderada (*proxy call session control functional entity*)

PDP Punto de decisión de política (*policy decision point*)

PEP Punto de observancia de política (*policy enforcement point*)

PF Función de política (*policy function*)

PHB Comportamiento por salto (*per hop behaviour*)

PIN Número de identificación personal (*personal identification number*)

PLMN Red móvil terrestre pública (*public land mobile network*)

PON Red óptica pasiva (*passive optical network*)

POTS Servicio telefónico tradicional (*plain old telephone service*)

PSAP Punto de respuesta de seguridad pública (*public safety answering point*)

QoS Calidad de servicio (*quality of service*)

RACF Función de control de admisión y recursos (*resource and admission control function*)

RDSI Red digital de servicios integrados (*integrated services digital network*)

RPH Encabezamiento de prioridad de recursos (*resource priority header*)

RSVP Protocolo de reserva de recursos (*resource reservation protocol*)

RTPC Red telefónica pública conmutada (*public switched telephone network*)

SAME Codificación de mensajes específica de la zona (*specific area message encoding*)

SCF Función de control de servicio (*service control function*)

SDH Jerarquía digital síncrona (*synchronous digital hierarchy*)

SIP Protocolo de iniciación de sesión (*session initiation protocol*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

SNC Conexión de subred (*subnetwork connection*)

SNCP Protección de conexión de subred (*subnetwork connection protection*)

SS7 Sistema de señalización N.° 7 (*signalling system No. 7*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TDM Multiplexación por división en el tiempo (*time division multiplexing*)

TDR Telecomunicaciones para operaciones de socorro (*telecommunications for disaster relief*)

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

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

UE Equipo de usuario (*user equipment*)

UN/ISDR Estrategia Internacional de las Naciones Unidas para la Reducción de Catástrofes (*United Nations International Strategy for Disaster Reduction*)

USI Interfaz universal de servicios (*universal services interface*)

VC Canal virtual (*virtual channel*)

VLAN LAN virtual (*virtual LAN*)

VoIP Transmisión de voz por IP (*voice over IP*)

VP Trayecto virtual (*virtual path*)

W-CDMA Acceso múltiple por división de código de banda ancha (*wideband code division multiple access*)

WPS Servicio de prioridad inalámbrico (*wireless priority service*)

xDSL Cualquier variante de línea de abonado digital (*any variant of digital subscriber line*)

XML Lenguaje de marcación extensible (*extensible markup language*)

XSD Definición de esquema SML (*XML schema definition*)

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:

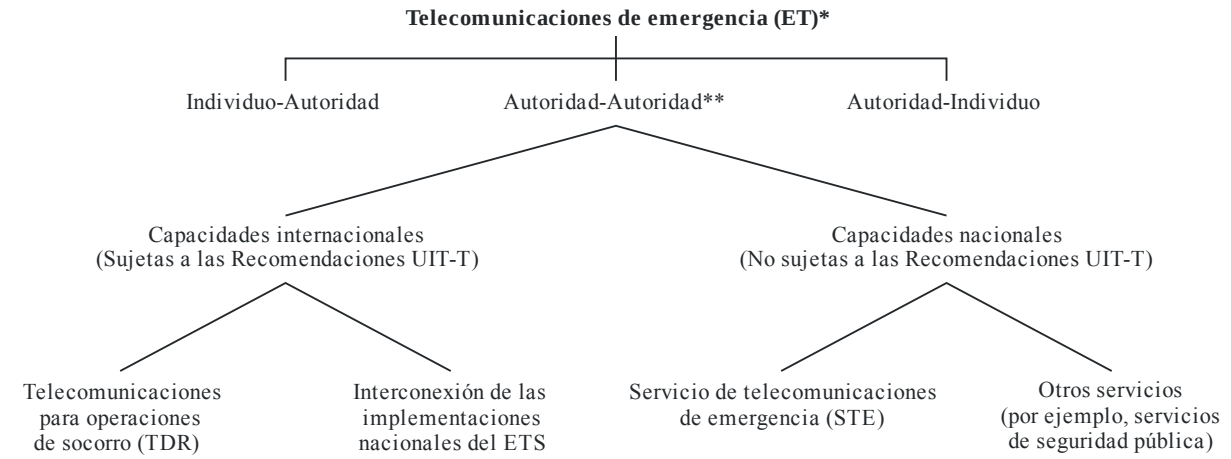
- Telecomunicaciones de emergencia — ET (*emergency telecommunications*)
- Servicio de telecomunicaciones de emergencia — STE (*emergency telecommunications service*)
- Telecomunicaciones para operaciones de socorro — TDR (*telecommunications for disaster relief*)
- Alerta temprana — EW (*early warning*)

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.
- STE: 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.

Tal como se indicó en la introducción, en algunas Recomendaciones, concretamente de la serie J.26x, se utiliza el término telecomunicaciones prioritarias para incluir servicios que requieren un tratamiento especial en comparación con otros. Salvo en el contexto de las Recomendaciones de la serie J.26x, en esta Recomendación no se hace referencia a las telecomunicaciones prioritarias. En la serie J.26x el término telecomunicaciones prioritarias incluye STE, TDR y EW.



* Incluidos algunos aspectos de la alerta temprana.
** Puede también aplicarse a las telecomunicaciones autoridad-individuo.

Y.2205(11)_F01

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 (STE)

   El STE es un servicio nacional que proporciona telecomunicaciones prioritarias a los usuarios autorizados del STE en caso de catástrofe o en situación de emergencia. Puede encontrarse una descripción del STE en [UIT-T E.107]. En [UIT-T E.107] se dan orientaciones para permitir las telecomunicaciones entre una implementación nacional del STE (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 (ONU/EIRD), en su Informe de septiembre de 2006 [b-UN Global Survey] 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 y 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. Sin embargo, al considerar los protocolos, mecanismos y soporte relativos a las telecomunicaciones de emergencia,

conviene tratar de no introducir características o requisitos que, pese a ser útiles, pueden agravar la complejidad sin aportar un beneficio apreciable. Es preciso actuar con cautela y tener en cuenta los gastos generales que supone el consumo de recursos y otros efectos antes de incorporar por ejemplo nuevas características a título de "prioridad".

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 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 [b-UN Global Survey].

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 [UIT-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).

Las funciones de red específicas de las telecomunicaciones de emergencia pueden dividirse en las siguientes categorías: invocación de servicio, autentificación y autorización, trato prioritario de extremo a extremo, interconexión de red e interfuncionamiento de protocolos.

Una invocación de servicio se refiere a la interacción del usuario con el elemento de usuario (por ejemplo, el teléfono) y la red con información que indica una solicitud de servicio de telecomunicaciones de emergencia para la red del proveedor de servicio. Hay diferentes enfoques, incluidos los acuerdos de abono para reconocer la solicitud. La información del abono se utiliza para autorizar algunas solicitudes de servicio.

La autentificación y autorización las realiza el proveedor del servicio para permitir o denegar el acceso del usuario al servicio invocado para telecomunicaciones de emergencia. Se prevé que la autorización propiamente dicha tiene lugar en la red medular.

El trato prioritario de extremo a extremo es un conjunto de capacidades utilizadas por la(s) red(es) para proporcionar una elevada probabilidad de establecimiento y mantenimiento del servicio de la red de origen a la red de terminación, con inclusión de cualesquiera redes de tránsito. El trato prioritario continúa aunque se invoque la liberación del servicio. El trato prioritario está incluido en el control de admisión y atribución de recursos de red, y el transporte de paquetes portadores de medios y señalización por los elementos de red que soportan el servicio.

La interconexión de redes y el interfuncionamiento de protocolos son necesarios para soportar el trato prioritario de extremo a extremo de la señalización y el transporte de medios a través de múltiples redes pertenecientes a diferentes proveedores que utilizan tecnologías diferentes. A título de ejemplo, los niveles de prioridad pueden variar en función de la tecnología utilizada en las múltiples redes, y podría ser necesario hacer corresponder un nivel definido de una tecnología con otra.

7.2 Alerta temprana

Los sistemas de alerta temprana necesitan un sistema de comunicación eficaz que sea fiable y robusto. 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.
- 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 la integridad de los sistemas de alerta temprana y la integridad y autenticidad de los mensajes (es decir, el envío únicamente de mensajes autorizados).
- Transmitir mensajes de alerta únicamente a los posibles afectados por una catástrofe inminente y evitar mensajes sin destino o innecesarios (por ejemplo, mensajes enviados a destinatarios erróneos y/o mensajes que no contengan información viable de utilidad).

Con miras a enviar mensajes de alerta únicamente a los posibles afectados por una catástrofe inminente, los sistemas de alerta temprana pueden tener objetivos relacionados con el filtrado de los mensajes de manera que lleguen a:

- grupos de usuarios;
- regiones o zonas geográficas, etc.,

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

8 Directrices y requisitos de seguridad generales

8.1 Directrices generales

Los elementos, sistemas, recursos, datos y servicios de red utilizados para las telecomunicaciones de emergencia pueden estar destinados a hacer frente a ciberataques. La integridad, confidencialidad y disponibilidad de telecomunicaciones de emergencia, en particular durante

ataques, dependerá de los servicios y prácticas de seguridad implementados en la NGN y en las capacidades de seguridad (por ejemplo, funciones de autentificación y autorización de usuario) implementadas como parte del servicio de aplicación de telecomunicaciones de emergencia. Entre las directrices generales que se pueden considerar para planificar la seguridad de las telecomunicaciones de emergencia cabe señalar, entre otras, las siguientes:

- La protección contra las amenazas a la seguridad de todos los aspectos de las telecomunicaciones de emergencia, con inclusión de la información y los datos relacionados con la señalización y el control, el portador y los medios y la gestión (por ejemplo, información sobre el perfil del usuario). Las amenazas a la seguridad de las telecomunicaciones de emergencia pueden tener lugar en diversas capas (por ejemplo, transporte, control de servicio o soporte de servicio) y en diferentes segmentos de la red (por ejemplo, acceso, red medular, interfaces de interconexión).
- El establecimiento y la observancia de políticas y prácticas de seguridad específicas para los servicios de telecomunicaciones de emergencia. Se deberían identificar e implementar para las telecomunicaciones de emergencia capacidades de mitigación con el fin de ofrecer protección contra diversas amenazas a la seguridad, y concretamente las capacidades y prácticas de seguridad que están más allá de las necesarias para servicios de aplicación general. Esto incluye políticas sectoriales encaminadas a proteger los datos sobre gestión y la información almacenada (por ejemplo, la información sobre el perfil del usuario) relacionada con las telecomunicaciones de emergencia.
- La concepción y aplicación de procedimientos para autentificar y autorizar usuarios, dispositivos o una combinación de usuarios y dispositivos, con el fin de proteger contra el acceso no autorizado a servicios, recursos e información (por ejemplo, información de usuario en sistemas de gestión y servidores de autentificación) relacionada con las telecomunicaciones de emergencia. Se deberían implementar, por ejemplo, funciones de autentificación y autorización para evitar el uso de recursos consagrados a las telecomunicaciones de emergencia por usuarios no autorizados con miras a evitar la denegación de servicio y otros tipos de ataque.
- La responsabilidad en cada red por la seguridad, dentro de su dominio, de las comunicaciones que atraviesan múltiples dominios de proveedor de red, de modo que puedan asegurarse las comunicaciones de extremo a extremo. Dado que las telecomunicaciones de emergencia pueden incluir comunicaciones que atraviesan diferentes dominios de proveedor de redes nacionales e internacionales (es decir, países/administraciones), es necesario establecer e implementar políticas de seguridad, relaciones de confianza, métodos y procedimientos para identificar el tráfico de telecomunicaciones de emergencia, la gestión de identidades y la autentificación de usuarios y redes a través de múltiples dominios de administración de red.

Para mayor información al respecto, véase [b-ATIS-1000010].

8.2 Requisitos generales

Las Recomendaciones sobre seguridad consignadas en [UIT-T Y.2701], [UIT-T Y.2702] y [UIT-T Y.2704], así como en las Recomendaciones sobre gestión de identidad (IdM) [UIT-T Y.2720], [UIT-T Y.2721] y [UIT-T Y.2722], son pertinentes para la seguridad de las telecomunicaciones de emergencia.

8.2.1 Control de acceso

Sólo se debe permitir el acceso a las telecomunicaciones de emergencia y demás recursos conexos a los usuarios autorizados. Se debe impedir todo acceso no autorizado, por ejemplo de intrusos haciéndose pasar por usuarios autorizados.

8.2.2 Autentificación

En aras de la seguridad, es preciso establecer mecanismos y capacidades para identificar, autentificar y autorizar el acceso de los usuarios, dispositivos o una combinación de usuario y dispositivo de telecomunicaciones de emergencia, según proceda, sobre la base de la política[1] y el nivel de seguridad para el servicio concreto en cuestión (por ejemplo, voz, datos, vídeo).

8.2.3 Confidencialidad y privacidad

Hay que proteger la confidencialidad y la privacidad de las telecomunicaciones de emergencia y la información del usuario final, incluidas la señalización, el tráfico portador y de control y la actividad e información del usuario final (por ejemplo, información sobre identidad, abono y localización).

8.2.4 Seguridad de la comunicación

Es necesario proteger las telecomunicaciones de emergencia contra intrusiones (por ejemplo, evitar la intervención ilegal, la piratería o la reproducción de tráfico portador o de señalización).

8.2.5 Integridad de los datos

Es necesario proteger la integridad de las telecomunicaciones de emergencia (por ejemplo, proteger contra la modificación, supresión, creación o reproducción no autorizadas), incluida su información y cualesquiera datos de configuración (marcación de prioridad, información sobre prioridad almacenada en las funciones de decisión de política, nivel de prioridad del usuario, etc.).

8.2.6 Disponibilidad

Debe protegerse la disponibilidad de las telecomunicaciones de emergencia y demás recursos conexos, específicamente contra la denegación de servicio y otras formas de ataque.

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

9.1 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 se 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 autentificados y

[1] En este contexto, la política abarca todas las políticas aplicables, como las generadas por las decisiones del proveedor de servicios NGN, los requisitos reglamentarios y otras normas del gobierno.

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 o sesiones de telecomunicaciones de emergencia. Las etiquetas que se utilizan para identificar y marcar llamadas o 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 o sesión de telecomunicaciones de emergencia (es decir, control de llamada o 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 o 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). La versión del IP utilizada puede variar de un proveedor a otro, y la conectividad de extremo a extremo puede exigir la adaptación de diferentes versiones, recurriendo por ejemplo a la tunelización de una versión dentro de otra. No obstante, esto no debería afectar el transporte de la información relacionada con el servicio de telecomunicaciones de emergencia.

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 o sesión de telecomunicaciones de emergencia pude 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][2]. 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 STE 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) autentificación y autorización de usuarios de telecomunicaciones de emergencia certificados.

9.1.1 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.

---

[2] 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."

9.1.2 Identificación, autentificación 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 autentificar 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, STE y TDR).

Es necesario identificar las peticiones de llamada o 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 autentificación y autorización de los usuarios de telecomunicaciones de emergencia. Se necesitan mecanismos y métodos específicos para realizar la autentificación 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).

En el apéndice II de [UIT-T Y.2702] se describen los métodos para la autentificación y autorización del STE, entre los que cabe citar los siguientes:

a) Utilización de un número de identificación personal (PIN): Conforme a este método se usa un PIN para autentificar la autorización del usuario para invocar al STE. Con este método se identifica al usuario pero no al dispositivo del usuario, y por lo tanto se utiliza normalmente en los casos en los que el usuario está autorizado para invocar el servicio STE desde cualquier dispositivo.

b) Utilización del perfil del servicio/abono: De conformidad con este método, se proporciona el perfil de servicio y terminal del usuario para indicar el abono STE. Cuando se autentifica el terminal como parte del procedimiento de registro normal del proveedor NGN (es decir, el proveedor STE), se identifica el abono STE del usuario. Cuando el usuario inicia una petición STE, la verificación con el perfil del servicio del usuario permite determinar si éste está autorizado o no para el STE.

c) Uso de una combinación de PIN y perfil del usuario: También se pueden utilizar métodos que combinan el empleo de PIN y el perfil del servicio para autentificar tanto al usuario como al dispositivo del usuario con el fin de ofrecer un STE con mayor nivel de seguridad.

d) Utilización de testigos de seguridad especiales y biométrica: Además de los métodos antes descritos, existen otros métodos más complejos que utilizan testigos de seguridad especiales y capacidades de biométrica para autentificar y autorizar a los usuarios STE y ofrecer un nivel más alto de seguridad respecto de la identidad.

Una vez que el usuario, el dispositivo o una combinación de ambos esté autentificado y autorizado de acuerdo con la política aplicable, es necesario marcar las llamadas o sesiones de telecomunicaciones de emergencia e indicarlo en la dirección de destino a las redes posteriores. Del mismo modo, una vez realizadas la autentificación y la autorización, es necesario que todos los aspectos de la llamada o sesión de telecomunicaciones de emergencia, señalización/control, tráfico portador y cualquier gestión aplicable reciban prioridad.

También ha de considerarse la aplicación de la autentificación y autorización a la entrega y recepción de llamadas o sesiones de telecomunicaciones de emergencia entre proveedores de NGN, teniendo en cuenta el entorno con múltiples proveedores y la separación entre el control de servicio y el transporte. La autentificación y autorización de proveedores de NGN para la entrega y recepción de llamadas o sesiones de telecomunicaciones de emergencia y del tráfico ha de basarse en los acuerdos de nivel de servicio y en la política aplicable.

Pueden aprovecharse las capacidades IdM consignadas en ([UIT-T Y.2720], [UIT-T Y.2721] y [UIT-T Y.2722]), con el fin de proporcionar mayor confianza en la información de identidad para aplicaciones de telecomunicaciones de emergencia. El apéndice III de [UIT-T Y.2721] contiene ejemplos de casos de uso de IdM relacionados con el STE, en los cuales se describe cómo se pueden utilizar las capacidades IdM para aplicaciones STE y en éste se abordan los siguientes temas:

- Seguridad de autentificación utilizando una combinación de usuario y dispositivo (por ejemplo, correlación entre la autentificación del usuario y la del dispositivo).
- Autentificación mejorada de usuarios STE para servicios prioritarios de próxima generación (por ejemplo, empleo de testigos de seguridad, certificados digitales, reconocimiento de voz y biométrica).
- Autentificación de las fuentes de comunicación de datos y de la parte llamante (por ejemplo, seguridad de fuentes de datos y mensajes).
- Identificación y autentificación de proveedores de servicio en un entorno de múltiples proveedores (por ejemplo, identificación de proveedores de servicios de red, acceso y contenido).
- Inicio y cierre único de sesiones (es decir, acceso a múltiples aplicaciones sin tener que proporcionar credenciales individualmente para cada aplicación).

9.1.3 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). El IETF está redactando un ejemplo de este mecanismo.

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

El CAC es un conjunto de acciones y políticas que toma la red en la fase de establecimiento de llamada o 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 autentificación 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 o 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 o 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 o 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 STE) en la NGN. El tráfico con este nivel de prioridad tiene la más alta prioridad de admisión en la NGN.

9.2 Estrato de servicio

9.2.1 Generalidades

Los países ya tienen o están estableciendo un STE 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 STE de un país se comunique con los usuarios de otro país. En este caso, es fundamental que la llamada o sesión de STE 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 STE 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 STE. Tales capacidades de protocolo se necesitan para las aplicaciones internacionales en el contexto de la comunicación entre implementaciones nacionales del STE a través de la red internacional (por ejemplo, interconexión de dos implementaciones nacionales del STE).

9.2.2 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 STE.

Espacio de nombre	Niveles
ets	5
wps	5

Todas las llamadas o sesiones del STE 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 o sesiones del STE entrantes se les asigna una designación "ets" en el encabezamiento "Prioridad de recursos". Las llamadas o sesiones del STE 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 o sesión cuando los recursos son limitados o están congestionados, como puede ocurrir en el acceso radioeléctrico a las redes inalámbricas.

9.2.3 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 STE.

9.2.4 Protocolos de control de sistema UIT-T H.323

En esta cláusula se presentan los protocolos utilizados por el sistema UIT-T 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 UIT-T H.323. El parámetro designación de prioridad de llamada UIT-T 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, STE), [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 soporta 16 niveles de prioridad. El indicador de llamada IEPS y el indicador de prioridad satisfacen los requisitos de STE en cuanto a la indicación del contexto de STE y la transmisión del nivel de prioridad, respectivamente. 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.

En [UIT-T H.248.81] se dan orientaciones sobre la utilización del indicador de llamada IEPS y el indicador de prioridad en los perfiles UIT-T H.248 para sistemas UIT-T H.323 y NGN con el fin de dar soporte a servicios con prioridad (por ejemplo, STE).

9.2.5 Diámetro

El protocolo Diámetro [IETF RFC 3588] permite la autentificación, autorización y contabilidad (AAA) de funciones y aplicaciones de red tales como el acceso a red y la movilidad IP.

Los siguientes pares de atributo-valor (AVP) han sido concebidos para ser utilizados en el protocolo diámetro con el fin de respaldar los servicios prioritarios (por ejemplo, el STE):

– Identificador del MPS.
– Prioridad de reserva.
– Nivel de prioridad (como parte de la prioridad de retención de atribución (ARP) AVP).
– Prioridad de sesión.

El AVP identificador del MPS definido por 3GPP en [b-3GPP TS 29.214]. El Identificador del MPS se emplea para marcar un servicio de prioridad (por ejemplo, una solicitud de STE/MPS) por la interfaz Rx. El AVP Identificador del MPS contiene la variante nacional del nombre del servicio prioritario.

El AVP prioridad de reserva está definido por el Instituto Europeo de Normas de Telecomunicaciones (ETSI) en [ETSI TS 183 017]. En [UIT-T Q.3321.1] y [UIT-T Q.3303.3] se especifica la utilización del AVP prioridad de reserva en las interfaces Rs y Rw de la función de control de recursos y admisión (RACF) [UIT-T Y.2111], respectivamente, para los servicios prioritarios. De manera similar, en [b-3GPP TS 29.214] (control de tasación y política a lo largo de un punto de referencia Rx) y [UIT-T Q.1741.6] se especifica el AVP prioridad de reserva en la interfaz Rx control de tasación y política (PCC) para los servicios prioritarios (por ejemplo, el STE). El AVP prioridad de reserva admite 16 niveles de prioridad que pueden usarse para solicitar trato prioritario. Los valores entre 0 y 15 van en orden ascendente, siendo "15" el más alto y "0" el menor. El AVP prioridad de reserva incluye el valor de prioridad del usuario.

El AVP nivel de prioridad (como parte del AVP prioridad de retención de atribución (ARP)) se define en [b-3GPP TS 29.212] (control de tasación y política a lo largo de un punto de referencia Gx) y en [UIT-T Q.1741.6]. Esta última especifica el AVP nivel de prioridad a lo largo

de la interfaz Gx control de tasación y política (PCC) para los servicios prioritarios (por ejemplo, el STE). El AVP nivel de prioridad admite 15 niveles de prioridad que pueden usarse para solicitar trato prioritario. Los valores entre 0 y 15 van en orden decreciente, siendo "1" el más alto y "15" el menor. Los valores de prioridad 1 a 8 se asignan a servicios que están autorizados para recibir un trato prioritario (por ejemplo, STE, MPS). El valor "0" está reservado y en caso de recibirlo se le trata como un error lógico. El AVP nivel de prioridad representa el valor prioritario del usuario.

El AVP prioridad de sesión se define en [b-3GPP TS 29.229] (interfaces Cx y Dx basadas en detalles del protocolo diámetro; detalles de protocolo) y en [UIT-T Q.1741.6]. En [b-3GPP TS 29.229] se especifica el uso del AVP prioridad de sesión a lo largo de las interfaces Cx y Dx para los servicios prioritarios (por ejemplo, STE). Análogamente, en [b-3GPP TS 29.229] (interfaces Cx y Dx basadas en detalles del protocolo diámetro; detalles de protocolo) y en [UIT-T Q.1741.6] se especifica la utilización del AVP prioridad de sesión a lo largo del interfaz Sh para los servicios prioritarios. El AVP prioridad de sesión admite 5 niveles de prioridad que pueden usarse para solicitar trato prioritario por las interfaces Cx, Dx y Sh. Los valores entre 0 y 4 están definidos en orden de prioridad decreciente, siendo "0" el más alto y "4" el menor.

9.3 Estrato de transporte

9.3.1 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 la capacidad saliente disponible de ese elemento, el único recurso que queda a dicho elemento es descartar el tráfico excedentario, 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 (por ejemplo, según se estipula en los SLA). El Foro TM ha proporcionado orientación sobre especificación y gestión de los SLA [b-TM Forum GB917], y ha considerado en particular cómo se podían aplicar esas orientaciones al STE.

La sobreconfiguración es una 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 o 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.

9.3.2 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.

El IETF está preparando 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, estas extensiones 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.

9.3.3 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.

9.3.4 EF DSCP para el tráfico admitido por capacidad

En [IETF RFC 5865] se define un DSCP VOICE-ADMIT para una clase de tráfico que está sujeta a un procedimiento CAC estricto e incluye al tráfico STE. Ello permitiría que el tráfico en tiempo real se conforme a la retransmisión rápida por saltos empleando un procedimiento CAC que conlleve autentificación, autorización y admisión de capacidad (véanse las cláusula 9.3.1 y 9.3.2 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.

9.3.5 Notificación de congestión explícita (ECN, *explicit congestion notification*)

En [IETF RFC 3168] se define la arquitectura de capa doble de la ECN como una arquitectura que funciona en la capa de red (es decir, IP) y la capa de transporte (es decir, TCP). Su objetivo es proporcionar oportunamente una información de retorno señalizada explícita a la fuente de congestión en sentido descendente, pero con una pérdida de paquetes mínima o nula, y por consiguiente con una perturbación mínima de los flujos. La transmisión de esta información señalizada se efectúa a través de nodos intermediarios que soportan la gestión de puesta en cola activa, que marca a los paquetes con una notificación de congestión y los retransmite en sentido descendente en vez de abandonar el paquete. Entonces el punto final del flujo envía la indicación de información de retorno (por ejemplo, ECN) a la fuente por un protocolo de transporte de capa superior. [IETF RFC 4340] amplió el soporte de ECN para incluir al protocolo de control de congestión de datos (DCCP, *data congestion control protocol*).

En el caso de los protocolos TCP y DCCP, la ECN desencadena algoritmos inherentes de respaldo que son transparentes para las aplicaciones. El beneficio general de esta característica es que las aplicaciones funcionan mejor para la red y reducen la carga, permitiendo así que un mayor número de usuarios/aplicaciones utilicen la red. Conforme a esta hipótesis de transparencia de las aplicaciones, la ECN no favorece específicamente a los usuarios del STE más que al público en

general. Antes bien, la ECN facilita el empleo continuo de los recursos de red tanto por los usuarios del STE como por el público en general.

El Grupo de Trabajo de Red del IETF está estudiando cómo se puede utilizar la ECN para flujos RTP a lo largo de UDP/IP que utilizan RTCP como mecanismo de retroalimentación. La solución consiste en transmitir al remitente las marcaciones de congestión experimentadas ECN utilizando RTCP, verificar la funcionalidad ECN de extremo a extremo y determinar cómo se inicia la notificación ECN. Los actuales estudios del IETF están diseñados con el fin de añadir soporte ECN para aplicaciones en tiempo real (por ejemplo, voz e imagen) utilizando RTP/RTCP. En este caso, la notificación de congestión se pone a disposición de las aplicaciones, las cuales pueden reaccionar de diversa manera ante esa notificación. Cabe esperar que la reacción por defecto estará en conformidad con la de los protocolos TCP y DCCP, en los cuales la aplicación reduce la carga en la red.

9.4 Soporte de la tecnología de acceso a la NGN

9.4.1 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 [b-IEEE 802.11]) y [b-IEEE 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.

Al determinar un trato prioritario para las telecomunicaciones de emergencia, se consideran los siguientes aspectos: clasificación o etiquetado del tráfico para trato prioritario, señalización para establecer el trayecto con miras a transportar ese tráfico y establecimiento de mecanismos, incluidas las políticas para admitir la prioridad solicitada. Algunos aspectos tales como la selección de los mecanismos, las políticas y las implementaciones conexas no están normalizados y pueden ser diferentes en cada región.

9.4.2 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 o 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.

9.4.2.1 Sistema de telecomunicaciones móviles universales (UMTS, *universal mobile telecommunications system*) y evolución a largo plazo (LTE, *long term evolution*)

En [b-3GPP TS 22.153] se especifica el servicio prioritario y el servicio prioritario multimedios para sistemas 3GPP, los cuales permiten a los usuarios autorizados obtener acceso prioritario a los próximos canales de radiocomunicaciones (tráfico de voz o datos) disponibles antes que otros usuarios durante situaciones en las que la congestión bloquea los intentos de llamada. El servicio prioritario admite la progresión de llamada prioritaria y la terminación de llamada para poder transmitir una llamada prioritaria de "extremo a extremo" desde una red móvil a otra red móvil, de red móvil a fija y de fija a móvil. El servicio prioritario multimedios admite la progresión prioritaria de las sesiones multimedios y la terminación para soportar sesiones multimedios prioritarias de "extremo a extremo" desde una red móvil a otra red móvil, de red móvil a fija y de fija a móvil.

Sobre la base de [b-3GPP TS 22.153], el 3GPP está elaborando un Informe Técnico de Fase 2 para mejorar el servicio prioritario multimedios (MPS) [b-3GPP TR 23.854] mediante la indicación de cambios en las especificaciones actuales 3GPP Fase 2 (es decir, [b-3GPP TS 23.401], [b-3GPP TS 23.203], [b-3GPP TS 23.328] y [b-3GPP TS 23.272]) y para soportar el MPS, incluidos los aspectos relativos al subsistema multimedios IP (IMS) y el control de tasación y política (PCC). Este TR está destinado a aclarar los requisitos arquitectónicos y flujos de llamada o sesión del MPS. Sobre la base de los requisitos de la Fase 2, se indicarán cambios en las especificaciones actuales de 3GPP Fase 3 con el fin de soportar MPS para tecnologías de acceso UMTS y LTE.

9.4.2.2 Evolución – Datos optimizados (EV-DO)

De manera similar al 3GPP, el 3GPP2 especificó un servicio prioritario multimedios (MMPS, *multimedia priority service*) para sistemas 3GPP2. La especificación 3GPP2 para MMPS es [b-3GPP2 S.R0117-0]. Las normas de interfaz de red de los sistemas 3GPP2 cuentan con varias capacidades tales como actualización de los niveles de prioridad del portador, y esas capacidades pueden utilizarse para proporcionar servicios MMPS. Asimismo, las normas de interfaz radioeléctrica de los sistemas 3GPP2 incluyen varias capacidades tales como la puesta en cola, y esas capacidades pueden utilizarse para proporcionar servicios MMPS.

9.4.2.3 Acceso a red WiMAX

[b-WFM Stage1-r1] define los requisitos de Fase 1 del servicio de telecomunicaciones de emergencia (STE) a través de redes WiMAX para la Versión 1.6, basada en la interfaz radioeléctrica [b-IEEE 802.16] 2009. [b-WFM Stage1-r2] mejora los requisitos de la Fase 1 STE WiMAX Versión 1.6 para que la Versión 2.0 admita la interfaz radioeléctrica [b-IEEE 802.16m].

En [b-WFM Stage2-a1] se especifica el marco para la solución de red WiMAX de Fase 2 del STE a efectos de que la Versión 1.6 admita los requisitos de Fase 1. Dicho marco versa sobre la indicación de prioridad iniciada por la red y el trato prioritario para la arquitectura de autentificación, autorización y contabilidad (AAA). Se están elaborando la arquitectura de control de tasación y política (PCC) y los mecanismos de prioridad iniciados en el UE para la Versión 2.0.

En [b-WFM Stage3-a1] se especifican los mensajes y los procedimientos de red WiMAX de Fase 3 para que la Versión 1.6 admita la indicación de prioridad y el trato prioritario, sobre la base del marco de la solución de Fase 2. Se añade un campo de indicación de prioridad en el parámetro descriptor QoS de los mensajes de diámetro y RADIUS WiMAX. En este documento también se describen los procedimientos de indicación de prioridad para la arquitectura AAA iniciada por la red, así como los mecanismos de trato prioritario en las entidades funcionales de la red de servicio de conectividad (CSN, *connectivity service network*), la pasarela ASN y la estación de base (BS). A continuación se indican los ámbitos fundamentales del soporte STE en la red WiMAX:

1) Tras el lanzamiento inicial por la red destinado al UE que corresponde a un abono WiMAX habilitado por el STE, las indicaciones de prioridad relacionadas con los flujos de servicio iniciales del UE se pasan del servidor autentificación, autorización y contabilidad (AAA) a la pasarela de red de acceso a servicio (ASN) y luego a la estación de base (BS). Esta última aplica el tratamiento prioritario a la programación y atribución de recursos para los flujos de servicio prioritarios.
2) Tras la invocación del STE desde un UE, las indicaciones de prioridad asociadas a los flujos de servicio para el UE se pasan de la función de aplicación (AF) al servidor AAA/función de política (PF) y posteriormente a la pasarela ASN con destino a la BS. Esta última aplica tratamiento prioritario a la programación y atribución de recursos para los flujos de servicio prioritario.
3) Después del traspaso, las indicaciones de prioridad relacionadas con los flujos de servicio para el UE que estaban en la BS servidora pasan a la BS de destino para el traspaso intra-ASN y de la pasarela ASN servidora a la pasarela ASN de destino. Las BS aplican tratamiento prioritario a la programación y atribución de recursos de todos los flujos de servicio prioritario durante la preparación y la acción de traspaso.
4) Tras ubicar por radiobúsqueda a un UE en modo inactivo, la indicación de prioridad asociada al flujo de servicio se pasa de la pasarela ASN con la función trayecto de datos al controlador radiobúsqueda de anclaje, y de ahí a la BS. Esta última aplica tratamiento prioritario a la programación y atribución de recursos para los flujos de servicio prioritario al transmitir mensajes de radiobúsqueda. En respuesta a la radiobúsqueda de prioridad, cuando un UE entra en la red la BS reconoce la prioridad de la llamada STE entrante y le confiere tratamiento prioritario al UE para que salga del modo inactivo y añade o modifica el flujo de servicio para la llamada STE al UE de destino.

Se están elaborando procedimientos y mensajes adicionales de Fase 3 del STE para la Versión 2.0, que comprende indicación de la prioridad y trato prioritario para alineación, creación de flujos de servicio e interfaz universal de servicios (USI).

9.4.3 Acceso fijo

Las redes de acceso fijo han de soportar mecanismos y capacidades específicos para otorgar un tratamiento preferente/prioritario a las llamadas o sesiones de telecomunicaciones de emergencia autorizadas/sesiones de telecomunicaciones de emergencia autorizadas. Pueden utilizarse mecanismos y capacidades específicos de cada tecnología (por ejemplo, [b-802.1p] con xDSL, IPCablecom, IPCablecom 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 o sesiones de telecomunicaciones de emergencia.

En los siguientes subpárrafos se describen los aspectos específicos de la tecnología.

9.4.3.1 Acceso a la red IPCablecom

En [UIT-T J.260] se definen los requisitos del servicio de telecomunicaciones prioritario por redes IPCablecom. En [UIT-T J.261] se define el marco para elaborar las especificaciones con miras a soportar esos requisitos tanto por redes IPCablecom como IPCablecom 2. En el marco se contemplan dos ámbitos clave, a saber, prioridad y autentificación, y se identifican para futuras versiones otros ámbitos tales como la capacidad de rehabilitación. El marco está definido para incluir los aspectos comunes y las diferencias resultantes de las arquitecturas utilizadas en las redes IPCablecom e IPCablecom 2 (basadas en IMS). Ambas redes son redes de paquetes que tienen las propiedades descritas en el párrafo 6, como la compartición de recursos para el tráfico de control y de datos. En el marco contenido en [UIT-T J.261] se clasifican los requisitos de prioridad de [UIT-T J.260] en lo tocante a la señalización, el etiquetado y los mecanismos.

En [UIT-T J.262] se define la especificación para soportar los requisitos de autentificación en las redes IPCablecom 2. En [UIT-T J.262] se incluyen ejemplos de flujos con el fin de mostrar los intercambios de mensajes en diferentes contextos hipotéticos correspondientes a la autentificación basada en PIN, la utilización del encabezamiento prioridad de recurso SIP: el agente usuario origina una llamada VoIP con destino a un usuario RTPC utilizando un PIN, el agente usuario origina una llamada VoIP con destino a otro agente usuario VoIP utilizando un PIN y autentificación basada en el abono.

En [UIT-T J.263] se define la especificación para la señalización de prioridad con fines de tratamiento prioritario utilizando el encabezamiento prioridad de recurso SIP [IETF RFC 4412]. La especificación contiene dos opciones: 1) el UA inicia la solicitud, incluido el encabezamiento prioridad de recurso; 2) sobre la base de la información contenida en la solicitud, P-CSC-FE inserta el encabezamiento prioridad de recurso con el valor del nivel de prioridad adecuado. Los valores de nivel de prioridad y el espacio de nombre que se han de utilizar en diferentes regiones se incluyen como anexos a [UIT-T J.263]. En algunas regiones se exige admitir los valores definidos en [IETF RFC 4412]. En [UIT-T J.263] también se describe la relación con los flujos de servicio que se establecen durante el aprovisionamiento del adaptador multiterminal incorporado (EMTA, *embedded multi-terminal adapter*) en la capa DOCSIS MAC con el fin de reflejar los parámetros de calidad de servicio requeridos para las telecomunicaciones prioritarias. No se ha identificado ningún

mecanismo de etiquetado para la transferencia de datos, puesto que RTP no contiene marcaciones para indicar prioridad. Los mecanismos habilitadores de prioridad para reservar recursos y efectuar el control de admisión son posibles gracias al establecimiento de puertas definidas como parte de la calidad de servicio dinámica (DQoS) en IPCablecom.

9.4.3.2 Acceso a red xDSL

En [BBF TR-101] se describe la arquitectura de referencia para la agregación DSL basada en Ethernet. El control de política en la red de acceso DSL está basado en las especificaciones consignadas en [BBF TR-058] y [BBF TR-059].

El método básico para proporcionar capacidades STE en una red de acceso DSL consiste en utilizar las capacidades de calidad de servicio (QoS) existentes para asignar prioridad a las llamadas o sesiones STE. Conforme a este método, el único dispositivo "consciente del STE" es el servidor de política/punto de decisión de política (PDP), y éste fija la prioridad adecuada que se ha de aplicar a los flujos utilizando las capacidades QoS en la pasarela de red de banda ancha (BNG).

Debido a la característica antibloqueo del dispositivo de interfaz de red (NID) y la trama de distribución principal (MDF), en estos elementos de red no se necesitan prestaciones STE. Se proporciona y fija la anchura de banda entre el NID y el multiplexor de acceso a la línea de abonado digital (DSLAM), y este último también se configura con características antibloqueo. Así, el enfoque elegido consiste en usar las capacidades QoS de la BNG para controlar el flujo de datos a través del DSLAM, con miras a garantizar que el tráfico no congestiona al DSLAM.

La función de agregación Ethernet se configura para transportar todo el tráfico entre la BNG y el DSLAM, y por lo tanto es otro elemento antibloqueo.

La pasarela de acceso CPE puede o no ser consciente del STE. En caso afirmativo, la pasarela de acceso podría asignar prioridad al tráfico STE para asegurar la transmisión a la red de acceso DSL, y garantizar que el DSLAM no se congestiona.

El servidor de política/PDP es responsable de proporcionar la política adecuada para el tráfico STE hacia la BNG. Para el STE, el servidor de política/PDP implementa las políticas de control de admisión, con el fin que la llamada o sesión STE tenga una gran probabilidad de éxito. Las políticas afectan el establecimiento, el mantenimiento y la terminación de la llamada o sesión STE a través de la red de acceso DSL con destino a la red de los locales del cliente. Se supone que el servidor de política/PDP recibirá la solicitud de llamada o sesión STE de la NGN (por ejemplo, entidad funcional de control de sesión de llamada apoderada (P-CSC-FE)). El servidor de política/PDP reconocerá la solicitud con la información STE adecuada y encargará a la BNG que proporcione debidamente el tratamiento prioritario.

La BNG es responsable de asignar prioridad al tráfico STE. Ésta cumple con las instrucciones del servidor de política/PDP al reservar y establecer recursos adecuados para la llamada o sesión STE. Ésta aplica el tratamiento prioritario, con inclusión de los paquetes portadores de marcación de trato prioritario para la transmisión a la pasarela de acceso CPE y de ahí a la red de banda ancha regional.

9.4.3.3 Red de acceso de fibra (FTTx)

En [UIT-T G.983.1] se describe la arquitectura de referencia de la red óptica pasiva (PON) de acceso de fibra. Dicha arquitectura de referencia se refiere a un sistema de gestión de nodo de acceso (ANMS) para el control de la terminación de línea óptica (OLT) y la terminación de red óptica (ONT). La ANMS proporciona la funcionalidad de punto de decisión de política (PDP), de cuya observancia se encargan los puntos de observancia de política (PEP) situados en OLT y ONT.

Hoy en día la red de acceso de fibra carece de observancia de política o de control de política directos. Sin embargo, para soportar el trato prioritario STE del establecimiento de llamada o sesión en la red de acceso de fibra, el ANMS tendrá que soportar las funciones dinámicas de control de política. El método básico para proporcionar capacidades STE en una red de acceso de fibra es utilizar las capacidades QoS existentes para asignar prioridad a las llamadas o sesiones STE. Conforme a este método, el único dispositivo "consciente del STE" es ANMS (por ejemplo, el servidor de política), y éste fija la prioridad adecuada que se ha de aplicar a los flujos utilizando las capacidades QoS en OLT y ONT. La política STE se señaliza por la interfaz Q3 (según se especifica en [UIT-T Q.812]) a la OLT y se refleja de la OLT a la ONT por conducto de la interfaz de gestión y control ONT (OMCI).

El ANMS es responsable de proporcionar la política adecuada para el tráfico STE hacia la OLT. Para el STE, el ANMS implementa las políticas de control de admisión, con el fin que la llamada o sesión STE tenga una gran probabilidad de éxito. Las políticas afectan el establecimiento, el mantenimiento y la terminación de la llamada o sesión STE en la red de acceso de fibra. El ANMS toma las decisiones de política finales y proporciona suficiente información como para que la OLT y la ONT efectúen la operación de control de recurso para el STE. Se supone que el ANMS recibirá la solicitud de llamada o sesión STE de la NGN (por ejemplo, entidad funcional de control de sesión de llamada apoderada (P-CSC-FE)). El ANMS reconocerá la solicitud con la información STE adecuada y encargará a la OLT que proporcione tratamiento prioritario.

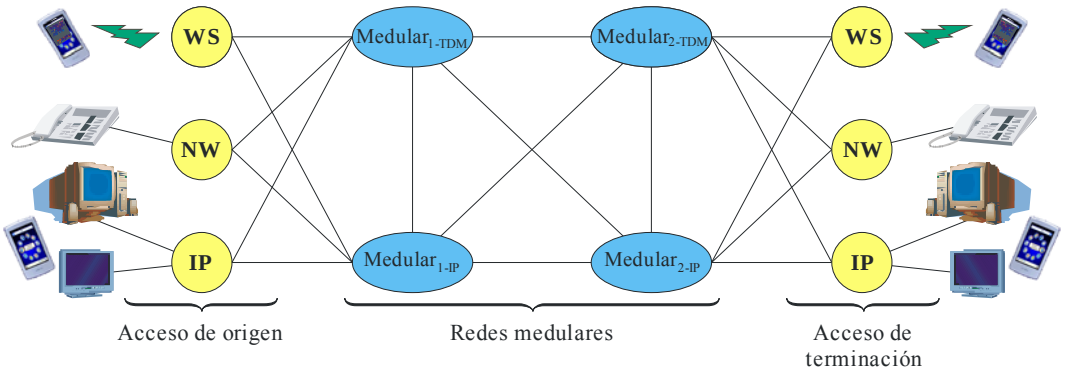
La OLT y la ONT están configuradas para transportar todo el tráfico STE. La OLT es responsable de asignar prioridad al tráfico STE. La OLT aplica las instrucciones del ANMS al reservar y establecer recursos adecuados para la manipulación de una llamada o sesión STE. Ésta aplica tratamiento prioritario, con inclusión de los paquetes portadores de marcación para el tratamiento prioritario de la transmisión.

10 Soporte de extremo a extremo para las telecomunicaciones de emergencia

En la figura 2 se muestra una matriz de llamada o sesión de extremo a extremo para diversos flujos de llamada o sesión STE, y se ilustran las llamadas o sesiones:

- que se originan y terminan en IP (por ejemplo, cable y DSL), alámbricas de banda estrecha (por ejemplo, teléfono POTS) y de acceso inalámbrico (por ejemplo, teléfono CDMA y GSM); y
- que pasan a través de redes medulares IP y con conmutación de circuitos (TDM).

Para soportar el STE de extremo a extremo es necesario el interfuncionamiento de la información específica del STE entre el dominio de tecnología IP y otros dominios tecnológicos (por ejemplo, dominios TDM alámbrico o inalámbrico), incluido el interfuncionamiento necesario para la llamada o sesión STE de extremo a extremo que podría atravesar diferentes dominios tecnológicos, según se ilustra en la figura 2. Por ejemplo, la información específica del STE (marcación de llamada STE, nivel de prioridad) debe señalizarse a través de la interfaz red-red (NNI) entre los proveedores NGN interconectados.



WS Acceso inalámbrico
NW Acceso inalámbrico en banda ancha

NOTA – Una red medular es la red que autentifica, la red de tránsito, o ambas.

Y.2205(11)_F02

Figura 2 – Matriz de llamada o sesión de extremo a extremo

Las hipótesis de llamada o sesión de la figura 2 pueden encontrarse en [b-ATIS-1000010]. En [b-ATIS-1000010] se definen los procedimientos y las capacidades necesarios para soportar el STE dentro y entre redes de proveedor de servicio basadas en IP. Sobre la base de la matriz de la figura 2, es posible considerar las siguientes hipótesis:

– Acceso de origen a la red básica 1
  - acceso alámbrico de origen a la red medular IP
  - acceso inalámbrico de origen a la red medular IP
  - acceso IP de origen a la red medular IP
  - acceso IP de origen a la red medular TDM

– Red medular 1 a red medular 2
  - red medular TDM a red medular IP
  - red medular IP a red medular TDM
  - red medular IP 1 a red medular IP 2

– Red medular 2 a acceso de destino
  - red medular IP a acceso de destino alámbrico
  - red medular IP a acceso de destino inalámbrico
  - red medular IP a acceso de destino IP
  - red medular TDM a acceso de destino IP.

El establecimiento de la llamada o sesión STE exige la implementación cuidadosa de los necesarios protocolos de señalización que transportan la información requerida que indica el carácter crítico del STE. Con miras a soportar el tratamiento prioritario de extremo a extremo, es importante admitir la correspondencia de la información de prioridad para facilitar el interfuncionamiento ininterrumpido entre los diferentes protocolos utilizados dentro de una red (por ejemplo, interfuncionamiento de protocolo vertical entre control de llamada o sesión y control de portador) o entre diferentes tipos de red (por ejemplo, interfuncionamiento de control de llamada o sesión entre dos redes), con inclusión de la RTPC. Análogamente, es esencial hacer corresponder la información de prioridad para facilitar el funcionamiento ininterrumpido entre los diferentes tipos de transporte, es decir, tipos de medios. Sin ese interfuncionamiento y esa correspondencia podría no lograrse el tratamiento prioritario de extremo a extremo.

El UIT-T está preparando una guía sobre la correspondencia de atributos del protocolo de señalización requeridos (información de prioridad STE) con el fin de soportar el establecimiento y la admisión adecuados de STE para diversas capas "horizontal" (por ejemplo, ISUP, SIP, UIT-T H.225.0) y "vertical" (por ejemplo, UIT-T H.248.0, Diámetro).

[UIT-T Q-Sup.57] estipula los requisitos de señalización para soportar capacidades preferenciales dentro de las redes IP para el STE. El apéndice III a la presente Recomendación contiene un ejemplo de flujo de llamada de [UIT-T Q-Sup.57] que ilustra el establecimiento y la autentificación satisfactorios de una llamada o sesión STE.

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

11.1 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.

11.2 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. CAP utiliza el lenguaje de marcación extensible (XML) y proporciona formatos normalizados para el intercambio de datos de información estructurada.

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 multidestinatario;
- 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, norma V1.1. OASIS también especifica CAP V1.2, que proporciona actualizaciones de CAP 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 que los sistemas existentes, como los sistemas UIT-T H.323, sean capaces de codificar, transportar y descodificar más fácilmente los mensajes CAP.

11.3 Procedimientos para el registro de arcos en el marco del arco identificador de objeto de alerta

En [UIT-T X.674], "Procedimientos para el registro de arcos en el marco del arco identificador de objeto de alerta", se prevé el registro de los arcos identificadores de objeto (OID) para identificar diferentes tipos de alertas y organismos encargados de alertas. En ésta se especifican concretamente los procedimientos encaminados al registro de arcos para identificar (todo tipo de) alertas y organismos encargados de alertas en el marco del arco identificador de objeto de alerta {joint-iso-itu-t(2) alerting(49)} a tenor de [UIT-T X.660].

En [UIT-T X.674] se facilita la asignación y el uso de los OID para identificar organismos encargados de alertas (por ejemplo, los designados por los Estados Miembros de la Organización Meteorológica Mundial (OMM)).

NOTA – La OMM mantiene al día un registro de las Autoridades de Alerta. Puede consultarse en la siguiente dirección: http://www-db.wmo.int/alerting/authorities.html.

12 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 o sesiones con el grado de prioridad deseado, permitiendo así que los servicios críticos tengan una mayor probabilidad de ser restaurados que los demás servicios.

13 Conmutación de protección y restablecimiento

13.1 Consideraciones generales

En [UIT-T G.808.1] se exponen algunos conceptos que son comunes para muchas tecnologías de transporte, y se identifican varias importantes cuestiones que se han de considerar al proporcionar protección al tráfico de telecomunicaciones de emergencia.

13.1.1 Protección individual

El concepto de protección individual se aplica a situaciones en las cuales es útil proteger sólo una parte de las señales de tráfico que necesita gran fiabilidad.

13.1.2 Protección grupal

Ésta permite la conmutación de protección mediante el tratamiento de una agrupación lógica de entidades de transporte como una sola entidad tras el comienzo de las acciones de protección.

13.1.3 Tipos arquitectónicos

En [UIT-T G.808.1] se identifican los siguientes tipos de arquitectura, los cuales se resumen a continuación.

13.1.3.1 Arquitectura de protección 1+1

En el tipo de arquitectura 1+1, una entidad de transporte de protección se destina como instalación de reserva a la entidad de transporte nominal.

13.1.3.2 Arquitectura de protección 1:n

En el tipo de arquitectura 1:n, una entidad de transporte de protección especializada es una instalación de reserva compartida por n entidades de transporte nominales.

13.1.3.3 Arquitectura de protección m:n

En el tipo de arquitectura m:n, m entidades de transporte de protección especializadas comparten instalaciones de reserva para n entidades de transporte nominales, siendo por lo general $m \leq n$.

13.1.4 Tipos de conmutación

La conmutación de protección puede ser de tipo de conmutación unidireccional o de tipo de conmutación bidireccional.

Cabe señalar que todos los tipos de conmutación, salvo la conmutación unidireccional 1+1, requieren un canal de comunicaciones entre los dos extremos del dominio protegido, denominado canal de conmutación de protección automática (APS).

En [UIT-T G.808.1] se proporciona una lista de las ventajas/desventajas que entraña la aplicación de tipos de conmutación a todos los casos antes mencionados.

En el contexto de las telecomunicaciones de emergencia basadas en IP puede resultar adecuada la conmutación unidireccional, puesto que en general los trayectos en cada dirección no están directamente asociados debido a la naturaleza unidireccional de los trayectos/encaminamientos a través de las redes IP.

13.1.5 Tipos de operación

La operación de protección puede ser de tipo reversible o irreversible.

En la operación de tipo reversible, la señal (servicio) de tráfico siempre vuelve a (o permanece en) la entidad de transporte nominal cuando se recupera del defecto.

En la operación de tipo irreversible, la señal (servicio) de tráfico no vuelve a la entidad de transporte original nominal.

En [UIT-T G.873.1] se indica que a menudo se proporciona protección 1+1 irreversible, ya que la protección está totalmente especializada, y eso evita un segundo "problema técnico" de tráfico. No obstante, puede haber motivos para proporcionar protección reversible (por ejemplo, de modo que el tráfico utilice la dirección "corta" en torno a un anillo, salvo durante condiciones de avería. Conforme a ciertas políticas de operador, se aplica operación reversible incluso para 1+1.

13.2 Arquitecturas de protección SDH

[UIT-T G.841] proporciona las especificaciones de equipos necesarias con el fin de elegir entre diferentes arquitecturas de protección para las redes de la jerarquía digital síncrona (SDH).

Las entidades protegidas pueden variar desde una sección múltiplex SDH única (por ejemplo, protección de sección múltiplex lineal) hasta una porción de un trayecto de extremo a extremo SDH (por ejemplo, protección de conexión de subred), o bien hasta la totalidad de un trayecto de extremo a extremo SDH. Las implementaciones físicas de estas arquitecturas de protección pueden incluir anillos o cadenas lineales de nodos. Cada clasificación de protección incluye directrices sobre objetivos de red, arquitectura, funcionalidad de la aplicación, criterios de conmutación, protocolos y algoritmos.

Además, [UIT-T G.842] contiene especificaciones para el interfuncionamiento de las arquitecturas de protección de red, y concretamente la interconexión de uno o más nodos entre anillos de protección MS compartidos y anillos de protección de conexión de subred (SNCP) de tipos similares y distintos.

13.3 Red de transporte óptica (OTN)

En [UIT-T G.873.1] se define el protocolo de conmutación de protección automática (APS) y la operación de conmutación de protección conforme a los esquemas de protección lineales para la red de transporte óptica a nivel de la unidad de datos del canal óptico (ODUk, *optical channel data unit*).

En esta Recomendación se consideran los siguientes esquemas de protección:

- Protección de conexión de subred ODUk con supervisión inherente (1+1, 1:n).
- Protección de conexión de subred ODUk con supervisión no intrusiva (1+1).
- Protección de conexión de subred ODUk con supervisión de subcapa (1+1, 1:n).

Para una dirección de transmisión dada, el "extremo cabeza" de la señal protegida es capaz de desempeñar una función de puente y en caso necesario depositar una copia de una señal de tráfico normal en una entidad encargada de protección. El "extremo cola" despeñará una función selectora, y seleccionará una señal de tráfico normal de su entidad de funcionamiento habitual o de una entidad de protección. En el caso de transmisiones bidireccionales, en las cuales se protegen ambas direcciones de transmisión, los dos extremos de la señal protegida desempeñarán normalmente las funciones selectora y de puente.

13.4 Conmutación de protección lineal Ethernet

En [UIT-T G.8031] se describe la conmutación de protección para las señales VLAN Ethernet, junto con detalles sobre las características de protección de la red de capa Ethernet (ETH), las arquitecturas y el protocolo APS.

En [UIT-T G.8031] se definen las arquitecturas de conmutación de protección lineal 1+1 y 1:1 con conmutación unidireccional y bidireccional.

En la arquitectura de conmutación de protección lineal 1+1, una entidad de transporte de protección está destinada a cada entidad de transporte nominal. El tráfico normal se copia y alimenta a las entidades de transporte nominal y de protección con un puente permanente en la fuente del dominio protegido. El tráfico en ambas entidades de transporte se transmite simultáneamente al sumidero del dominio protegido, en donde se efectúa una selección entre las entidades de transporte nominal y de protección, sobre la base de algunos criterios predeterminados tales como una indicación de defecto de servidor.

Aunque la selección tiene lugar únicamente en el sumidero del dominio protegido en la arquitectura de conmutación de protección lineal 1+1, para la conmutación de protección 1+1 bidireccional se necesita el protocolo de coordinación APS, de modo que los selectores en ambas direcciones seleccionen la misma entidad.

En la arquitectura de conmutación de protección 1:1 lineal, la entidad de transporte de protección está destinada a la entidad de transporte nominal. Sin embargo, el tráfico normal se transporta ya sea en la entidad de transporte nominal y en la entidad de transporte de protección utilizando un puente selector en la fuente del dominio protegido. El selector en el sumidero del dominio protegido selecciona la entidad que transporta el tráfico normal. Puesto que la fuente y el sumidero deben estar coordinados para asegurar que el puente selector en la fuente y el selector en el sumidero seleccionan la misma entidad, se necesita el protocolo de coordinación APS.

13.5 Conmutación de protección de anillo Ethernet

En [UIT-T G.8032] se define el protocolo de conmutación de protección automática (APS) y los mecanismos de conmutación de protección para topologías de anillo Ethernet de capa ETH, con inclusión de detalles sobre las características de protección de anillo Ethernet, las arquitecturas y el protocolo APS de anillo.

El protocolo de protección definido en [UIT-T G.8032] permite la conectividad protegida punto a punto, punto a multipunto y multipunto a multipunto dentro del anillo o los anillos interconectados, denominada topología "de red multianillo/escalera".

13.6 Conmutación de protección lineal para MPLS de transporte (T-MPLS)

En [UIT-T G.8131] se describen los requisitos y mecanismos de la conmutación de protección SNC y protección de camino de extremo a extremo para redes MPLS de transporte (T-MPLS). En ésta se describen los tipos de arquitecturas de protección SNC y de protección de camino, los tipos de conmutación unidireccional y bidireccional y los tipos de operación reversible e irreversible. Se define asimismo el protocolo de conmutación de protección automática (APS) utilizado para alinear ambos extremos del dominio protegido.

En esta Recomendación [UIT-T G.8131] se especifica la arquitectura 1+1 y 1:1; la primera arquitectura funciona con conmutación unidireccional y la segunda con conmutación bidireccional.

13.7 Conmutación de protección ATM

En [UIT-T I.630] se proporciona arquitecturas y mecanismos para la conmutación de protección en la capa ATM. La arquitectura incluye el ámbito y la disposición del dominio protegido. El recurso para las entidades encargadas de la protección se asigna previamente. El mecanismo incluye al activador de la conmutación de protección, los mecanismos de abstención y el protocolo de control de la conmutación de protección.

En [UIT-T I.630] se describe la protección VP/VC individual y la protección grupal. La protección VP/VC individual es una técnica a tenor de la cual se utiliza una sola conexión de red o subred para la entidad nominal y la entidad de protección. La protección grupal es una técnica a tenor de la cual se utiliza un conjunto lógico de una o más conexiones de red o subred para la entidad nominal y la entidad de protección.

Actualmente en esta [UIT-T I.630] se describe la conmutación de protección 1+1 y 1:1 bidireccional y la conmutación de protección 1+1 unidireccional.

13.8 Conmutación de protección para redes MPLS

En [UIT-T Y.1720] se estipulan los requisitos y mecanismos para la funcionalidad de conmutación de protección 1+1, 1:1, en malla compartida y 1+1 en paquetes para el plano de usuario de las redes de capa MPLS. El mecanismo que en ésta se define está diseñado para soportar un LSP punto a punto de extremo a extremo.

En [UIT-T Y.1720], elaborada para especificar las técnicas de conmutación de protección, se destacan las diferencias entre la conmutación de protección y el reencaminamiento, a saber:

Conmutación de protección: implica que tanto el encaminamiento como los recursos han sido calculados y atribuidos previamente a un LSP de protección especializado antes de un fallo. Por lo tanto, la conmutación de protección ofrece la firme garantía de poder volver a obtener los recursos de red necesarios después del fallo.

Reencaminamiento: implica que no se ha definido un LSP de protección especializado, y por lo tanto ni el encaminamiento ni los recursos han sido calculados o atribuidos previamente. Normalmente el reencaminamiento se utiliza en los casos en los cuales existen funciones de encaminamiento y señalización, y cuando la red o el cliente debe lanzar una "petición de reconexión", y por lo tanto dicha petición debe rivalizar con otros tipos de tráfico similares para obtener el recurso necesario. Por consiguiente, el reencaminamiento no ofrece garantía alguna de poder volver a obtener los recursos de red necesarios después del fallo y en general es más lento que la conmutación de protección.

La conmutación de protección es necesaria para la recuperación rápida después de un fallo, y por consiguiente realza la fiabilidad y disponibilidad de las redes MPLS.

Para la conmutación de protección hay que tener en cuenta lo siguiente:

1) La conmutación de protección debe aplicarse a la totalidad del LSP.
2) Una protección c prioritaria entre el fallo de la señal y las solicitudes de conmutación del operador.
3) Se debe proporcionar la posibilidad de lograr la protección en la capa MPLS lo más rápido posible (con sujeción a la resolución temporal del mecanismo de detección de defecto).
4) Una relación de protección del 100%, es decir que el 100% del tráfico activo degradado se protege de una falla en un solo LDP activo.
5) Siempre que sea posible se debe soportar una capacidad de tráfico adicional.

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 pueden 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 cabal 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 último, 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 STE desde cualquier ubicación/dispositivo que contacta con cualquier otro usuario (STE 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 STE 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 911, 112, etc., donde las sesiones dentro de una región se reenvían a un único punto público de respuesta de seguridad (PSAP).

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 o 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 o estatal es el centro de información de emergencias (http://alert.dc.gov/eic/site/default.asp) del sitio web 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/8l/8l_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.

Apéndice III

Ejemplo de flujos de llamada o sesión STE en la NGN

(Este apéndice no forma parte integrante de la presente Recomendación)

En este apéndice se proporciona un ejemplo de flujo de llamada o sesión STE extraído de [UIT-T Q-Sup.57] que es aplicable a las NGN. En dicho flujo de llamada se ilustra el establecimiento satisfactorio de una llamada o sesión STE en la cual se utiliza un PIN para la autentificación y autorización del usuario.

En la figura III.3 se ilustra un método de autentificación del usuario STE en el que se utiliza un PIN que el usuario introduce en la red IP. Un servidor de medios (MS) es una combinación de la entidad funcional de control de recursos de medios (MRC-FE) y la entidad funcional de procesamiento de recursos de medios (MRP-FE). Todas las solicitudes SIP incluyen un encabezamiento de prioridad de recurso (RPH) [IETF RFC 4412] para indicar que se necesita tratamiento prioritario.

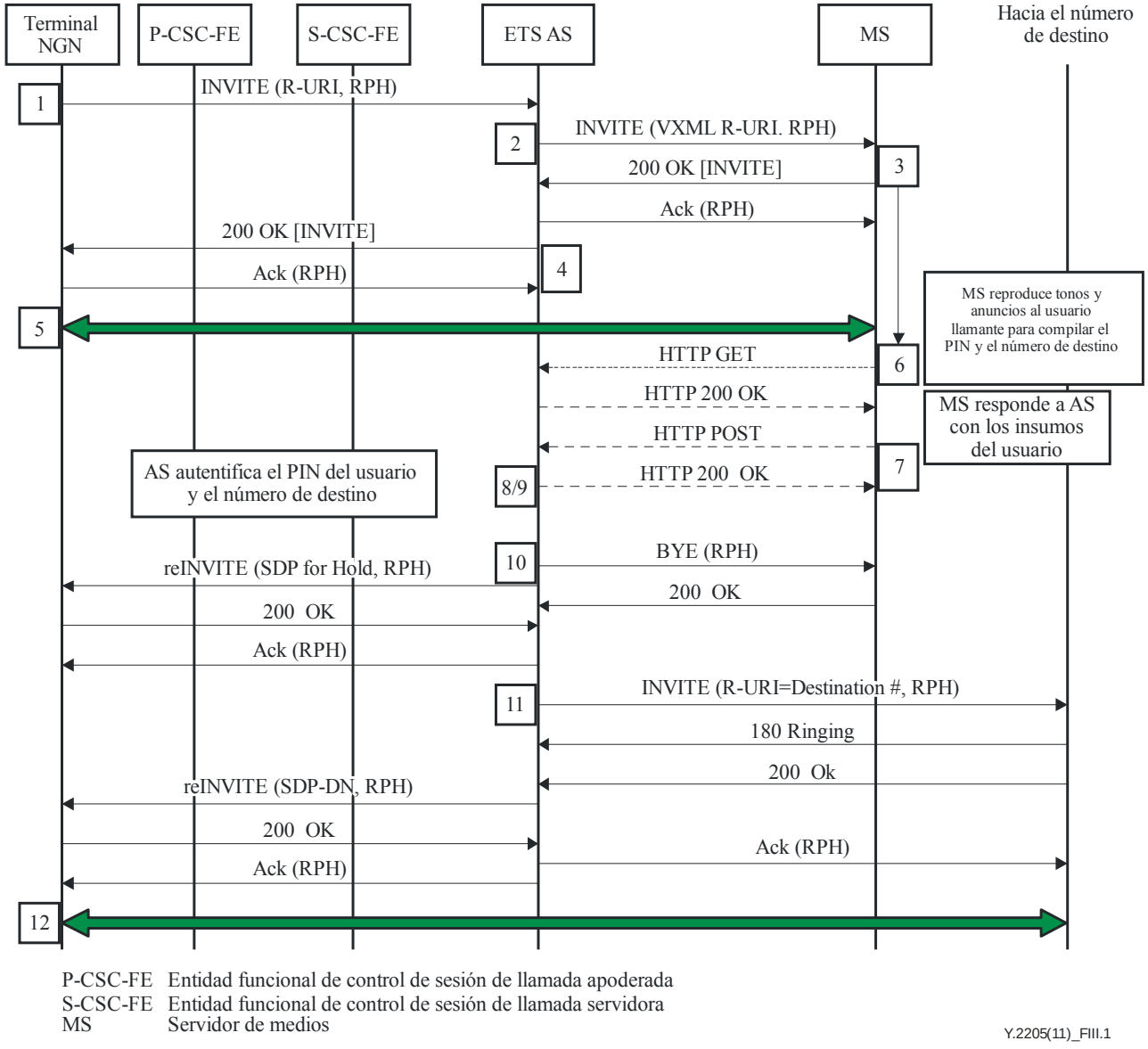


Figura III.1 – Establecimiento de llamada o sesión STE utilizando autentificación PIN

1) La llamada o sesión se encamina a un servidor de aplicación (AS) STE en el que se inicia el procesamiento de la autentificación.

2) AS STE envía un mensaje INVITE al servidor de medios seleccionado, con un ofrecimiento SDP asociado a la parte llamante. El mensaje INVITE contiene el URL del guión XML vocal almacenado en AS STE. El guión describe cómo debe interactuar la MS con la parte llamante (qué anuncio debe reproducir, cómo compilar dígitos, cuántos dígitos recoger, los temporizadores entre dígitos, etc.).

3) Tras recibir el mensaje INVITE, la MS:

   - puede enviar un 100 Trying al AS STE;
   - recupera el guión XML vocal directamente de AS STE utilizando HTTP y el URL en el mensaje INVITE (MS envía un HTTP GET al AS STE y éste devuelve el mensaje XML vocal en un HTTP 200 OK);
   - valida el guión;
   - formula y envía un mensaje 200 OK con su propio SDP a AS STE.

4) AS STE envía un mensaje 200 OK hacia la parte llamante (terminal NGN), incluyendo en el mismo la información de sesión recibida de la MS.

5) En este punto la conexión de medios está disponible entre la MS y la parte llamante.

6) Tras recibir el guión ACK y VXML en el HTTP 200 OK, la MS ejecuta el guión SML vocal. Reproduce una melodía y compila los dígitos (PIN) introducidos por la parte llamante.

7) Entonces la MS envía los dígitos compilados directamente a AS STE utilizando un mensaje HTTP POST.

8) Tras recibir los dígitos compilados, AS STE verifica si esos dígitos (PIN) son válidos:

   - Si los dígitos recibidos no son válidos (número de dígitos recibidos o el número equivocado), AS STE determina que se necesita una nueva interacción con la parte llamante. AS STE devuelve el mensaje HTTP 200 OK a la MS con un nuevo guión XML vocal. AS STE proporcionará instrucciones para el tratamiento final.
   - Si los dígitos recibidos son válidos, AS STE proporcionará instrucciones a la MS de reproducir el anuncio para compilar los dígitos (número de destino).

9) AS STE determina que los dígitos introducidos por la parte llamante son válidos.

10) AS STE libera a la MS de la llamada o sesión con un SIP BYE, y envía el mensaje reINVITE hacia la parte llamante, con un SDP para poner los medios en espera.

11) AS STE envía un INVITE hacia la parte de destino. Al recibir el mensaje 200 OK (respuesta), AS STE envía un reINVITE con el SDP asociado con la destinación hacia la parte llamante.

12) Se establece el trayecto de medios entre la parte llamante y el número de destino con la autentificación AS STE en el trayecto de control de llamada.

Bibliografía

[b-UIT-T Q-Sup.62] UIT-T Q-series Recommendations – Supplement 62 (2011), *Overview of the work of standards development organizations and other organizations on emergency telecommunications service*.

[b-UN Global Survey] Estrategia Internacional de las Naciones Unidas para la Reducción de Catástrofes, *Informe Final sobre un "Estudio mundial de los sistemas de alerta temprana"*.
<http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf>.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Impreso en Suiza
Ginebra, 2012