Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2201

(09/2009)

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

Requisitos y capacidades de las NGN del UIT-T

Recomendación UIT-T Y.2201

RECOMENDACIONES UIT-T DE LA SERIE Y

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

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

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

Recomendación UIT-T Y.2201

Requisitos y capacidades de las NGN del UIT-T

Resumen

En la Recomendación UIT-T Y.2201 se suministran los requisitos de alto nivel para los servicios y capacidades de las redes de la próxima generación (NGN, *next generation network*).

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T Y.2201	2007-04-27	13
2.0	ITU-T Y.2201	2009-09-12	13

Palabras clave

Autentificación, autorización, capacidades, compatibilidad, conocimiento del contexto, contabilidad, denominación, direccionamiento, entorno de servicio abierto, gestión, gestión de identidad, habilitador de servicio, identificación, interfuncionamiento, movilidad, multidifusión, NGN, numeración, OAM, perfil, política, privacidad, QoS, red de empresa, requisitos de capacidad, seguridad, soporte de IPv6, tasación, TVIP.

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

Recomendación UIT-T Y.2201

Requisitos y capacidades de las NGN del UIT-T

1 Alcance

En esta Recomendación se especifican los requisitos principales que se imponen al desarrollo de un conjunto de Recomendaciones del UIT-T que constituirá la de las NGN.

Estos requisitos y las capacidades correspondientes especificadas en esta Recomendación son acordes con los fines generales expresados en [UIT-T Y.2001], y se basan en los objetivos de las NGN. Versión 2 [b-UIT-T Y-Sup.7].

En general, los requisitos se suministran teniendo en mente una visión de conjunto de las NGN, y no con el fin de constituirse en requisitos funcionales precisos para las diversas entidades NGN.

Los requisitos más detallados quedan fuera del alcance de esta Recomendación.

Se acepta que es posible que una determinada NGN esté constituida por un conjunto (o superconjunto) arbitrario de servicios soportados por las NGN, y por capacidades especificadas en esta Recomendación.

NOTA 1 – El texto extraído de [UIT-T Y.2201] se indica en azul. Del mismo modo, en el apéndice I se identifican las principales diferencias entre esta Recomendación y [UIT-T Y.2201] en términos de requisitos y capacidades de alto nivel.

NOTA 2 – También es necesario estudiar la manera en que las NGN pueden contribuir al ahorro de energía, aunque la CE 5 del UIT-T se está encargando de tales estudios a partir de los resultados del Grupo Temático sobre las TIC y el cambio climático del UIT-T. Por ende, quedan en estudio los aspectos de esta Recomendación relativos a los requisitos de ahorro de energía. Pueden encontrarse los resultados del Grupo Temático sobre las TIC y el cambio climático del UIT-T en [b-UIT-T Climate].

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.

[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 de emergencia y marco de interconexión para la implementación del ETS.*

[UIT-T E.164] Recomendación UIT-T E.164 (2005), *Plan internacional de numeración de telecomunicaciones públicas.*

[UIT-T E.212] Recomendación UIT-T E.212 (2008), *Plan de identificación internacional para las redes públicas y los abonos.*

[UIT-T G.711] Recomendación UIT-T G.711 (1988), *Modulación por impulsos codificados (MIC) de frecuencias vocales.*

[UIT-T G.722] Recomendación UIT-T G.722 (1988), *Codificación de audio de 7 kHz dentro de 64 kbit/s.*

[UIT-T G.722.2] Recomendación UIT-T G.722.2 (2003), *Codificación en banda ancha de voz a unos 16 kbit/s utilizando banda ancha multivelocidad adaptativa.*

[UIT-T G.729] Recomendación UIT-T G.729 (2007), *Codificación de la voz a 8 kbit/s mediante predicción lineal con excitación por código algebraico de estructura conjugada.*

[UIT-T G.729.1] Recomendación UIT-T G.729.1 (2006), *Codificador incorporado a velocidad binaria variable basado en el codificador G.729: Tren de bits de un codificador de banda ancha adaptable de 8 a 32 kbit/s compatible con G.729.*

[UIT-T G.808.1] Recomendación UIT-T G.808.1 (2006), *Conmutación de protección genérica – Protección lineal de camino y de subred.*

[UIT-T H.263] Recomendación UIT-T H.263 (2005), *Codificación de vídeo para comunicación a baja velocidad binaria.*

[UIT-T H.264] Recomendación UIT-T H.264 (2005), *Codificación de vídeo avanzada para los servicios audiovisuales genéricos.*

[UIT-T I.610] Recomendación UIT-T I.610 (1999), *B-ISDN Principios y funciones de operaciones y mantenimiento de la RDSI-BA.*

[UIT-T M.3050.0] Recomendación UIT-T M.3050.0 (2007), *Mapa de operaciones de telecomunicación mejorado – Introducción.*

[UIT-T M.3050.1] Recomendación UIT-T M.3050.1 (2007), *Plan de aplicaciones de telecomunicaciones mejorado (eTOM) – El marco del proceso empresarial.*

[UIT-T M.3060] Recomendación UIT-T M.3060/Y.2401 (2006), *Principios para la gestión de redes de la próxima generación.*

[UIT-T Q.825] Recomendación UIT-T Q.825 (1998), *Especificaciones de aplicaciones de la red de gestión de telecomunicaciones en la interfaz Q.3: Registro de detalles de llamadas.*

[UIT-T Q.1703] Recomendación UIT-T Q.1703 (2004), *Marco de capacidades de servicio y de red desde la perspectiva de la red para los sistemas posteriores a las IMT-2000.*

[UIT-T Q.1706] Recomendación UIT-T Q.1706/Y.2801 (2006), *Requisitos de gestión de movilidad para las NGN.*

[UIT-T X.462] Recomendación UIT-T X.462 (1996), *Tecnología de la información – Gestión de sistemas de tratamiento de mensajes: Información de registro cronológico.*

[UIT-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.*

[UIT-T Y.101] Recomendación UIT-T Y.101 (2000), *Terminología de la infraestructura mundial de la información: Términos y definiciones.*

[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.1710] Recomendación UIT-T Y.1710 (2002), *Requisitos de la funcionalidad operación y mantenimiento para redes con conmutación por etiquetas multiprotocolo.*

[UIT-T Y.1730] Recomendación UIT-T Y.1730 (2004), *Requisitos de las funciones de operación, administración y mantenimiento en redes basadas en Ethernet y en servicios Ethernet.*

[UIT-T Y.1901] Recomendación UIT-T Y.1901 (2009), *Requisitos para la admisión de servicios de TVIP.*

[UIT-T Y.2001] Recomendación UIT-T Y.2001 (2004), *Visión general de las redes de próxima generación, versión 1.*

[UIT-T Y.2012] Recomendación UIT-T Y.2012 (2006), *Requisitos funcionales y arquitectura de las NGN versión 1.*

[UIT-T Y.2051] Recomendación UIT-T Y.2051 (2008), *Términos y definiciones aplicables a las redes de la próxima generación.*

[UIT-T Y.2091] Recomendación Y.2091 (2008), *Requisitos para la admisión de servicios de TVIP.*

[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.2201] Recomendación UIT-T Y.2201 (2007), *Requisitos de las redes de próxima generación, versión 1.*

[UIT-T Y.2212] Recomendación UIT-T Y.2212 (2008), *Requisitos de los servicios de entrega gestionados.*

[UIT-T Y.2213] Recomendación UIT-T Y.2213 (2008), *Requisitos y capacidades de servicio NGN para aspectos de red de aplicaciones y servicios basados en la identificación.*

[UIT-T Y.2215] Recomendación UIT-T Y.2215 (2009), *Requisitos y marco general para el soporte de los servicios VPN en las NGN, incluido el entorno móvil.*

[UIT-T Y.2233] Recomendación UIT-T Y.2233 (2008), *Requisitos y marco de referencia que admiten capacidades de contabilidad y tasación en las redes de la próxima generación.*

[UIT-T Y.2234] Recomendación UIT-T Y.2234 (2008), *Capacidades de entorno de servicio abierto para aplicaciones y servicios de usuario NGN.*

[UIT-T Y.2236] Recomendación UIT-T Y.2236 (2009), *Framework for NGN support of multicast based services.*

[UIT-T Y.2701] Recomendación UIT-T Y.2701 (2007), *Requisitos de seguridad de la red de próxima generación.*

[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 Z.100] Recomendación UIT-T Z.100 (2007), *Lenguaje de especificación y descripción.*

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

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

3 Definiciones

3.1 Términos definidos en otro sitio

Esta Recomendación utiliza los siguientes términos definidos en otro sitio.

3.1.1 contabilidad [UIT-T X.462]: Acción de recolectar información sobre las operaciones realizadas en un sistema, y los efectos de esas operaciones.

3.1.2 dirección [UIT-T Y.2091]: Identificador de un punto de terminación específico que sirve para el encaminamiento hacia dicho punto.

3.1.3 interfaz aplicación-red [UIT-T Y.2012] **(ANI, *application network interface*)**: Interfaz que proporciona un canal para las interacciones e intercambios entre las aplicaciones y los elementos de las NGN. La ANI ofrece las capacidades y los recursos necesarios para la realización de aplicaciones.

3.1.4 facturación [UIT-T Q.1703]: Función administrativa que se emplea para emitir facturas a clientes del servicio, invitarlos a pagar, obtener ingresos y atender a reclamaciones de los clientes.

3.1.5 tarificación [UIT-T Q.825]: Conjunto de funciones necesarias para establecer el precio atribuido a la utilización del servicio.

3.1.6 red empresarial [UIT-T Y.2701]: Red privada que soporta múltiples usuarios y puede estar en múltiples sitios (por ejemplo, una empresa, un campus).

NOTA – Los equipos de una red privada son propiedad de una empresa, o se gestionan en su nombre, y se interconectan para prestar servicios de telecomunicaciones a un grupo definido de usuarios pertenecientes a dicha esa empresa.

3.1.7 cliente [UIT-T M.3050.1]: El que compra productos y servicios de la empresa o recibe ofertas o servicios gratuitos. Puede ser una persona o una entidad comercial.

3.1.8 usuario extremo [UIT-T M.3050.1]: Es quien realmente utiliza los productos o servicios ofrecidos por la empresa. El usuario extremo consume el producto o el servicio. Véase también la definición de Abonado.

3.1.9 entidad [UIT-T Y2720]: Todo lo que tiene existencia separada y distinta y puede identificarse unívocamente. Ejemplos de entidad en el contexto de la gestión de identidad, son los siguientes: abonados, usuarios, elementos de red, redes, aplicaciones de soporte lógico, servicios y dispositivos. Una entidad puede contar con múltiples identificadores.

3.1.10 federación [UIT-T Y.2720]: Establecimiento de una relación entre dos o más entidades o una asociación que abarca un número variable de proveedores de servicio y proveedores de identidad.

3.1.11 traspaso [UIT-T Q.1706]: Capacidad para prestar servicios, con efecto en el acuerdo de nivel de servicio, a un objeto en movimiento, durante y después de dicho movimiento.

3.1.12 red propia [UIT-T Q.1706]: La red a la que suele estar conectado un usuario móvil, el proveedor de servicio con el que está asociado el usuario móvil, y donde se gestiona la información de abono del usuario.

3.1.13 identificador [UIT-T Y.2091]: Serie de cifras, caracteres y símbolos u otra forma de datos utilizados para identificar abonados, usuarios, elementos de red, funciones, entidades de red que

ofrecen servicios o aplicaciones, u otras entidades (por ejemplo, objetos lógicos o físicos). Los identificadores pueden ser utilizados para registro o autorización. Ellos pueden ser públicos para todas las redes, compartidos entre un número limitado de redes o propios a una red específica (los identificadores privados no están normalmente comunicados a terceras partes).

3.1.14 identidad [UIT-T Y.2720]: Información acerca de una entidad que resulta suficiente para identificar a dicha entidad en un determinado contexto.

3.1.15 gestión de identidad [UIT-T Y.2720]: Conjunto de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicación, correlación y vinculación, cumplimiento de una política, autenticación y asertos) que se utilizan para:

– garantizar la información de identidad (por ejemplo, identificadores, credenciales, atributos);

– garantizar la identidad de una entidad (por ejemplo, usuarios/abonados, grupos, dispositivos de usuario, organizaciones, proveedores de red y servicios, elementos y objetos de red, y objetos virtuales);

– habilitar aplicaciones de negocios y de seguridad.

3.1.16 proveedor de identidad [UIT-T Y.2720]: Entidad que crea, mantiene y gestiona información digna de confianza sobre la identidad de otras entidades (por ejemplo, usuarios/abonados, organizaciones y dispositivos) y ofrece servicios basados en la identidad, así como en la confianza, el negocio de que se trate y otros tipos de relaciones.

3.1.17 internet [UIT-T Y.101]: Conjunto de redes interconectadas que utilizan el protocolo internet, que les permite funcionar como una única y gran red virtual.

3.1.18 NGN IPv6 [UIT-T Y.2051]: NGN que soporta los protocolos de direccionamiento y encaminamiento, así como los servicios asociados a IPv6. Una NGN IPv6 reconocerá y procesará los encabezamientos y opciones IPv6 utilizando diversas tecnologías de transporte subyacentes en el estrato de transporte.

3.1.19 movilidad [UIT-T Y.2001]: Capacidad del usuario u otras entidades móviles para comunicarse y acceder a servicios, independientemente de los cambios de ubicación o del entorno técnico. El grado de disponibilidad de servicio puede depender de varios factores, entre ellos las capacidades de la red de acceso, los acuerdos de nivel de servicio entre la red propia del usuario y la red visitada (si los hubiere), etc. El término movilidad incluye la capacidad de telecomunicación con o sin continuidad de servicio.

NOTA – En [UIT-T Y.2001] esto se denomina "movilidad generalizada".

3.1.20 gestión de la movilidad [UIT-T Q.1706]: Conjunto de funciones que se utilizan para permitir la movilidad. Entre dichas funciones se cuentan la autenticación, la autorización, la actualización de la posición, el servicio de radiobúsqueda, la telecarga de información de usuario y otras más.

3.1.21 nomadismo [UIT-T Q.1706]: Capacidad del usuario para cambiar su punto de acceso a la red estando en movimiento; al cambiar de punto de acceso se interrumpe completamente la sesión de servicio del usuario y se inicia una nueva, es decir no es posible el traspaso o la continuidad de servicio. Se supone que, en general, los usuarios interrumpen su sesión de servicio antes de desplazarse hacia otro punto de acceso.

3.1.22 información de identificación personal [UIT-T Y.2720]: La información que tiene que ver con una persona viva, y que hace posible identificarla (lo que incluye la información que permite identificar a una persona cuando se combina con otra información, incluso cuando por sí sola no permite identificar claramente a esa persona).

3.1.23 movilidad personal [UIT-T Q.1706]: Éste es el tipo de movilidad del que se habla en el caso en que el usuario cambia de terminal de acceso a la red al cambiar de ubicación. Capacidad que tiene un usuario para acceder a los servicios de telecomunicaciones desde cualquier terminal utilizando una identificación personal, y la capacidad de la red para prestar dichos servicios conforme al perfil de servicio del usuario.

3.1.24 presencia [UIT-T Y.2720]: Conjunto de atributos que caracterizan una entidad en relación con la situación presente.

3.1.25 red pública [b-UIT-T I.570]: Red que presta servicios al público en general.

NOTA – Esta definición no comprende aspectos jurídicos o reglamentarios y no se refiere en modo alguno a la propiedad.

3.1.26 itinerancia [UIT-T Q.1706]: Capacidad de un usuario para acceder a los servicios, conforme a su perfil de usuario, desde fuera de la red propia a la que está abonado, es decir a través de un punto de acceso de una red visitada. Para ello se requiere la capacidad de acceder la red visitada, que exista una interfaz entre las redes propia y visitada, así como un acuerdo de itinerancia entre los respectivos operadores de red.

3.1.27 transferencia sin discontinuidades [UIT-T Q.1706]: Es un caso especial de movilidad con continuidad de servicio, preserva la posibilidad de proporcionar servicios a los objetos móviles durante o después de su desplazamiento sin afectar los acuerdos de nivel de servicio.

3.1.28 servicio [Suplemento 1 a la serie Z de Recomendaciones UIT-T]: Conjunto de funciones y facilidades ofrecido a un usuario por un proveedor.

3.1.29 continuidad de servicio [UIT-T Q.1706]: Capacidad que tiene un objeto móvil para mantener un servicio en funcionamiento, incluidos los estados corrientes, tales como el entorno de red usuario y la sesión para un determinado servicio.

3.1.30 abonado [UIT-T M.3050.1]: El abonado es responsable de la firma de contratos para los servicios suscritos y del pago de dichos servicios.

3.1.31 movilidad de terminal [UIT-T Q.1706]: Caso de movilidad en el que el mismo equipo terminal se desplaza o es utilizado en distintas ubicaciones. Capacidad que tiene un terminal para acceder a los servicios de telecomunicaciones en diferentes sitios y mientras está en movimiento, y capacidad de la red para identificarlo y determinar su posición.

3.1.32 red de usuario [UIT-T Y.2701]: Red privada que comparte equipos terminales que pueden servir a múltiples usuarios.

3.1.33 red visitada [UIT-T Q.1706]: Red exterior a la red propia que ofrece servicio a un usuario móvil. Este término tiene más relación con la empresa que con la geografía.

3.2 Términos definidos en la presente Recomendación

La presente Recomendación define los términos siguientes.

3.2.1 ingreso: Comunicación desde un usuario de una red pública a un usuario de una red de empresa.

3.2.2 egreso: Comunicación desde un usuario de una red de empresa a un usuario de una red pública.

3.2.3 enlace empresarial (BT, *Business Trunking*): Conexión de una red de empresa de la próxima generación (NGCN) a una NGN.

3.2.4 aplicación de enlace empresarial: Aplicación NGN que ofrece capacidades de tránsito entre redes de empresa de la próxima generación (NGCN) o capacidades de ingreso desde las NGN a una NGCN y/o de egreso desde una NGCN a las NGN.

NOTA – Una aplicación de enlace empresarial también puede ofrecer servicios adicionales más allá de las capacidades de ingreso, egreso y tránsito básicas a la NGCN.

3.2.5 conocimiento del contexto: Capacidad para determinar o influir en la siguiente acción o proceso de telecomunicaciones mediante remisión al estado de las entidades pertinentes, que forman un entorno coherente como contexto.

3.2.6 identificador de usuario de una red empresarial: Identifica al usuario de la red empresarial en las comunicaciones que entran, salen o transitan por las NGN, en representación de un usuario de la red empresaria de origen o como identidad objetivo encaminable a nivel global.

3.2.7 comunicación empresarial: Toda comunicación que:

1) se origina en una red empresarial de la próxima generación (NGCN); o

2) se termina en una NGCN; o

3) se origina en las NGN en nombre de una empresa; o

4) se termina en las NGN en nombre de una empresa,

y está sujeta a acuerdos especiales entre el operador de la NGN y la empresa.

3.2.8 capacidades de comunicación empresarial: Capacidades, cuyo anfitrión es una red empresarial de la próxima generación (NGCN) o una NGN, que permite y/o enriquece las comunicaciones empresariales.

NOTA – La aplicación de enlace empresarial, los servicios empresariales propios y las líneas arrendadas virtuales con ejemplos de capacidades de comunicación empresarial cuyo anfitrión es la NGN.

3.2.9 servicios empresariales propios (HES): Aplicación de las NGN mediante la cual la NGN es anfitriona de todas las capacidades de comunicación empresarial de origen y/o terminación para los usuarios empresariales directamente conectados a la NGN y que están abonados a esta aplicación en la misma.

NOTA – Se conoce comúnmente como IP-Centrex.

3.2.10 red empresarial de la próxima generación (NGCN): Red empresarial autónoma diseñada para aprovechar las nuevas soluciones de comunicaciones IP y que puede tener su propia configuración de aplicaciones y servicios.

NOTA – A los efectos de la presente Recomendación, se trata de una red empresarial que dispone de una interfaz IP con la NGN.

3.2.11 sitio NGCN: Parte separada de una red empresarial de la próxima generación (NGCN).

NOTA – Un sitio NGCN puede representar una parte de una NGCN limitada a un emplazamiento geográfico determinado. Cuando un sitio NGCN da servicio a más de un emplazamiento geográfico, todos ellos tendrán acceso a una NGN gracias al acuerdo de conexión concertado entre el sitio NGCN y la NGN. La comunicación entre distintos sitios NGCN pertenecientes a la misma NGCN puede, aunque no es necesario, atravesar sus respectivas NGN. Por ejemplo, estas comunicaciones pueden encaminarse por las NGN sólo durante periodos de tráfico elevado o fallo de los equipos de la NGCN. Un sitio NGCN puede tener acceso a su NGN directamente o a través de otra NGN que ofrezca una capacidad de tránsito. Una NGCN puede tener sitios NGCN en distintos países.

3.2.12 clasificación con prioridad: Clasificación de las clases de tráfico según el nivel de prioridad.

3.2.13 mecanismos de activación de prioridad: Los que permiten la habilitación en la red de un tratamiento adecuado del tráfico, conforme a las clases de prioridad.

3.2.14 tráfico de red privada: tráfico enviado a una NGN, o recibido desde la misma, para su procesamiento de conformidad con una serie de normas acordadas específicas de una empresa o comunidad de empresas estrechamente relacionadas.

3.2.15 tráfico de red pública: tráfico enviado a una NGN o recibido desde la misma, para su procesamiento de conformidad con las normas de las NGN normales.

3.2.16 inscripción única: Capacidad que tiene un usuario para utilizar una autenticación, expedida por un operador de red o un proveedor de servicio a otro operador de red o proveedor de servicio, bien sea para acceder a un servicio o itinerar en una red visitada.

3.2.17 identidad de equipo terminal: Identificador único de un equipo terminal.

3.2.18 usuario: Un usuario incluye un usuario de extremo [UIT-T Y.2091], persona, abonado, sistema, equipo terminal (por ejemplo, FAX, PC), entidad (funcional), proceso, aplicación, proveedor o red empresarial.

3.2.19 atributo de usuario: Característica que describe al usuario (por ejemplo, tiempo de validez de la identidad del usuario, estado del usuario ("disponible" o "no molestar"), etc.).

3.2.20 identidad de usuario: Un tipo de contraseña, imagen o seudónimo asociado con un usuario, que atribuyen y comparten los operadores y proveedores de servicio para poder identificarlo, autenticar su identidad o autorizar la utilización de un servicio. Por ejemplo, los identificadores biométricos como la imagen del ojo, la huella digital, un URI SIP, etc.

4 Siglas y acrónimos

En esta Recomendación se emplean las siguientes siglas y acrónimos:

AMR Multivelocidad adaptativa (*adaptive multi rate*)

ANI Interfaz aplicación-red (*application network interface*)

API Interfaz de programación de aplicaciones (*application programming interface*)

ATM Modo de transferencia asíncrono (*asynchronous transfer mode*)

B2B De empresa a empresa (*business to business*)

BA Banda amplia

BE Banda estrecha

CC Contenido de la comunicación (*content of communication*)

CD Disco compacto (*compact disk*)

cPVR Grabador de vídeo personal de cliente (*client personal video recorder*)

DECT NG Telecomunicaciones inalámbricas digitales mejoradas de la nueva generación (*digital enhanced cordless telecommunications new generation*)

DNS Sistema de nombres de dominio (*domain name system*)

DTMF Multifrecuencia bitono (*dual tone multi frequency*)

EAN Notificación de alertas de emergencia (*emergency alert notification*)

ENUM Correspondencia de números telefónicos (*telephone number mapping*)

ETS Servicio de telecomunicaciones de emergencia (*emergency telecommunications services*)

EVRC Códec mejorado de velocidad variable (*enhanced variable rate codec*)

HES Servicios de empresa acogidos (*hosted enterprise services*)

HTML Lenguaje de marcación hipertexto (*hyper text markup language*)

IdM Gestión de identidades (*identity management*)

IEPS	Plan internacional de preferencias en situaciones de emergencia (*international emergency preference scheme*)
IM	Mensajería instantánea (*instant messaging*)
IMS	Subsistema multimedios IP (*IP multimedia subsystem*)
IN (o RI)	Red inteligente (*intelligent network*)
IP	Protocolo internet (*internet protocol*)
IPv4	Versión 4 del IP (*internet protocol version 4*)
IPv6	Versión 6 del IP (*internet protocol version 6*)
IRI	Información relativa a la intercepción (*intercept related information*)
LDAP	Protocolo ligero de acceso al directorio (*lightweight directory access protocol)*
LEA	Organismos encargados de hacer cumplir la ley (*law enforcement agencies*)
MMS	Servicio de mensajería multimedia (*multimedia messaging service*)
MPLS	Conmutación por etiquetas multiprotocolo (*multi-protocol label switching*)
NAI	Identificador de acceso de red (*network access identifier*)
NAPT	Traducción de puerto de direcciones de red (*network address port translation*)
NAT	Traducción de dirección de red (*network address translation*)
NGCN	Red empresarial de la próxima generación (*next generation corporate network*)
NGN	Redes de próxima generación (*next generation network*)
NNI	Interfaz red-red (*network-network interface*)
nPVR	Grabador de vídeo personal de la red (*network personal video recorder*)
OAM	Operaciones, administración, mantenimiento (*operations, administration and maintenance*)
OIP	Presentación de identidad de origen (*origination identity presentation*)
OMA	*Open Mobile Alliance*
OS	Sistema operativo (*operating system*)
OSA	Acceso de servicio abierto (*open service access*)
OTN	Red óptica de transporte (*optical transport network*)
PBX	Centralita privada (*private branch eXchange*)
PC	Computador personal (*personal computer*)
PDA	Agenda digital (*personal digital assistant*)
PII	Información de identificación personal (*personally identifiable information*)
PNP	Plan privado de numeración (*private numbering plan*)
POTS	Servicio telefónico tradicional (*plain old telephone service*)
PSAP	Punto de respuesta de seguridad pública (*public safety answering point*)
QoE	Calidad percibida (*quality of experience*)
QoS	Calidad de servicio (*quality of service*)
QoSM	Medición de la calidad de servicio (*quality of service measurement*)

RACF Funciones de control de recursos y admisión (*resource and admission control functions*)

RDSI Red digital de servicios integrados

RTPC Red telefónica pública conmutada

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

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

SMS Servicio de mensajes cortos (*short message service*)

SR Resiliencia de servicio (*service resiliency*)

TDR Servicio de telecomunicaciones de socorro (*telecommunications for disaster relief*)

TE Equipo terminal (*terminal equipment*)

TIP Presentación de identidad de terminación (*termination identity presentation*)

TVIP Televisión con el protocolo Internet

UC Comunicación no solicitada (*unsolicited Communication*)

UDDI Descubrimiento, descripción e integración universales (*universal discovery, description and integration*)

UMTS Sistema de telecomunicaciones móviles universales (*universal mobile telecommunications system*)

UNI Interfaz usuario-red (*user to network interface*)

URI Identificador de recurso unificado (*uniform resource identifier*)

USN Red de sensores ubicua

VoD Vídeo a la carta (*video on demand*)

VoIP Transmisión de la voz mediante el protocolo Internet (*voice over Internet Protocol*)

VPN Red privada virtual (*virtual private network*)

WiFi Fidelidad inalámbrica (*wireless fidelity*)

xDSL Diversos tipos de línea digital de abonado (*digital subscriber line*)

5 Convenios

En la presente Recomendación:

La expresión "se le exige que" indica un requisito que debe cumplirse estrictamente, no permitiéndose desviación alguna si la Recomendación pretende reclamar su conformidad.

La expresión "se le prohíbe" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si el documento pretende ser conforme.

La expresión "se recomienda" indica un requisito recomendado pero que no se exige con carácter taxativo. Por ello no es necesario cumplir este requisito para reclamar su conformidad.

La expresión "no se recomienda" indica un requisito no recomendado, pero que no está prohibido. Por consiguiente, podrá afirmarse la conformidad con esta especificación aun cuando este requisito esté presente.

La expresión "puede opcionalmente" indica un requisito opcional admisible que no reviste en absoluto el carácter de Recomendación. Esta expresión no pretende dar a entender que la implementación del fabricante deba suministrar una opción o característica que puedan ser

activadas opcionalmente por el operador de red o proveedor del servicio. Más bien significa que el fabricante puede proporcionar opcionalmente esta característica sin menoscabo de su derecho de reclamar la conformidad con la especificación.

A los efectos de la presente Recomendación , se considera que los términos "red de empresa" y "red empresarial" son sinónimos y pueden utilizarse indistintamente.

6 Transporte

6.1 Conectividad de transporte

El estrato de transporte NGN [UIT-T Y.2012] utilizará el protocolo IP a fin de garantizar una conectividad pública que sea a la vez general, ubicua y mundial. Dicho protocolo puede transportarse utilizando varias tecnologías subyacentes, tanto en el acceso como en el núcleo del estrato de transporte (por ejemplo, xDSL, ATM, MPLS, retransmisión de tramas u OTN), de acuerdo con el entorno del operador en cuestión.

NOTA – Lo anterior no impide que los operadores presten directamente a sus usuarios servicios específicos de determinada tecnología (por ejemplo, ATM, MPLS, retransmisión de tramas u OTN).

En la conectividad se ha de tener en cuenta:

1) la utilización del IPv4 y del IPv6;
2) las comunicaciones en tiempo real y las que no lo son;
3) la conectividad uno a uno;
4) la conectividad entre uno y varios.

6.2 Modos de comunicación

Las NGN tendrán que aceptar los siguientes modos de comunicación:

– uno a uno;
– uno a varios;
– varios a varios;
– varios a uno.

6.3 Componentes de la red de transporte

Uno de los objetivos de las NGN es admitir servicios y aplicaciones independientemente de las tecnologías de la red de acceso y la red núcleo. Por consiguiente:

1) Las NGN soportarán varias tecnologías de función de transporte de acceso y núcleo.
2) Toda función de transporte de acceso NGN podrá proporcionar conectividad IP, al nivel del estrato de transporte, entre las funciones de usuario extremo y las funciones principales de transporte.
3) Las NGN tendrán que ser compatibles con cualquier red de usuario, sin importar su nivel de complejidad de configuración.

6.4 Anexión a la red

A continuación se presentan los requisitos de anexión a la red:

1) Las NGN soportarán el registro al nivel de la red de acceso, la inicialización de funciones de usuario extremo para el acceso a los servicios NGN, y la gestión del espacio de direcciones IP de la red de acceso, incluida la función NAT.
2) El perfil de usuario contendrá información de autenticación de acceso e información relacionada con la configuración de acceso de red requerida.

3) Las NGN tendrán que soportar la reconfiguración de los servicios a disposición del usuario, cuando este último se desplace y acceda a ellos desde una ubicación distinta de aquella en la que se abonó. Los servicios pueden depender de uno o varios de los siguientes factores: el dispositivo de usuario, la red de acceso y los acuerdos (por ejemplo, acuerdos de itinerancia) entre el proveedor de servicio y el de red de acceso. La red de acceso deberá atribuir recursos según el tipo de servicios que se vayan a prestar.

4) Cuando varias redes de acceso estén conectadas a una sola red troncal NGN, cada una de ellas deberá poder autenticar o autorizar el acceso de un usuario que llegue a ella por itinerancia desde otra red de acceso, basándose en la información obtenida de la red de acceso a la que está abonado dicho usuario.

5) Para garantizar la disponibilidad de los servicios de itinerancia, los procedimientos de conexión a la red de acceso NGN tendrán que soportar la autenticación de red de acceso basada en un método normalizado, con el fin de identificar los usuarios a nivel de la red de acceso (por ejemplo, el mecanismo de identificador de conexión de red (NAI, *network attachment identifier*) especificado en [b-IETF RFC 2486]).

6.5 Soporte de IPv6

IPv6 soporta no sólo extensiones del espacio de dirección IP, sino también diversas características avanzadas que influyen en las funciones de las NGN y las entidades funcionales pertinentes. Quiere esto decir que IPv6 tiene más flexibilidad de introducción de nuevos servicios/aplicaciones empleando la combinación de encabezamientos de extensión y opciones.

Por consiguiente, en esta cláusula se identifican los requisitos generales de las NGN IPv6, que están influidas por las características de IPv6. Las NGN IPv6 han de satisfacer los siguientes requisitos:

– las NGN IPv6 han de soportar los encabezamientos de extensión y opciones de IPv6;

– las NGN IPv6 han de aceptar los planes de direccionamiento IPv6.

6.5.1 Multidireccionamiento en las NGN IPv6

– Las NGN IPv6 han de soportar múltiples capacidades de acceso de usuario, incluidas las capacidades para acceder a las redes empleando diferentes tecnologías (por ejemplo, red móvil, Wi-Fi).

– Los terminales de usuario han de disponer de múltiples conexiones a múltiples interfaces de red y/o múltiples direcciones IPv6.

– Se recomienda que los terminales de usuario que empleen el multidireccionamiento con IPv6 adquieran (o desechen) otras direcciones IPv6 dinámicamente.

– Se recomienda que los terminales de usuario que empleen el multidireccionamiento con IPv6 adquieran (o desechen) otras interfaces de red dinámicamente.

– Las NGN IPv6 han de adquirir (o desechar) otros prefijos IPv6 dinámicamente.

6.5.2 Señalización en las NGN IPv6

1) Las NGN IPv6 han de soportar la compatibilidad de señalización con otras redes (por ejemplo, NGN IPv4).

2) Las NGN IPv6 han de soportar la señalización con un mínimo de modificaciones necesarias de los protocolos de señalización utilizados en las NGN IPv4.

6.5.3 Migración a IPv6 de las NGN

Las NGN han de soportar una función de migración a IPv6 en las funciones de transporte de acceso o de transporte de núcleo.

6.6 Soporte de multidifusión

Estas capacidades permiten a las aplicaciones entregar contenido a múltiples usuarios al mismo tiempo.

Además de las de unidifusión, es necesario que se soporten las capacidades de multidifusión a fin de utilizar eficientemente los recursos de la red y adaptar la entrega de los datos.

Los siguientes requisitos se aplican a las NGN:

1) es obligatorio ofrecer capacidades de multidifusión en un único dominio NGN;
2) se recomienda ofrecer capacidades de multidifusión en múltiples dominios NGN;
3) las NGN han de ofrecer capacidades de entrega de datos por multidifusión;
4) las NGN han de ofrecer capacidades de control de servicio de multidifusión;
5) las NGN han de soportar capacidades de gestión de grupo de multidifusión;
6) las NGN han de soportar mecanismos de seguridad para la multidifusión;
7) las NGN han de soportar el nomadismo en las comunicaciones multidifusión;
8) se recomienda que las NGN soporten capacidades de QoS de grupo de multidifusión predefinidas sin soportar la negociación de QoS;
9) se recomienda que las NGN soporten la movilidad sin solución de continuidad para las comunicaciones multidifusión;
10) las NGN pueden opcionalmente soportar la fiabilidad de las capacidades de multidifusión.

NOTA – Pueden encontrarse más detalles al respecto en [UIT-T Y.2236].

7 Soporte de servicios y aplicaciones

7.1 Entorno de servicio abierto

7.1.1 Requisitos generales del entorno de servicio abierto

Las capacidades de entorno de servicio abierto son consecuencia de las características generales de las NGN, en el sentido de que permiten soportar y establecer un entorno adecuado para la creación y configuración, dentro de un mismo estrato de servicio, de un servicio ampliado, flexible y abierto.

La puesta en marcha de nuevas funcionalidades en las redes actuales puede ser limitada o imposible, debido a las capacidades del equipo instalado. La configuración de software destinada a implementar nuevas funcionalidades se restringe esencialmente a los fabricantes de equipos, puesto que las interfaces de programación de aplicaciones (API) suelen ser patentadas (es decir, no son gratuitas).

Las NGN aceptan nuevas capacidades y soportan una amplia gama de servicios emergentes, incluidos los que cuentan con funcionalidades avanzadas y complejas. Como resultado de una iniciativa de terceras partes proveedoras de aplicaciones y servicios, consistente en desarrollar nuevas aplicaciones y capacidades a las que se pueda acceder a través de interfaces abiertas y normalizadas, hay una necesidad cada vez mayor de cooperación entre los proveedores de red y los de servicios en el desarrollo de interfaces de red de aplicación (ANI) normalizadas. Además, se recomienda soportar la reutilización y la portabilidad del software, así como la utilización de software comercial, lográndose de esta manera un desarrollo rentable.

Algunos de los beneficios generales que se pueden obtener al emplear un entorno abierto de servicio son:

– Los proveedores de red y terceros pueden desarrollar fácilmente aplicaciones y capacidades.
– Se puede lograr que las capacidades sean portátiles o reutilizables a través de las redes.

– Las ANI abiertas y normalizadas permitirán interacciones entre entidades y aplicaciones NGN (por ejemplo, para la creación de servicio).

Dentro de un entorno abierto de servicio, cada capacidad deberá poder actuar independientemente o en combinación con otras, para poner en funcionamiento las respectivas aplicaciones. Cada capacidad efectúa, a pedido de la entidad solicitante (por ejemplo, un tercero), todas las funciones de servicio que le correspondan. Se pueden configurar las aplicaciones en diferentes redes, con lo cual las capacidades han de poder funcionar sin importar cuál sea la tecnología de red subyacente.

Las NGN cumplirán los siguientes requisitos generales del entorno abierto de servicio:

1) Independencia con relación a los proveedores de red: las funcionalidades, las operaciones y la gestión de aplicaciones y servicios no dependerán de las infraestructuras de los proveedores de red ni de las tecnologías de red subyacentes.
2) Independencia con relación a los fabricantes: habrá un entorno abierto de servicio en el que existan varios fabricantes de equipos, de tal manera que los usuarios puedan contar con una amplia oferta de servicios y aplicaciones, en un ambiente de competencia.
3) Transparencia en la ubicación: en un entorno distribuido, los proveedores de servicio deberán poder utilizar las capacidades desde cualquier lugar, y sin importar dónde éstas se encuentren realmente.
4) Transparencia de red: el entorno abierto de servicio aceptará aplicaciones y servicios que ignoren los tipos de tecnología y de terminal que se estén empleando.
5) Transparencia de protocolo: la que se logra al suministrar herramientas normalizadas de interfaz de programación de protocolo, necesarias para llevar a cabo procesos independientes de control de servicio y proteger detalles técnicos de redes complejas, en el entorno abierto de servicio.
6) El acceso seguro a capacidades del entorno abierto de servicio cumplirá los requisitos generales de seguridad NGN, conforme a la cláusula 10.

NOTA – Pueden encontrarse otros requisitos para el soporte del entorno de servicio abierto en [UIT-T Y.2234].

7.2 Habilitadores de servicio

La categoría de "habilitadores de servicio" reúne capacidades que proporcionan medios para los servicios y las aplicaciones específicos o avanzados, o permiten el acceso a información específica suministrada por esas mismas capacidades o su tratamiento.

NOTA – En el apéndice II se presenta un ejemplo en que se vinculan los servicios seleccionados con los activadores de servicio seleccionados.

7.2.1 Gestión de grupo

Esta capacidad suministra funcionalidades relacionadas con la gestión segura y eficiente de grupos de entidades de red (terminales, usuarios, nodos de red, etc.). Puede servir a las aplicaciones y los servicios a varios fines, entre ellos las aplicaciones VPN, la distribución de contenidos de vídeo, la gestión de dispositivos, la configuración y gestión de redes y servicios, los servicios de emergencia (de notificación a la comunidad), etc.

Un ejemplo común en el que se requiere gestión de grupo es el de un servicio VPN prestado por un operador de red. Tratándose de una VPN, se tiene que definir un grupo cerrado con la lista de los usuarios del servicio, cuyas comunicaciones se recomienda proteger con relación a los otros usuarios. Se recomienda que las NGN gestionen este tipo de grupos y proporcionen comunicaciones seguras dentro de cada uno de ellos.

Otro ejemplo es la distribución simultánea, por parte de una fuente de multidifusión, de contenidos de vídeo hacia varios usuarios de un grupo. En este tipo de aplicación, también es fundamental la capacidad de gestión de grupo. Los requisitos de la gestión de grupo son:

1) Las NGN proveerán una capacidad que permita la creación de grupos en el estrato de transporte.

2) Las NGN proveerán una capacidad que permita la creación de grupos de servicios o grupos específicos de un servicio (en el estrato de servicio).

3) Las NGN gestionarán grupos, y permitirán la comunicación de grupos segura.

7.2.2 Gestión de información personal

Esta capacidad permite la gestión de información estática y dinámica, específica de aplicación (relacionada con el usuario y con el contexto de comunicación). Algunos ejemplos de información específica de aplicación son: información de contacto de usuario, sobre membresía de la aplicación (contraseña, etc.), de parámetros -por defecto- de aplicación, de preferencias de ancho de banda o QoS (por ejemplo, según las redes de acceso disponibles), de preferencias de medios, especificada por el usuario, etc. Esta información es suministrada por las aplicaciones (por ejemplo, por los servicios de notificación e información) con arreglo a ciertas preferencias predefinidas por el usuario y algunos atributos de política (en diversos dispositivos móviles y varios tipos de red de acceso), y puede almacenarse y ser gestionada por la capacidad de gestión de información personal, a nombre de los usuarios. La capacidad de gestión de la información personal, en su calidad de representante del usuario ante las aplicaciones, también puede obtener esta información de las aplicaciones a nombre de los usuarios.

Los requisitos que ha de cumplir la capacidad de gestión de la información personal son:

1) Se puede opcionalmente proveer una capacidad de gestión de la información personal. Ésta puede almacenar y gestionar, a nombre de los usuarios, información estática y dinámica, específica de aplicación; también puede obtenerla de las aplicaciones, a nombre de ellos mismos.

2) Debería protegerse la información gestionada por la capacidad de gestión de la información personal contra las operaciones no autorizadas de acceso, extracción o manipulación, etc.

3) Se recomienda que la capacidad de gestión de la información personal soporte diferentes contextos de comunicación.

7.2.3 Tratamiento de mensajes

En las redes de hoy en día se soportan algunos servicios tanto en los entornos alámbricos como en los inalámbricos, mientras que otros son exclusivos de uno solo de ellos. Por ejemplo, si bien el servicio de mensajes cortos (SMS) se diseñó teniendo en mente un ámbito inalámbrico, ya existe también en algunas redes fijas; la mensajería instantánea, por su parte, se creó pensando en redes alámbricas, y no obstante algunas redes móviles ya cuentan con ese servicio. Las expectativas de los diferentes servicios también varían, al haberse diseñado algunos de ellos como servicios "en tiempo real", mientras que otros pertenecen al tipo de servicios "casilla de correo", es decir que el mensaje se almacena para ser entregado después.

La capacidad de tratamiento de mensajes proporciona funcionalidades para los servicios basados en mensajes, entre las que está el control de servicio de mensajería instantáneo y en diferido. Algunos ejemplos de mensajería en tiempo real son el IM y el de conversación (chat), y del otro tipo son el correo electrónico, y los servicios SMS y de mensajería multimedios (MMS, *multimedia messaging service*).

Los requisitos generales son:

1) La capacidad de tratamiento de mensajes NGN soportará servicios de mensajería a los que se pueda acceder desde ambos tipos de terminales, móviles y fijos.

2) La capacidad de tratamiento de mensajes NGN soportará servicios de mensajería instantánea y en diferido.

NOTA – Puede ocurrir que el soporte de servicios de mensajería también requiera la capacidad de gestión de grupo.

Además, hay requisitos de usuario necesarios para que la capacidad de tratamiento de mensajes implemente características de configuración de servicios de mensajes, tales como la selección, el filtrado, el formateado, y el procesamiento y la gestión de grupo (por ejemplo, el aislamiento de grandes volúmenes de telecomunicación no solicitada).

7.2.4 Presencia

La capacidad (servicio) de presencia es la que permite tener acceso a información relacionada con la presencia y su disponibilidad para los usuarios y los servicios. Por presencia se entiende el conjunto de atributos que caracterizan las propiedades actuales (por ejemplo, estado, ubicación, etc.) de una entidad.

Una entidad es, a este respecto, cualquier dispositivo, servicio, aplicación, etc., capaz de suministrar información de presencia. Por otra parte, la disponibilidad indica la capacidad y disposición que tiene una entidad para comunicarse, sobre la base de diversas propiedades y políticas asociadas con dicha entidad -por ejemplo, la hora, las capacidades del dispositivo, las preferencias y capacidades de medios, etc. Los conceptos de presencia y disponibilidad se emplean casi siempre al mismo tiempo para ofrecer un conjunto completo de información de presencia.

Los usuarios de las NGN podrán ser tanto proveedores de información de presencia (algunas veces denominados entidades presentes [b-ETSI TR 121.905]), como sus solicitantes (observadores).

La capacidad de presencia se obtiene a través de tres grupos de capacidades, cuyos requisitos se describen a continuación.

Recolección de información de presencia:

1) Las NGN proveerán una capacidad para recolectar información que describa el estado de conectividad de la entidad presente, por ejemplo, el o los dispositivos empleados por un usuario.

2) Las NGN proveerán una capacidad para recolectar información relacionada con la ubicación de la entidad presente, de conformidad con las leyes y reglamentos nacionales.

3) Las NGN ofrecerán una capacidad para recolectar información relativa al contenido multimedios de la entidad presente.

4) Las NGN ofrecerán una capacidad para agrupar la información de presencia de múltiples entidades presentes.

Distribución de presencia:

5) Las NGN proveerán una capacidad para habilitar una entidad, por ejemplo, un usuario, a ser informada del estado actual de presencia de la entidad presente. Otro ejemplo es el de la utilización de esta capacidad con el fin de permitir a otro servicio acceder a la información de presencia del usuario.

6) las NGN ofrecerán una capacidad para distribuir la información relativa al contenido multimedios de la entidad presente.

7) las NGN ofrecerán una capacidad para enviar notificaciones por tandas a múltiples entidades presentes.

8) las NGN han de distribuir la información de presencia basándose en el tiempo de expiración (duración), que puede ser un evento temporal o un periodo de validez.

Gestión de presencia:

9) Las NGN han de ofrecer la gestión de presencia, un conjunto de capacidades para gestionar la información de presencia recolectada.

10) Se gestionará el control de acceso a la información de presencia (a través de las capacidades de distribución de información de presencia) conforme a los requisitos de las reglas de acceso y privacidad de la entidad presente.

11) Las capacidades de gestión de información de presencia darán a la capacidad de distribución la posibilidad de suministrar sólo una parte de la información de presencia cuando se requiera.

12) Las capacidades de gestión de información de presencia aceptarán la recolección de peticiones, provenientes de ciertas entidades, tendientes a obtener información de presencia para otras entidades. De igual manera, se ofrece a la entidad presente la posibilidad de incidir en la distribución de su información de presencia, por ejemplo, para aceptar o rechazar peticiones según de cuál observador provengan.

7.2.5 Gestión de la ubicación

Capacidad que permite prestar servicios y aplicaciones basados en la ubicación, que utilizan información sobre la ubicación de los usuarios y de los dispositivos en la red. La ubicación de los usuarios y los dispositivos en la red puede ser su posición física real, lo que da más importancia a las aplicaciones que tienen contexto y relevancia locales.

Con frecuencia, los mecanismos que permiten establecer y comunicar la información relativa a la ubicación dependen de la tecnología de red de acceso, es decir que se recomienda implementar el soporte de las aplicaciones y servicios basados en la ubicación, para cada una de dichas tecnologías.

Los requisitos que ha de cumplir la gestión de la ubicación son:

1) Las NGN proporcionarán una capacidad de gestión de la ubicación para determinar e informar sobre la ubicación de usuarios y dispositivos dentro de las NGN.

2) Las NGN proporcionarán funcionalidades adicionales que sirvan para garantizar la exactitud y autenticidad de la información de ubicación utilizada por aplicaciones y servicios, con el fin de mitigar posibles efectos adversos causados por información fraudulenta o falsa.

3) Al configurar servicios y aplicaciones basados en la ubicación, se tendrán en cuenta los aspectos relacionados con la privacidad.

4) La capacidad de gestión de la ubicación proveerá un medio para publicar la información de ubicación, de acuerdo con la información que se tenga en los perfiles de usuarios y dispositivos.

7.2.6 Mecanismo de envío de información sin solicitud por parte del destinatario

Este mecanismo otorga la capacidad de transmitir información desde un remitente hasta un receptor, sin que este último tenga que solicitarlo previamente, por ejemplo, utilizando el mecanismo "push" basado en el SIP.

Si bien el usuario puede configurar estos servicios a partir de una gama de servicios prestados por los proveedores, el receptor no necesita emitir una petición específica relacionada con la información que se va a enviar. Ésta puede ser enviada como resultado de una invocación de activador que depende de la aplicación o periódicamente.

Así, por ejemplo, se puede utilizar este mecanismo para notificar la disponibilidad de un mensaje MMS.

El requisito del "push" es:

1) Las NGN soportarán la capacidad de envío de información sin solicitud por parte del destinatario en conformidad con la legislación nacional.

NOTA – La invocación de estos servicios puede requerir el acuerdo del usuario.

7.2.7 Gestión de dispositivo

Gracias a la gestión de dispositivo, la red cuenta con capacidades de gestión y control de dispositivos, que pueden servir para:

– La gestión de configuración de hardware o de software, por ejemplo la información relativa al hardware del dispositivo, las capacidades de medios y la versión del software.

– Las actualizaciones a distancia del software, con o sin la intervención del usuario, por ejemplo la corrección de errores, características, OS, software patentado, clientes de aplicación.

– El diagnóstico de fallos a distancia.

Los requisitos generales que ha de cumplir la gestión de dispositivo son:

1) Las NGN soportarán las actualizaciones de dispositivo.

2) Las NGN soportarán la autoconfiguración de dispositivo.

3) Las NGN soportarán la recolección de información de conexión de dispositivo, por ejemplo de la dirección IP y de la ubicación.

4) La gestión de dispositivo puede opcionalmente suministrar funciones de registro, gestión y actualización de información de dispositivo.

5) La gestión de dispositivo puede opcionalmente suministrar funciones para verificar a distancia el estado del dispositivo, incluidos los cambios y actualizaciones de dicho estado, y la generación de informes de diagnóstico.

6) La gestión de dispositivo será segura, y siempre la efectuará una entidad fiable en conformidad con la legislación nacional.

NOTA 1 – Se recomienda que la gestión de dispositivo permita instalar preferencias y aplicaciones de usuario.

NOTA 2 – Puede ocurrir que sea necesario el acuerdo del usuario a la hora de invocar los servicios de gestión de dispositivo.

7.2.8 Tratamiento de sesión

Las NGN proporcionarán las capacidades necesarias para establecer, gestionar y terminar sesiones de servicio extremo a extremo que abarquen, por ejemplo, varias partes, un grupo de puntos extremos asociados con dichas partes, y una descripción de las conexiones multimedios entre los puntos extremos. Estas capacidades deben ser suministradas tanto para entornos de red fija como para los de red móvil, con el fin de poder satisfacer diferentes requisitos de servicio y utilizar los servidores de aplicación adecuados para el funcionamiento del servicio.

Las funciones de tratamiento de sesión son las siguientes:

– establecimiento de sesión;

– presentación de la identidad de la parte que origina y de la parte a la que se está conectado en una sesión;

– supresión de la identidad de la parte que origina y de la parte a la que se está conectado en una sesión;

– entrega y supresión de información facultativa proporcionada por el usuario (por ejemplo, imágenes, vídeo o texto, durante el establecimiento de sesión);

– tratamiento de una sesión entrante por la parte donde termina la sesión;

– negociación de capacidad para una sesión entrante;
– aceptación, omisión, redirección o rechazo de una sesión entrante;
– negociación de medios y de sus componentes durante el establecimiento de sesión;
– tratamiento de una sesión en curso;
– modificación de medios y de sus componentes durante una sesión en curso;
– suspensión y reinicio de una sesión en curso;
– fin de una sesión;
– terminación de sesión controlada por la red.

Los requisitos generales que ha de cumplir el tratamiento de sesión son:

1) El tratamiento de sesión utilizará los servidores de aplicación adecuados para el funcionamiento de servicio.
2) El usuario podrá invocar una o varias sesiones y activar aplicaciones multimedios, que compitan entre ellas, dentro de cada sesión.
3) El tratamiento de sesión soportará sesiones en diversos tipos de medios (voz, vídeo, texto).
4) Se soportará el control de admisión de sesión basado en niveles definidos de QoS y de seguridad.
5) Los mecanismos de control de admisión de sesión cubrirán múltiples servicios (por ejemplo, voz, texto y vídeo).
6) Si hay uno o dos participantes en la sesión, la red puede opcionalmente terminar la sesión en cualquier momento a petición de cualquiera de los usuarios de la sesión. La red puede opcionalmente terminar por sí misma una sesión en cualquier momento de ésta (por ejemplo, en condiciones de fallo).
7) Si hay más de dos participantes en la sesión la red puede opcionalmente terminar la sesión en cualquier momento a petición de cualquiera de los usuarios de la sesión. La red puede opcionalmente terminar por sí misma una sesión en cualquier momento de ésta (por ejemplo, en condiciones de fallo).

7.2.9 Soporte de aplicación a través de la web

Gracias a él, es posible mejorar la utilización de las capacidades de dispositivo y de las características de red, en el caso de aplicaciones basadas en la web.

Las capacidades de soporte de este tipo de aplicaciones permiten al usuario disponer de un entono web coherente que abarca varios entornos de red (local, en la oficina, en un vehículo, etc.) y varios dispositivos (PC, computador portátil, PDA, teléfono celular, etc.).

Las interacciones que conforman este soporte son:

– (aplicación) servidor a servidor;
– servidor a terminal;
– terminal a servidor;
– terminal a terminal (o par a par).

Las NGN proveerán un soporte de aplicaciones basadas en la web que satisfaga lo siguiente:

1) la interoperabilidad entre entornos de red alámbricos e inalámbricos;
2) el acceso seguro a las aplicaciones;
3) el nomadismo;
4) bajos retrasos de tiempo de aplicación y una utilización eficaz del ancho de banda.

Se recomienda que las NGN provean un soporte de aplicaciones basadas en la web que satisfaga lo siguiente:

5) la reutilización de las tecnologías existentes y de los componentes NGN (por ejemplo, autenticación) en la configuración de las aplicaciones basadas en la web.

6) la reutilización de las herramientas de elaboración e integración;

7) la coherencia para el usuario a través de las redes;

8) el soporte de técnicas de composición de servicio;

9) la escalabilidad de aplicaciones basadas en la web;

10) la no degradación de la fiabilidad NGN.

NOTA – Es posible que las NGN estén limitadas en lo que tiene que ver con las capacidades de soporte de aplicaciones basadas en la web.

7.2.10 Sincronización de datos

Se entiende por sincronización de datos el acto de establecer una equivalencia entre dos conjuntos de datos. Esta característica permite sincronizar datos enviados por la red desde diferentes terminales, incluidos las agendas digitales, los teléfonos móviles, los computadores portátiles y los PC. Las aplicaciones que pueden necesitar sincronización son, por ejemplo, las de calendarios, la gestión de información de contacto, la gestión de información empresarial almacenada en bases de datos y la gestión de documentos web.

Se recomienda que las NGN soporten un sincronizador de datos con las capacidades siguientes:

1) La sincronización de datos transmitidos por la red desde y hacia terminales que soportan esta capacidad.

2) La sincronización de un terminal con los datos correspondientes transmitidos por la red.

3) La sincronización de datos transmitidos entre los diferentes terminales.

Sin un sincronizador de datos está soportado, los siguientes requisitos se aplican:

1) La capacidad de sincronización de datos no dependerá del protocolo de transporte.

2) Se soportará la información transmitida arbitrariamente por la red.

3) Se recomienda que la capacidad de sincronización de datos conozca las limitaciones de recursos de los terminales.

7.3 Conocimiento del contexto

El conocimiento del contexto es la capacidad para determinar o influir en la siguiente acción o proceso de telecomunicaciones mediante remisión al estado de las entidades pertinentes, que forman un entorno coherente como contexto. El estado de cada entidad y su estado combinado se tratan como información de contexto. Ejemplos de información de contexto son la conectividad del abonado, la ubicación de bienes seleccionados en un sistema de distribución y el estado del tráfico en la red.

Se asumen las siguientes funciones principales:

- **Generador de contexto**: Genera información de contexto y permite acceder a ella. El generador de contexto puede estar dentro o fuera de una NGN.
- **Solicitante de contexto**: Solicita información de contexto y se refiere a ella. Puede estar dentro o fuera de una NGN.
- **Distribuidor de contexto**: Recopila, distribuye, procesa y, opcionalmente, almacena información de contexto, ejerciendo de mediador entre el generador de contexto y el solicitante de contexto.

Cuando estas funciones las realiza la NGN, se recomienda que ésta facilite:

1) Seguridad de la información de contexto desde el punto de vista del generador de contexto:
   - El solicitante de contexto deberá acceder a la información de contexto sólo cuando el generador de contexto se lo permita. Es necesario mantener esta política durante todo el tiempo en que la información de contexto esté activa en la NGN.
   - El rastreo involuntario del generador de contexto ha de estar obligatoriamente prohibido.

     NOTA – Este requisito supone que la información de contexto de un generador de contexto está abierta a distintos solicitantes de contexto por distintos motivos. Ha de estar relacionada únicamente a un fin determinado. Por ejemplo, aunque un generador de contexto permita a un usuario acceder a su historial de compra de libros (para obtener información sobre posibles nuevas publicaciones), se prohíbe terminantemente que otras aplicaciones, como de distribución de publicidad sobre entradas de cine, discos de música o ropa deportiva, conozcan esta información.
   - No deberá haber fugas o abusos de información de contexto en el proceso de distribución de la NGN.
   - No deberá haber fugas o abusos de la información de contexto almacenada en la base de datos de una NGN.
2) Fiabilidad de la información de contexto desde el punto de vista del solicitante de contexto:
   - Se recomienda que la información de contexto se transfiera de manera transparente al solicitante de contexto sin modificarla.
   - Se recomienda transferir al solicitante de contexto la información de contexto más reciente.
   - Conviene abandonar automáticamente la información de contexto antigua.
   - No se podrá generar o abrir información de contexto falsa.
3) Facilidad de utilización de la información de contexto desde el punto de vista del solicitante de contexto/proveedor de aplicación:
   - Se recomienda normalizar el formato y la semántica de datos de la información de contexto de manera que diversos solicitantes de contexto/proveedores de aplicación puedan utilizarla.
   - Se recomienda que el solicitante de contexto, si se le permite, puede buscar fácilmente la información de contexto.
   - Se recomienda que el solicitante de contexto pueda, si se le permite, utilizar la información de contexto en cualquier momento.
   - La información de contexto primaria puede opcionalmente convertirse en información de contexto adecuada a fin de que el proveedor de aplicación pueda fácilmente desarrollar una aplicación utilizando la información de contexto convertida.
   - El distribuidor de contexto puede opcionalmente seleccionar automáticamente elementos y datos de servicio de entre varias alternativas a fin de que un creador de aplicación tercero pueda fácilmente desarrollar una aplicación empleando la información de contexto.
4) La información de contexto se transferirá en tiempo real o a la demanda, si el solicitante de contexto así lo desea.
5) Adaptabilidad del distribuidor de contenido.
   - Se recomienda manejar grandes cantidades de información de contexto a fin de evitar las inferencias erróneas a partir de información de contexto limitada.

– Se recomienda que el distribuidor de contexto sea flexible a fin de manejar diversos tipos de información de contexto y soportar distintas aplicaciones.

6) Distribución eficaz de la información de contenido.

8 Encaminamiento

Las NGN proporcionarán capacidades de selección de trayectos apropiados de encaminamiento entre el punto extremo que origina el tráfico y el que lo recibe.

Las NGN soportarán los métodos de encaminamiento más adecuados para los proveedores de servicios NGN. En particular, soportarán:

1) métodos de encaminamiento tanto estáticos como dinámicos;

2) métodos de encaminamiento que puedan funcionar efectivamente dentro de una sola NGN;

3) métodos de encaminamiento que puedan funcionar efectivamente dentro de varias NGN, con lo cual se permite la interoperabilidad;

4) encaminamiento basado en las gamas de números [UIT-T. E.164];

Se recomienda que las NGN soporten:

5) el encaminamiento basado en el conocimiento del contexto (por ejemplo, encaminamiento basado en la presencia, la ubicación y la información personal).

NOTA – En la cláusula 7.3 se presenta más información sobre el conocimiento del contexto.

9 Calidad de servicio

Las NGN deberán soportar la QoS extremo a extremo a través de diferentes redes, con diversas tecnologías de infraestructura proporcionadas por varios operadores, a fin de garantizar el nivel de servicio requerido por los usuarios o por las aplicaciones. Las NGN aceptarán varios niveles de QoS, que pueden ser negociados entre el usuario y el proveedor, y/o entre proveedores. Lo anterior incluye la utilización de mecanismos de control de recursos y admisión, la diferenciación de clases de tráfico, la gestión de la prioridad, los mecanismos de señalización de QoS, la medición y la gestión de la calidad de funcionamiento para garantizar la calidad, y el control de la sobrecarga o de la congestión.

9.1 Requisitos generales de QoS

Las NGN deberán satisfacer los siguientes requisitos de QoS:

1) Admitir diferentes tecnologías y modelos comerciales.

2) Soportar los diversos procesos relacionados con la duración del servicio (por ejemplo, abonamiento/configuración, invocación, supervisión).

3) Aceptar diferentes capacidades de los CPE (por ejemplo, es posible que algunos CPE acepten la señalización en el estrato de transporte, mientras que otros no).

4) Controlar los recursos de transporte relacionados con la QoS en las redes de paquetes y en las fronteras de red, conforme a sus capacidades [UIT.T Y.2111].

5) Admitir el control de recursos y admisión dentro de una NGN y entre varias de ellas.

6) Admitir el control relativo de la QoS y el control absoluto de la QoS [UIT-T Y.2111].

7) Admitir requisitos de QoS orientados a la aplicación.

8) Verificar la disponibilidad de recursos de transporte de extremo a extremo [UIT-T Y.2111].

9) Admitir la diferenciación de QoS entre diversas categorías de tráfico de paquetes, incluidos los flujos de paquetes y designaciones de usuario [UIT-T Y.2111].

10) Autorizar peticiones de QoS y funcionar únicamente en función de las peticiones autorizadas [UIT-T Y.2111].

11) Admitir el control NAPT de extremo cercano dinámico y la selección de modo de funcionamiento cortafuegos [UIT-T Y.2111].

12) Admitir el NAT de extremo lejano (distante) transversal [UIT-T Y.2111].

13) Facilitar control de recursos y admisión para la multidifusión a fin de soportar, por ejemplo, la TVIP [UIT-T Y.2111].

14) Facilitar control de recursos y admisión para el soporte del nomadismo [UIT-T Y.2111].

9.2 Clases de QoS de red

1) Se recomienda que las NGN tengan en cuenta la calidad de funcionamiento de red en el estrato de transporte.

2) Se recomienda que las NGN soporten clases de QoS NGN basadas en [UIT-T Y.1541].

9.3 Prioridad de servicio o de aplicación

Se recomienda que las NGN tengan prioridad de servicio o de aplicación, a saber:

1) esquemas de clasificación de prioridad para el control de admisión y restauración;

2) extensiones de señalización que indiquen niveles de prioridad a través de la UNI, la NNI y la ANI;

3) mecanismos de activación de prioridad que ejecuten la acción de prioridad deseada.

9.4 Control de QoS

Se recomienda que las NGN soporten:

1) la granularidad de control de QoS por flujo, por sesión y por clase de servicio;

2) el comportamiento dinámico de la QoS (es decir, se recomienda que sea posible modificar los atributos de QoS durante una sesión activa);

3) el control de recursos de QoS basado en un método distribuido, centralizado o híbrido;

4) los mecanismos de control de admisión y control de congestión;

5) los mecanismos necesarios para garantizar la entrega oportuna y fiable de paquetes de señalización y control;

6) los mecanismos necesarios para prestar con prioridad los servicios de telecomunicaciones de emergencia y de telecomunicaciones de carácter prioritario;

7) los métodos de control de admisión en función de los recursos, por ejemplo, utilizando la información de medición de la calidad de funcionamiento.

9.5 Señalización de QoS

Se recomienda que las NGN utilicen mecanismos de señalización con el fin de soportar la QoS.

La descripción de los requisitos de señalización de QoS está fuera del alcance de esta Recomendación, y se trata en otras Recomendaciones.

9.6 Calidad de funcionamiento

Para garantizar la QoS, las NGN han de permitir la medición y la gestión de la calidad de funcionamiento.

Se recomienda que las mediciones de la calidad de funcionamiento y su gestión admitan:

1) la garantía de prestación, por parte de los proveedores, de la calidad de funcionamiento de red de cliente (para poder comparar con los SLA);
2) el suministro por los proveedores de información de calidad de funcionamiento a clientes potenciales;
3) la solución de problemas por parte de los proveedores, en su redes, a lo largo de trayectos definidos;
4) la indicación interna del proveedor de cualquier efecto sobre la calidad de servicio provocado por modificaciones a sus redes;
5) la supervisión mutua entre proveedores de la calidad de funcionamiento de sus redes;
6) el suministro de información a otras funciones NGN, por ejemplo, a la RACF.

La descripción de los requisitos de medición y gestión de la calidad de funcionamiento está fuera del alcance de esta Recomendación, y se trata en otras Recomendaciones.

9.7 Gestión de procesamiento y de tráfico

Con el fin de impedir una sobrecarga de procesamiento y de tráfico, y de mantener el tiempo de respuesta a un nivel razonablemente bajo, evitando así que los usuarios desistan de sus solicitudes de servicio, se recomienda que las NGN provean mecanismos de detección y control de sobrecarga (incluidos controles expansivos, tales como el equilibrio de carga y la replicación de recursos) tanto en el servicio como en el estrato de transporte.

Se recomienda que las NGN dispongan de mecanismos de control de sobrecarga que:

1) indiquen a otras redes las condiciones y el grado de sobrecarga;
2) optimicen el caudal efectivo (por ejemplo, las solicitudes de servicio o los paquetes admitidos por segundo), teniendo en cuenta las prioridades de servicio en el recurso sobrecargado;
3) logren lo anterior durante todo el evento de sobrecarga, sin importar la capacidad del recurso sobrecargado o la cantidad de fuentes de sobrecarga;
4) permitan que la red que recibe la indicación de sobrecarga controle el tráfico.

10 Identificación y seguridad

NOTA – La utilización en esta cláusula del término "identidad" no implica su significado absoluto. En concreto, no constituye la validación positiva de una persona.

10.1 Requisitos generales de identificación, autentificación y autorización

Los requisitos especificados en esta cláusula no se circunscriben a ningún conjunto de servicios NGN en particular.

NOTA 1 – Los mecanismos de autenticación y autorización están fuera del alcance de esta Recomendación.

Las capacidades de identificación, de autenticación y de autorización deben cumplir ciertos requisitos en ambos estratos, el de transporte y el de servicio. En el primero de ellos, se trata de requisitos sobre cómo se pueden utilizar los recursos de transporte NGN. En el otro, los requisitos atañen a la asociación entre un usuario y un servicio, o entre dos usuarios, incluido el caso en que ambos usuarios estén en redes NGN diferentes.

NOTA 2 – Algunas veces se ha empleado la expresión "proveedor de servicio" para referirse al proveedor de servicios del estrato de transporte. En esta cláusula, el proveedor de red se denomina simplemente "(la) NGN," y el "proveedor de servicio" es exactamente eso: quien provee el servicio, que puede estar en cualquier lugar y no tiene por qué ser el proveedor de red.

Los requisitos generales para las capacidades de identificación, autenticación y autorización son:

1) Las NGN soportarán funciones de autenticación y autorización para ambos estratos, el de transporte y el de servicio. Para la autenticación de estrato de transporte se requiere que la red identifique a un usuario, antes de que éste obtenga acceso a ella y a funciones privilegiadas. Una función de autenticación puede ser importante cuando se trate de impedir la utilización no autorizada de las redes, por ejemplo, para evitar que se efectúen comunicaciones no solicitadas de gran cantidad de datos. Gracias a la función de autorización, se crea una autoridad que controla el acceso a los recursos de red y se contrarresta la violación de acceso.

2) Cada usuario de las NGN será identificado unívocamente mediante uno de los siguientes tipos de NUI, o ambos:
   - Identidad pública de usuario: información que suele emplear un usuario NGN para comunicarse con otro usuario.
   - Identidad privada de usuario: la que puede utilizar un usuario NGN para identificarse ante su red o proveedor de servicio NGN. La NUI privada es un componente utilizado para la autenticación.

3) Las NGN permitirán la identificación, la autenticación y la autorización separadas, tanto de usuarios como de equipo terminal.

4) Las NGN permitirán la verificación de la asociación entre el usuario y el equipo terminal de usuario, en el caso de algunos servicios específicos.

5) Se recomienda procesar de modo seguro la autenticación, la autorización y la tasación efectuadas por el proveedor de red y el de servicio NGN.

6) Un proveedor de servicio suministrará los mecanismos necesarios para la presentación de la identidad pública de quien origina la comunicación, cuando corresponda y sea permitido.

7) Un proveedor de servicio suministrará los mecanismos necesarios para retener la identidad pública de quien origina la comunicación, si éste o la red restringen su presentación.

8) Un proveedor de servicio que realice autenticaciones tendrá que soportar mecanismos para establecer la autenticidad de una identidad pública de usuario presentada en una comunicación entrante.

9) Un proveedor de servicio que realice autenticaciones tendrá que soportar mecanismos para la presentación de la identidad pública de usuario de la parte conectada a quien origina la comunicación, si viene al caso y si no ha sido restringido por dicha parte o por la red.

10) Las NGN deberán poder verificar la identidad privada de usuarios y terminales (si las hubiere). Además, serán capaces de verificar la autenticación y la autorización de usuarios y terminales que vayan a utilizar los recursos NGN.

11) Un proveedor de servicio deberá poder verificar la identidad privada de los usuarios de los servicios que presta. Además, también deberá poder verificar la autenticación y la autorización de usuarios que vayan a utilizar recursos que él gestiona.

12) Las identidades públicas y privadas de los usuarios NGN que utilizan recursos del estrato de transporte (identidades que se emplean para la autenticación y la autorización) serán administradas por el operador de red correspondiente.

13) Las identidades públicas y privadas de los usuarios NGN que utilizan recursos del estrato de servicio (identidades que se emplean para la autenticación, la autorización y el encaminamiento) serán administradas por el operador de red correspondiente, y el usuario no podrá modificarlas.

14) Las identidades privadas de los usuarios NGN, proporcionadas a los efectos de autenticación o autorización, no podrán en ningún caso ser visibles para los otros usuarios.

15) Las identidades públicas de los usuarios de servicios NGN pueden opcionalmente ser visibles para los otros usuarios siempre que no participen intermediarios.

16) Un proveedor de servicio puede opcionalmente permitir a un usuario acceder a un servicio desde varios terminales en paralelo, utilizando la misma identidad pública y privada.

17) Puede ser posible que un usuario tenga varias identidades privadas de usuario, a través de un solo procedimiento de abonado.

18) Puede opcionalmente ser posible emplear una sola autenticación y autorización de usuario para varios servicios (firma única).

NOTA 3 – Aunque se requiera un solo evento de autenticación, puede ocurrir que se necesiten varios eventos de autorización. Además, en el lado del cliente se puede implementar la firma única, de manera que aunque se requieran varias autenticaciones, la persona que utiliza el sistema sólo tenga que efectuar la autenticación una vez. Aunque en de las NGN no se requiere el soporte de capacidades de firma única, siempre que las tecnologías actuales la soporten se espera que también se emplee con las NGN.`

La autenticación del identificador de un abonado o usuario no está destinada a la validación positiva de una persona.

10.2 Requisitos de identificación

En las NGN se incluyen capacidades para la identificación de usuario, con lo cual los operadores de red y los proveedores de servicio pueden identificar a los usuarios de ciertos servicios NGN, y utilizar esta información para lo que sea necesario (por ejemplo, para los procedimientos de autenticación y autorización). Las NGN han de ofrecer capacidades para que el usuario identifique a los proveedores NGN (en todos los estratos) cuando existe una relación directa.

Los requisitos que debe cumplir la capacidad de identificación son:

1) Identidades múltiples de usuario

Un usuario NGN podrá tener varias identidades públicas y privadas, que deberán poder distinguirse entre sí (por ejemplo, para uso personal y comercial).

2) Portabilidad de identidad

Las NGN proporcionarán capacidades que permitan contar con una portabilidad de identidad equivalente a la de número en los entornos RTPC.

3) Independencia de identidad

Se recomienda atribuir la NUI pública al usuario, sin importar su repositorio, el terminal de usuario ni las tecnologías de red subyacentes. No obstante, es posible lograr la compatibilidad con versiones anteriores (por ejemplo, el microteléfono POTS) utilizando las funciones de interfuncionamiento adecuadas.

4) Soporte de atributos de identidad

La información de atributo de identidad privada, como por ejemplo desde cuándo es válida dicha entidad de usuario, el abonado, la red que se utiliza, etc., se puede opcionalmente asociar con una entidad de usuario.

5) Soporte de condiciones de atributo

Un proveedor de atributo (por ejemplo, red, usuario principal, usuario extremo) puede opcionalmente asociar a la identidad de usuario las condiciones (por ejemplo, la fijación de un temporizador como condición de validez) que debe cumplir un atributo de usuario.

6) Autorización selectiva de atributo

Las NGN soportarán la autorización selectiva de información de atributo de identidad privada de usuario por parte de un proveedor de atributo (por ejemplo, la validez de la identidad).

7) Soporte de la programación de abonado

Se recomienda que las NGN soporten la programación por parte del abonado de varios permisos para diferente información de atributo, por ejemplo, el acceso y la utilización de información de atributo de identidad privada, atributo por atributo.

8) Vinculación de usuario y terminal

Las NGN soportarán, para ciertos servicios, una vinculación dinámica de la identidad pública de usuario y la identidad de equipo terminal.

9) Asociación a terminales múltiples

Las NGN deberán permitir, para ciertos servicios, la asociación de la identidad privada o pública de usuario a varias identidades de equipo terminal (móvil o fijo). Es posible que se permita al usuario utilizar varios terminales en un momento determinado.

10) Transferencia de información de identidad

Las NGN soportarán, para ciertos servicios, la transferencia de información NUI por parte de usuarios NGN que introduzcan información bien sea en sus propios terminales o en el terminal de recepción (por ejemplo, terminal en el punto de venta).

11) Administración de identificador de usuario público

El identificador de usuario público habrá de ser administrado por el operador de red y el usuario no podrá modificarlo.

12) Autenticidad del identificador de usuario público

El operador de red tendrá que garantizar la autenticidad de un identificador de usuario público presentado para una sesión entrante a un usuario cuando la comunicación se realiza enteramente dentro de una red fiable.

10.3 Requisitos de autentificación

La autentificación es el proceso mediante el cual se verifican las identidades de usuario y de equipo terminal. Desde la óptica del proveedor, una NGN puede distinguir entre autentificación de red y autentificación de servicio. Para un usuario, por su parte, una NGN puede distinguir entre autentificación de usuario y de equipo terminal. La autentificación de red es el proceso a través del cual los proveedores de red verifican las identidades de usuario o de equipo terminal, para el acceso de red. La autentificación de servicio es aquella en la que se verifican las identidades de usuario o de equipo terminal a los efectos de utilización de un servicio. Desde el punto de vista de los abonados, las NGN deben ofrecer a un utilizador la capacidad de autentificar e identificar un proveedor de red de transporte.

Desde el punto de vista de los abonados, la NGN debe ofrecer a un utilizador la capacidad de autentificar e identificar un proveedor de servicio.

Se recomienda que la NGN asegure la independencia de sus capacidades.

Estos conceptos de identificación se pueden unificar en uno solo o utilizar separadamente, según la tecnología de transporte o el modelo comercial empleados. Por ejemplo, cuando el proveedor de red sea también el de servicio, se puede emplear un solo flujo de autentificación.

Los requisitos que debe cumplir la capacidad de autenticación son:

1) Las NGN admitirán la utilización de varios mecanismos de autentificación de red, conforme a las tecnologías subyacentes de red de acceso.

2) Se recomienda que la autentificación de servicio sea independiente de la tecnología de red de acceso NGN y mantener un mecanismo coherente de autentificación de servicio.

3) Las NGN podrán solicitar al usuario o al equipo terminal que suministren información de autentificación, de manera explícita o implícita.

4) Se recomienda que las NGN admitan mecanismos de autentificación basados en soporte lógico y físico.

5) Se aceptará la autentificación de equipo terminal mediante información de perfil de dispositivo.

6) Se recomienda que las NGN provean capacidades de autentificación mutua entre el proveedor de servicio y el usuario.

7) Se recomienda que una red NGN provea capacidades de autentificación recíproca entre el proveedor de red de transporte y el usuario.

10.4 Requisitos de autorización

Los requisitos que debe cumplir la capacidad de autorización son:

1) Las NGN permitirán el acceso al servicio a usuarios o dispositivos autenticados basándose en sus derechos de acceso, perfiles de usuario y política de red.

2) Se recomienda que la autorización de servicio sea independiente de las tecnologías de red de acceso NGN.

3) Se recomienda que la capacidad de autorización soporte los casos de movilidad especificados en la versión 1 de las NGN, cuando corresponda.

10.5 Gestión de identidad

1) Las NGN han de soportar un método estructurado de gestión de identidad (IdM) de la(s) identidad(es) (incluida la información conexa, como identificadores, atributos, aseveraciones y políticas) de entidades tales que:
   a) Usuarios/grupos.
   b) Organizaciones/federaciones/empresas/proveedores de servicios.
   c) Dispositivos/elementos de red/sistemas.
   d) Objetos (procesos de aplicación, contenido, datos).

2) Las NGN han de soportar las capacidades de IdM para permitir:
   a) La gestión segura del ciclo de vida (por ejemplo, registro, validación, revocación) de la identidad (identidades) de una entidad.
   b) El descubrimiento e intercambio seguros de la información de identidad asociada con la identidad (identidades) de una entidad. Esto comprende el descubrimiento e intercambio de la información de identidad que puede estar ubicada en un dominio NGN y a través distintos dominios NGN.

3) Las NGN han de soportar capacidades de aplicación de la política en vigor asociada con la identidad o información de identidad de una entidad.

4) Las NGN han de soportar capacidades de IdM comunes que utilizarán múltiples servicios y aplicaciones, entre otros:
   a) Servicios de comunicación en tiempo real (por ejemplo, VoIP, TV lineal y servicios de mensajería en tiempo real).
   b) Otros servicios de comunicaciones (por ejemplo, transacciones por la web).

5) Las NGN han de soportar capacidades de IdM para permitir la aseveración anónima de la información de identidad (por ejemplo, identificadores y atributos), de acuerdo con la política aplicable.

6) Las NGN han de soportar capacidades de IdM para permitir la compatibilidad entre elementos de red dentro de un dominio NGN (es decir, intrarred) y entre dominios o federaciones NGN diferentes. Para ello, es necesario.

   a) Emplear interfaces normalizadas para el intercambio de información de IdM.

   b) Emplear mecanismos normalizados (por ejemplo, protocolos, estructura y esquemas de datos) para el intercambio de datos de IdM.

7) Las NGN han de soportar capacidades IdM para facilitar a los usuarios extremos características de fácil utilización, como.

   a) Procedimiento único de inscripción/desinscripción a múltiples servicios y aplicaciones.

   b) Convergencia fijo/móvil.

   c) Control y protección de la información de identificación personal (IIP).

8) Las NGN han de soportar capacidades de IdM para habilitar la seguridad de servicios y aplicaciones.

9) Las NGN han de soportar la seguridad de las capacidades, funciones, datos y comunicaciones de IdM.

10.6 Requisitos de seguridad

Las NGN incluirán las características de seguridad incorporadas en las redes existentes y permitirá que exista una conexión segura con otras redes NGN u otras que no lo sean. Los requisitos se basan en la aplicación de [UIT-T X.805] a las NGN y, por ende, abarcan las siguientes dimensiones de seguridad NGN: control de acceso, autenticación, no repudiación, confidencialidad de datos, seguridad de la comunicación, integridad de datos, disponibilidad y privacidad.

Las NGN deberán contar con:

1) La protección contra la utilización no autorizada de recursos de red, y el acceso no autorizado a flujos de información y aplicaciones.

2) La autenticación de la identidad de las entidades de comunicación, si la política así lo solicita.

3) Un mecanismo para la confidencialidad de datos.

4) Un mecanismo para la integridad de datos.

5) Una metodología que defina responsabilidades, en la que los individuos sean responsables de las consecuencias de sus acciones.

6) La disponibilidad y accesibilidad de la red, cuando una entidad autorizada lo solicite.

7) Mecanismos de no repudiación, para evitar que alguna de las entidades o partes que participan en una comunicación niegue falsamente que ha participado en toda la comunicación, o en parte de ella.

8) Privacidad de la información de usuario, por ejemplo, información sobre las preferencias, los perfiles, la presencia, la disponibilidad y la ubicación. Esto se logra si la información sólo se comunica cuando se presenta una autorización válida.

9) Protección destinada a disminuir al mínimo el efecto de los ataques a la red, desde el exterior o desde el interior.

10.7 Protección de la infraestructura esencial

Se recomienda a los proveedores de servicio que dispongan de capacidades para proteger su infraestructura NGN de ataques malintencionados, como la negación de servicio, las escuchas clandestinas, la simulación, la manipulación de mensajes (modificación, retardo, supresión, inserción, reproducción, reencaminamiento, encaminamiento erróneo o reordenación de mensajes),

el repudio o la falsificación. La protección puede incluir la prevención y detección de las agresiones, la recuperación después de las mismas, y las medidas para evitar las interrupciones de servicio.

En la cláusula 10.6 se presentan los requisitos de seguridad.

11 Gestión

Las capacidades de gestión NGN abarcarán áreas que cubran aspectos tales como la planificación, la instalación, las operaciones, la administración, el mantenimiento y la configuración de redes y servicios. El objetivo principal es obtener redes que tengan capacidad de supervivencia y sean rentables.

Las capacidades de gestión NGN también incluyen la supervisión y el control de componentes de servicio y de transporte NGN, mediante la comunicación de información de gestión a través de las interfaces entre componentes NGN y sistemas de gestión, entre varios sistemas de gestión que soportan las NGN, y entre componentes NGN y el personal de servicio o los proveedores de red.

Las capacidades de gestión NGN soportarán los objetivos de las NGN:

1) proporcionando la capacidad para gestionar, durante toda su vida útil, los componentes NGN, tanto lógicos como físicos. Lo anterior incluye los recursos en el estrato de transporte y en el de servicio, las funciones de transporte de acceso, la interconexión entre componentes y las redes y terminales de usuario;
2) proporcionando la capacidad para gestionar los componentes de servicio NGN, sin importar cuáles sean los componentes de transporte subyacentes, y facultando a las organizaciones que ofrecen servicios NGN (que pueden pertenecer a diferentes proveedores de servicios) para que establezcan una oferta distintiva de servicios a sus clientes;
3) proporcionando las capacidades de gestión que faculten a las organizaciones que prestan servicios NGN para ofrecer a los usuarios servicios personalizados y crear nuevos servicios a partir de las capacidades NGN (que pueden pertenecer a diferentes proveedores de servicios);
4) proporcionando las capacidades de gestión que suministren a las organizaciones que prestan servicios NGN mejoras que incluyan el autoservicio de usuario (por ejemplo, la prestación de servicio, la notificación de fallos, la notificación en línea de facturas);
5) desarrollando una arquitectura y unos servicios de gestión que permitan a los proveedores de servicio reducir el tiempo transcurrido entre el diseño, la creación y la prestación de nuevos servicios;
6) garantizando la seguridad de la información de gestión, incluida la información de cliente y de usuario;
7) permitiendo que las organizaciones o los individuos autorizados dispongan de los servicios de gestión, en todo lugar y en cualquier momento;
8) aceptando las redes de comercio electrónico basadas en conceptos de funciones comerciales (cliente, proveedor de servicio, proveedor complementario, intermediario y proveedor (por ejemplo, un fabricante de equipos)) [UIT-T Y.110], [UIT-T M.3050.0];
9) permitiendo que las empresas o los individuos realicen varias funciones en diferentes redes y también dentro de una misma red (por ejemplo, una como proveedor de servicio al por menor y otra como proveedor de servicio al por mayor) [UIT-T M.3050.0];
10) aceptando los procesos B2B entre organizaciones que provean servicios y capacidades NGN;
11) permitiendo la gestión de redes híbridas que contengan recursos NGN y otros que no lo sean;

12) integrando una visión abstracta de los recursos (de red, de computación y de aplicación), que oculte la complejidad y la multiplicidad de tecnologías y dominios.

Los requisitos específicos para la gestión de las NGN están fuera del alcance de esta Recomendación y se describen en las Recomendaciones pertinentes, por ejemplo la [UIT-T M.3060].

NOTA – Véanse asimismo los requisitos de la cláusula 16.2, "Contabilidad y tasación".

12 Tratamiento de la movilidad

La gestión de la movilidad incluye la capacidad que tienen los entes móviles, por ejemplo, los usuarios, los terminales y las redes, de pasar de una red a otra (itinerancia), sean estas últimas NGN o no. En las NGN, se tratan dos tipos de movilidad, a saber la movilidad personal y la de terminal [UIT-T Q.1706].

En las NGN, la movilidad personal existe siempre que los usuarios empleen mecanismos de registro para asociarse con un terminal que, a su vez, puede ser asociado por la red a dichos usuarios. Cuando haya interfaces, para registro de usuario, entre usuarios y terminales, y entre usuarios y redes, se supone que se utilizarán dichas interfaces en las NGN.

Asimismo, en esta versión hay movilidad de terminal Intra e Inter redes cuando se utilizan mecanismos de registro para asociar el terminal a la red. Cuando existe el soporte de movilidad de terminal con continuidad de servicio, se espera que las NGN también lo tengan.

Los requisitos generales para la gestión de la movilidad, teniendo en mente las necesidades del usuario, son:

Para los servicios en los que se requiera la movilidad, las NGN deberán:

1) garantizar el nomadismo para ambos tipos de movilidad, la personal y la de terminal;
2) soportar la movilidad para las tecnologías de acceso existentes, y para las capacidades de QoS y las de seguridad actuales;
3) soportar la gestión de ubicación para el registro, la actualización de la ubicación y la traducción de dirección, con el fin de permitir la movilidad más allá de las fronteras de red de los proveedores;
4) soportar la gestión de abonamiento;
5) soportar la seguridad necesaria para impedir el acceso no autorizado y garantizar la privacidad del usuario, teniendo en cuenta, siempre que corresponda, la continuidad y el traspaso de servicio;
6) soportar la confidencialidad de la ubicación, ocultando a entidades que no sean de confianza la información relacionada con ésta;
7) soportar la capacidad de radiobúsqueda para el establecimiento de llamadas entrantes, ahorrando así energía en los terminales móviles y reduciendo la cantidad de señalización en la red;
8) soportar la gestión de movilidad IP o, como mínimo, ser suficientemente compatibles con la tecnología IP para permitir un funcionamiento eficaz e integrado.

Para los servicios en que convenga la movilidad, las NGN deberán:

– soportar la continuidad de servicio Intra-a.C. e Inter-a.C. La continuidad del servicio comprende los siguientes casos:
  a) continuidad de servicio para movilidad del terminal;
  b) continuidad de servicio para movilidad de la persona.

NOTA 1 – Los niveles de continuidad de servicio pueden diferir de un caso a otro, en función de condiciones tales como restricciones de la tecnología de acceso y nivel de servicio soportado por el proveedor de servicio/red.

NOTA 2 – La continuidad de servicio Inter-CN (red núcleo) queda en estudio.

En el caso de los servicios vocales, las NGN han de soportar la continuidad de servicio para movilidad del terminal.

Las NGN han de facilitar capacidades de soporte de la continuidad de servicio habida cuenta de las condiciones de la red (por ejemplo, el número de sesiones de usuario, los eventos de movilidad y el consumo de anchura de banda) así como los requisitos de usuario.

Se recomienda que las NGN permitan la adaptación a fin de soportar la continuidad de servicio cuando los requisitos de usuario y las condiciones de la red no coinciden. La adaptación puede incluir la negociación/renegociación de la QoS de la red y/o los parámetros del terminal (por ejemplo, modificación/adaptación de códec).

NOTA 3 – Los requisitos de gestión de la movilidad en las NGN pueden consultarse en [UIT-T Q.1706].

13 Gestión de perfiles

13.1 Gestión de perfil de usuario

El perfil de usuario es un conjunto de información almacenada sobre un usuario (o un abonado). En un entorno NGN, la gestión de los atributos de perfil de usuario es particularmente importante, puesto que dicha información es requerida por varias capacidades, entre las cuales las de autenticación, de autorización, de movilidad, de ubicación, de tasación, etc. Los perfiles de usuario contienen información relacionada con el transporte e información relacionada con el servicio. Los perfiles de usuario se pueden almacenar en bases de datos diferentes, en el estrato de servicio y en el de transporte, que opcionalmente disponen de funciones de intercambio de datos entre ellas.

Los requisitos generales del perfil de usuario son:

1) Habrá un perfil de usuario para cada usuario, que puede estar formado por varios "componentes".
2) Dichos componentes pueden opcionalmente estar distribuidos en la red local y en el entorno de terceros proveedores de servicio; los criterios de privacidad y protección de datos serán respetados.
3) Dentro de la red local, los componentes pueden opcionalmente estar distribuidos en varias entidades.
4) En la red local habrá una funcionalidad que permita ubicar componentes de perfil de usuario, con lo cual los servicios y aplicaciones no necesitan conocer la ubicación real de los componentes que están bajo el control de la red local.
5) Los servicios, las aplicaciones y otras entidades NGN deberán estar en condiciones de obtener el perfil completo de usuario o partes de él (según corresponda) en una transacción; los criterios de privacidad y protección de datos serán respetados.
6) Existirán medios eficaces para recuperar cada componente de perfil de usuario en un periodo razonable, para servicios en tiempo real.

   NOTA – Si bien la gestión de perfil de usuario no pretende suministrar ninguna clasificación de la información que pueda contener un perfil de usuario, es posible emplear categorías del tipo información general de usuario, información específica de servicio, etc.

Se espera que los requisitos específicos del perfil de usuario, su utilización y su gestión se traten en futuras Recomendaciones del UIT-T.

13.2 Gestión de perfil de dispositivo

El perfil de dispositivo es un conjunto de información almacenada sobre un equipo de usuario. En un entorno NGN, la gestión de los atributos de perfil de dispositivo también es importante, puesto que dicha información, junto con la del perfil de usuario, es requerida por varias capacidades, entre las cuales las de autenticación, de autorización, de movilidad, de ubicación, de tasación, etc. Los perfiles de dispositivo pueden contener información relacionada con el transporte e información relacionada con el servicio. Los perfiles de dispositivo se pueden almacenar en bases de datos diferentes, en el estrato de servicio y en el de transporte, que opcionalmente disponen de funciones de intercambio de datos entre ellas.

NOTA 1 – Esta información puede comprender la identificación, la dirección y el nombre del terminal, atributos estáticos como los medios y protocolos aceptados, detalles sobre la pantalla (tamaño en píxeles, resolución de color, tiempo de respuesta, etc.), velocidad de transmisión, ancho de banda y potencia de procesamiento; y atributos que cambian dinámicamente, como la utilización de terminal de usuario, la ubicación geográfica y las aplicaciones que están funcionando en el terminal.

Los perfiles de dispositivo pueden servir para:

– rastrear dispositivos robados o inapropiados;

– establecer el tipo y el nivel del servicio que puede prestarse al usuario (basándose en las capacidades del dispositivo);

– establecer la calidad de servicio requerida para una conexión entre terminales (basándose en las capacidades del dispositivo).

Los requisitos que han de cumplir los perfiles de dispositivo son:

1) Habrá un perfil de dispositivo para cada equipo de usuario, que puede opcionalmente estar formado por varios "componentes".

2) Dichos componentes pueden opcionalmente estar distribuidos en la red local y en el entorno de terceros proveedores de servicio.

3) Dentro de la red local, los componentes pueden opcionalmente estar distribuidos en varias entidades.

4) En la red local habrá una funcionalidad que permita ubicar componentes de perfil de dispositivo, con lo cual los servicios y aplicaciones no necesitan conocer la ubicación real de los componentes, y están bajo el control de la red local.

5) Los servicios, las aplicaciones y otras entidades NGN pueden opcionalmente estar en condiciones de obtener el perfil completo de dispositivo o partes de él (según corresponda) en una transacción; los criterios de privacidad y protección de datos serán respetados.

6) Existirán medios eficaces para recuperar cada componente de perfil de dispositivo en un periodo razonable, para servicios en tiempo real.

NOTA 2 – Si bien la gestión de perfil de dispositivo no pretende suministrar ninguna clasificación de la información que pueda contener un perfil de dispositivo, es posible emplear categorías del tipo información general de dispositivo, información específica de servicio, etc.

Se espera que los requisitos específicos del perfil de dispositivo, su utilización y su gestión se traten en futuras Recomendaciones del UIT-T.

14 Tratamiento de medios

14.1 Gestión de recursos de medios

Los mecanismos de gestión de recursos de medios se suelen emplear junto con los servicios tradicionales de tratamiento de voz y las interacciones de usuario con voz y DTMF. En las NGN habrá que ampliarlos para poder soportar nuevos servicios de datos, vídeo y contenido.

Las NGN tendrán que soportar varios recursos de medios y capacidades de gestión de recursos de medios, con el fin de ser compatibles con una amplia gama de aplicaciones.

Las capacidades de recursos de medios para las NGN son:

– la grabación de medios (por ejemplo, correo vocal);
– la reproducción de medios grabados (por ejemplo, recuperación de correo vocal, tonalidades y anuncios);
– el reconocimiento de la DTMF (por ejemplo, servicios interactivos de respuesta vocal);
– el reconocimiento avanzado de voz (por ejemplo, servicios interactivos de respuesta vocal);
– la conversión de medios (por ejemplo, de texto a voz, de voz a texto, de fax a correo electrónico);
– la transcodificación;
– la utilización simultánea de vídeo/texto/audio/datos (por ejemplo, conferencias);
– la duplicación de medios (por ejemplo, casos de intercepción legal);
– la inserción de medios (por ejemplo, imagen, texto, vídeo) en trenes multimedios.

Otras capacidades de recursos de medios para las NGN son:

– descarga de medios (por ejemplo, clips de vídeo/audio, imágenes);
– difusión en directo de medios (por ejemplo, vídeo a la carta);
– transferencia transparente;
– almacenamiento y entrega de medios distribuidos (múltiples copias de medios, múltiples segmentos de medios);
– direccionamiento dinámico de medios (ubicación de los medios existentes en el almacén adecuado para que el usuario pueda acceder a ellos en tiempo real).

14.2 Requisitos para los códecs

14.2.1 Generalidades

Los requisitos generales para los códecs de las NGN son:

1) Siempre que sea posible, se debe evitar la transcodificación.
2) Las NGN soportarán la negociación extremo a extremo de cualquier códec entre entidades NGN (terminales, elementos de red). Las entidades que se encuentran en el borde de la NGN (por ejemplo, terminales NGN y equipos de usuario) y el equipo de red que origina y termina el flujo de medios IP NGN se encargan de negociar y escoger un códec común para cada sesión de medios "extremo a extremo". Las NGN deberán aceptar la negociación extremo a extremo de códecs de texto, por ejemplo los especificados en las Recomendaciones del UIT-T.

Para los códecs de las NGN se recomiendan las siguientes características:

1) funcionamiento autoadaptativo a la variación de las condiciones de QoS;
2) solucionar los efectos de la modificación del nivel de servicio en el funcionamiento del códec;
3) compatibilidad con los códecs de la RTPC/RDSI;
4) descubrimiento/interrogación de los parámetros del códec;
5) selección/negociación y renegociación intermedia de los parámetros del códec.

14.2.2 Códecs de audio

Se prevén las siguientes clases de códecs de audio:

a) "audio de banda estrecha" para la gama de audio entre 300 Hz y 3 400 Hz;

b) "audio de banda ancha" para la gama de audio entre 50 Hz y 7 000 Hz;

c) "audio de banda superancha" para la gama de audio entre 50 Hz y 14 000 Hz;

d) "audio de banda total" para la gama de audio entre 20 Hz ~ 20 000 Hz, con capacidades multicanal asociadas (mono, estéreo, etc.).

A fin de permitir la compatibilidad entre las NGN y otras redes (incluidas la RTPC, las redes móviles y otras NGN), las NGN han de ser capaces de aceptar y presentar voz codificada conforme a [UIT-T G.711] cuando se conecten con otra red. Cuando no se haya escogido un tamaño de empaquetado por negociación de códec entre terminales y/o elementos de red, o no se haya llegado a un acuerdo bilateral al respecto, se recomienda emplear un tamaño de empaquetado de voz de muestras de 10 ms para el códec vocal UIT-T G.711; este valor se recomienda porque permite un balance óptimo entre el retardo extremo a extremo y la utilización de la red. Se acepta que puede opcionalmente haber restricciones de red que hagan necesario escoger por acuerdo bilateral un valor mayor, en cuyo caso conviene utilizar un valor de 20 ms.

NOTA 1 – Cuando se escoge un tamaño de empaquetado por negociación de códec entre terminales y/o elementos de red, la presente Recomendación no impone ningún requisito al valor seleccionado.

NOTA 2 – Nada de lo dicho anteriormente establece requisitos relativos a los códecs que han de soportar los terminales ni obliga a las NGN a soportar la transcodificación de audio entre cualquier código y G.711.

Además, se recomienda el soporte de los siguientes códecs de audio:

– AMR [ETSI TS 126.071]: a fin de soportar los terminales 3GPP y facilitar el interfuncionamiento con las redes 3GPP.

– UIT-T G.729A [UIT-T G.729]: a fin de facilitar el interfuncionamiento con las redes VoIP existentes y soportar los terminales VoIP existentes.

– EVRC/EVRC-B [TIA-127-C]: a fin de soportar los terminales 3GPP2 y facilitar el interfuncionamiento con las redes 3GPP2.

14.2.3 Códecs de audio de banda ancha

14.2.3.1 Generalidades

La cláusula 14.2.1 tiene prioridad sobre la presente cláusula a fin de reducir la transcodificación y mejorar tanto la compatibilidad en banda ancha como la calidad de extremo a extremo.

El audio de banda ancha es una capacidad que puede ser soportada por:

– entidades en los bordes de las NGN (por ejemplo, NGN-TE), que tengan capacidades de audio de banda ancha;

– equipos de red donde se origina y termina el flujo de medios IP NGN con contenido de audio de banda ancha.

Los terminales con capacidades de audio de banda ancha han de tener también capacidades de banda estrecha y ajustarse a los requisitos de la cláusula 14.2.2.

Los equipos de red que facilitan capacidades de audio de banda ancha han de tener también capacidades de banda estrecha y ajustarse a los requisitos de la cláusula 14.2.2.

Puede opcionalmente realizarse la transcodificación de audio para ofrecer compatibilidad de servicio de extremo a extremo, pero se recomienda evitar esta operación en la medida de lo posible.

14.2.3.2 Códecs de audio de banda ancha en terminales

Se recomienda que los terminales donde se originan y terminan los flujos de medios IP de extremo a extremo en las NGN, que soportan el audio de banda ancha, dispongan de uno o más de los siguientes códecs de audio de banda ancha:

– UIT-T G.722 [UIT-T G.722].

NOTA 1 – Obligatorio para los equipos de usuario DECT NG; utilizado en algunos equipos de usuario VoIP y/o heredados.

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

NOTA 2 – Obligatorio para los equipos de usuario 3GPP y/o utilizado en los equipos de usuario con movilidad conforme al acceso 3GPP.

– UIT-T G.729.1 [UIT-T G.729.1].

NOTA 3 – Utilizado en algunos equipos de usuario DECT NG y algunos equipos de usuario VoIP y/o heredados.

– EVRC-WB [TIA-127-C].

NOTA 4 – Obligatorio para los equipos de usuario 3GPP2 y/o equipos de usuario con movilidad conforme al acceso 3GPP2.

NOTA 5 – Los terminales pueden ofrecer otros códecs además de los enumerados.

NOTA 6 – Excepcionalmente, se recomienda que los terminales que ofrezcan uno o más códecs de audio de banda ancha no enumerados anteriormente (por ejemplo, terminales existentes/heredados) puedan funcionar en las NGN. Tales terminales pueden sufrir una compatibilidad de audio de banda ancha limitada.

14.2.3.3 Códecs de audio de banda ancha en redes

Se recomienda que los equipos de red donde se originan y terminan los flujos de medios IP NGN de extremo a extremo, que soportan el audio de banda ancha, dispongan de los siguientes códecs de audio de banda ancha:

– UIT-T G.722 [UIT-T G.722].

NOTA 1 – A fin de soportar los equipos de usuario DECT NG, algunos equipos de usuario VoIP y/o heredados y/o el interfuncionamiento con otras redes.

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

NOTA 2 – A fin de soportar los equipos de usuario 3GPP, los equipos de usuario con movilidad conforme con el acceso 3GPP y/o el interfuncionamiento con redes 3GPP.

– UIT-T G.729.1 [UIT-T G.729.1].

NOTA 3 – Cuando se hayan de soportar equipos de usuario DECT NG, equipos de usuario VoIP y/o heredados y/o el interfuncionamiento con algunas redes VoIP y heredadas.

– EVRC-WB [TIA-127-C].

NOTA 4 – Cuando se hayan de soportar equipos de usuario 3GPP2, equipos de usuario con movilidad conforme al acceso 3GPP2 y/o el interfuncionamiento con redes 3GPP2.

14.2.4 Códecs de vídeo

A fin de facilitar el interfuncionamiento de los servicios de comunicación de vídeo entre las NGN y otras redes, se recomienda el soporte de los códecs UIT-T H.263 perfil 0 [UIT-T H.263] y UIT-T H.264 perfil básico [UIT-T H.264].

NOTA – Esto no impone requisitos sobre los códecs de vídeo que han de soportar los terminales ni obliga a las NGN a soportar la transcodificación de vídeo entre cualquier códec y códecs basados en H.263 [b-UIT-T H.263] o H.264 [b-UIT-T H.264].

15 Gestión de contenido

Se recomienda que las NGN ofrezcan capacidades de gestión del contenido a fin de gestionar diversos y enormes recursos de contenido.

NOTA 1 – Los objetos de la gestión del contenido suelen clasificarse en contenido empresarial (por ejemplo, documentos de la empresa), contenido de servicios web (por ejemplo, ficheros HTML, imágenes); contenido de servicios TVIP (por ejemplo, difusión de datos de relativamente gran tamaño). La gestión del contenido en las NGN permite gestionar el ciclo de vida del contenido (por ejemplo, desde la creación, pasando por la edición, aprobación, publicación y mantenimiento, hasta el archivo). Además, la gestión de contenido permite soportar procesos B2B entre organizaciones, de conformidad con los acuerdos contraídos entre ellas.

NOTA 2 – Los requisitos de gestión del contenido de los servicios TVIP se encuentran en la cláusula 14.1.

NOTA 3 – Entre otras, las capacidades de gestión de contenido incluyen:

– Adquisición de contenido, agregación e importación de contenido/metadatos desde múltiples fuentes externas.

– Validación y verificación del formato de contenido/metadatos, así como definición de la relación entre el contenido y sus metadatos.

– Clasificación del contenido en función de diversas normas de clasificación.

– Manipulación de contenido y metadatos (por ejemplo, adición, modificación, búsqueda, procesamiento de derechos de autor, adaptación).

  NOTA 4 – La adaptación del contenido comprende la capacidad de transformación del mismo a fin de ajustarse a las capacidades de los dispositivos y/o las limitaciones de la red.

– Envío de contenido dentro de la NGN, de conformidad con la asignación de recursos de entrega de contenido, restricciones de publicación de contenido, etc.

– Supervisión y auditoría de contenido (por ejemplo, supervisión del estado del contenido y/o resultados de la manipulación del contenido, realización de análisis y estadísticas de contenido).

16 Funcionamiento y configuración

16.1 Requisitos de NNA (numeración, denominación y direccionamiento)

Las NGN tienen como objetivo crear un entorno de numeración, denominación y direccionamiento, para los usuarios, los operadores de red y los proveedores de servicios, que sea eficiente, seguro y fiable. Siempre que fuere necesario, se habrá de tener en cuenta el aspecto reglamentario así como la interoperabilidad con la RTPC/RDSI.

En la evolución hacia las NGN se debe preservar completamente la soberanía de los Estados Miembros de la UIT en lo relativo a los planes de numeración, denominación y direccionamiento, conforme a [UIT-T E.164], a otras Recomendaciones pertinentes y a otros organismos de normalización.

A continuación se describen los requisitos que se deben cumplir para tener las capacidades de numeración, denominación y direccionamiento. Salvo indicación contraria, todos son válidos para ambos estratos, de transporte y de servicio.

1) Se admitirán los modos de atribución de direcciones dinámico y fijo.

2) Las capacidades de numeración, denominación y direccionamiento se pueden opcionalmente implementar a través de un esquema de correspondencia para cada servicio, o mediante uno que sea común a varios servicios.

3) Se admitirá la actualización dinámica de la base de datos de denominación (por ejemplo, tratándose de un terminal móvil, las direcciones en una o varias capas pueden opcionalmente cambiar dinámicamente dependiendo de la ubicación del terminal).

NOTA – Estos depósitos pueden ser directorios UIT-T X.500 a los que se accede como se especifica en [b-UIT-T X.511].

16.1.1 Numeración

Los requisitos de numeración que se aplican a las NGN son:

1) Los mecanismos de direccionamiento soportarán la capacidad para distinguir entre los planes de marcación y de numeración.

2) Los mecanismos de direccionamiento soportarán la capacidad para traducir una secuencia de marcación en el esquema de numeración.

3) Las NGN soportarán la numeración UIT-T E.164 (números mundiales).

4) Se recomienda que las NGN acepten numeración que no sea UIT-T E.164 (números locales).

5) Se recomienda que las NGN acepten números cortos en los planes nacionales de marcación.

6) No se recomienda que las NGN impidan la numeración privada y empresarial (véase la cláusula 17).

7) Cuando se empleen números que no son UIT-T E.164 (números locales) o secuencias de marcación, el direccionamiento NGN establecerá el entorno en el cual dichos números locales son válidos.

8) Las NGN soportarán la numeración UIT-T E.164 internacional.

9) Las NGN soportarán la numeración UIT-T E.164 nacional.

10) Las NGN soportarán indicativos cortos (números no UIT-T E.164) en los planes nacionales de marcación.

11) Las NGN soportarán la numeración privada (por ejemplo numeración para servicios específicos y empresarial) (véanse las cláusulas 17.1 y 17.2).

12) Cuando se utilicen números UIT-T E.164 nacionales o indicativos cortos o números privados, el direccionamiento NGN habrá de dejar el margen necesario dentro del cual estos números son válidos.

13) Las NGN distinguirán entre los números telefónicos y los identificadores alfanuméricos que sólo tengan números, y se recomienda que los considere como tales a los efectos del encaminamiento.

16.1.2 Esquemas NNA

1) En el estrato de transporte, las NGN aceptarán esquemas de direccionamiento IP basados en el IPv4, el IPv6 o en ambos.

   NOTA 1 – Se recomienda observar que una mezcla de IPv4 e IPv6 en el entorno de un solo operador puede causar problemas en la prestación del servicio.

2) Los dominios NGN pueden opcionalmente soportar equipos de usuario, en las interfaces usuario-red, que utilicen solamente el IPv4, solamente el IPv6 o ambos.

   NOTA 2 – Se supone que los equipos basados en el IPv6 también pueden aceptar el IPv4 en la interfaz usuario-red.

3) Las NGN, versión 1, soportarán el establecimiento de comunicación multimedios IP (cuando se origina, así como cuando se termina) utilizando como mínimo los identificadores uniformes de recursos de teléfono UIT-T E.164 (URI Tel, *telephone uniform resource identifiers*), por ejemplo, tel: +4412345678, y los identificadores uniformes de recursos SIP (URI SIP), por ejemplo, sip:my.name@company.org. Para el caso de los URI Tel:

   – se aceptarán UIT-T E.164 internacionales;

   – se aceptarán los números UIT-T E.164 nacionales y los indicativos cortos.

4) En algunas situaciones de servicio, por ejemplo, el interfuncionamiento con la RTPC/RDSI, las NGN soportarán el establecimiento de comunicación multimedios IP (cuando se origina, así como cuando se termina) utilizando numeración UIT-T E.164 con soporte del tipo ENUM, cuando corresponda.

5) Los esquemas de numeración soportarán los tipos de servicios unidifusión y multidifusión.

6) Los esquemas de numeración deberían soportar tipos de servicios de difusión.

7) Es posible soportar otros esquemas de numeración, denominación y direccionamiento.

NOTA 3 – Quedan en estudio otros esquemas de numeración, denominación y direccionamiento, como los nombres distinguidos especificados en [b-UIT-T X.501].

16.1.3 Resolución NNA

En [UIT-T Y.2001] se describen los principios y requisitos fundamentales que ha de cumplir la resolución de nombre, dirección y numeración. En este orden de ideas, se suministran aquí los siguientes requisitos:

1) Escalabilidad: se recomienda que las NGN sean escalables, con el fin de poder hacer frente a la demanda cada día mayor de resolución de nombre o dirección.

2) Fiabilidad: las capacidades de resolución de nombre o dirección no podrán verse afectadas por un fallo en un solo punto (gracias a, por ejemplo, mecanismos distribuidos de resolución).

3) Seguridad: se tendrán que poner en marcha medidas de seguridad para las capacidades de resolución de nombre o dirección.

NOTA – Estas capacidades pueden opcionalmente emplear bases de datos en apoyo de servicios de directorio internas o externas a la NGN (por ejemplo, una base de datos del DNS de Internet, LDAP [b-UIT-T X.511]). Algunos ejemplos de medidas de seguridad pueden ser la autenticación de usuario, la seguridad de datos, la sincronización de datos y la recuperación después de fallo.

16.1.4 Interfuncionamiento NNA

Las funciones de interfuncionamiento traducen números, nombres y direcciones, cuando así lo requiere el tipo de interconexión de red.

1) Las NGN soportarán varios tipos de interfuncionamiento de dirección de estrato de transporte, minimizando su efecto sobre el servicio prestado a los usuarios (es decir, casos de interfuncionamiento entre diferentes dominios de direccionamiento, tales como los basados en los esquemas de numeración del IPv4 o del IPv6, y los basados en esquemas de numeración públicos o privados).

2) Si fuere necesario, se utilizarán capacidades de traducción de direcciones para poder aceptar diferencias de formato de dirección, en ambos estratos, de transporte y de servicio, minimizando su efecto sobre el servicio prestado a los usuarios.

16.2 Contabilidad y tasación

En las NGN se soportan capacidades de contabilidad y tasación con el fin de proveer al operador de red con este tipo de información relativa a la utilización de los recursos existentes en la red.

Los requisitos que han de cumplir las NGN en lo que toca a contabilidad y tasación son:

1) Las capacidades de contabilidad y tasación incluirán la posibilidad de recolectar información con miras a su ulterior procesamiento (tasación fuera de línea), así como la posibilidad de interactuar en tiempo casi real con aplicaciones del tipo servicios prepagados (tasación en línea).

2) Se dispondrá de mecanismos abiertos para la gestión de la tasación.

3) Se soportarán diversas políticas de tasación (por ejemplo, la tasación por tarifa fija y la basada en la utilización por sesión).

4) Las capacidades de contabilidad y tasación soportarán servicios con funcionalidad multidifusión. Las funciones de contabilidad estarán en condiciones de informar qué usuario recibió cuál información, tanto al inicio como al final de una sesión multidifusión.

5) Las NGN permitirán todo tipo de arreglos contables, incluida la transferencia entre proveedores de información contable o de tasación. Este requisito también abarca los acuerdos relativos al comercio electrónico.

   Considérese, por ejemplo, el caso de los servicios de suministro de contenido con la funcionalidad de multidifusión, que pueden ser prestados en el marco de actividades conjuntas de varias empresas (por ejemplo, varios proveedores de contenido y uno de red): además de la funcionalidad de tasación de usuarios, se necesita la funcionalidad de tasación entre las empresas.

6) Las NGN han de soportar interfaces y protocolos entre los elementos de red y los elementos de contabilidad y entre los elementos de contabilidad y tasación a fin de recopilar y transportar datos de utilización de recursos (por ejemplo, medidas de contabilidad y registros de información de tasación (CIR)). Estas interfaces y protocolos han de ser conformes con [UIT-T Y.2233].

7) Las NGN han de soportar funcionalidades de gestión para el funcionamiento sin discontinuidad de los elementos funcionales de contabilidad y tasación [UIT-T Y.2233].

8) Se recomienda que las NGN soporten la funcionalidad de contabilidad y tasación por flujos para los distintos servicios NGN (por ejemplo, utilización de recursos de flujo unidireccional, utilización de recursos de flujo bidireccional, utilización de recursos de sesión). Esta funcionalidad ha de ser precisa, fiable y adaptable.

NOTA – La utilización de la información de tasación recopilada por una NGN, a los efectos de los acuerdos de tasación, está fuera del alcance de esta Recomendación.

16.3 Requisitos de OAM

Se suele aceptar que las capacidades OAM son importantes en las redes públicas para facilitar la operación, verificar la calidad de funcionamiento y reducir los costos de funcionamiento de las redes, haciendo mínimas las interrupciones de servicio, la degradación de servicio y los periodos de inactividad operacional. En particular, estas capacidades son fundamentales para las redes sujetas a cumplir (y, por ende, a medir y a comparar) ciertos objetivos de calidad de funcionamiento y disponibilidad de red [UIT-T Y.1710], [UIT-T Y.1730].

Las NGN proporcionará funciones OAM para ambos estratos, el de servicio y el de transporte.

Para poder prestar servicios NGN confiables, que puedan soportar los requisitos estipulados en los SLA, los servicios NGN han de tener sus propias capacidades OAM.

NOTA 1 – Las capacidades OAM de que trata esta subcláusula son complementarias con las descritas en la cláusula 11.

Los requisitos generales de OAM para las NGN son:

1) Soportará la capacidad de escoger, por parte del proveedor de red o de servicio, las funciones OAM deseadas.

2) Las funciones OAM han de poder utilizarse con aplicaciones punto a punto, punto a multipunto y multipunto a multipunto.

3) Las funciones OAM permitirán pasar eficientemente a tamaños mayores de red.

4) Se soportará la capacidad de detección de fallos, defectos y averías.

5) Se soportará la capacidad de diagnosticar, localizar y notificar a las entidades de gestión de red, y tomar las medidas correctivas del caso.

6) Se soportará la capacidad que permite a la NGN evitar que el usuario active las funciones OAM de proveedor de red o de servicio.

7) Se soportará la capacidad que permite a la NGN evitar que el usuario detecte o localice fallos (pues ésta es una tarea del proveedor de red o de servicio).

8) El tráfico OAM seguirá el mismo trayecto que el de usuario.

9) Se detectarán automáticamente las siguientes anomalías:

   – pérdida de datos;
   – pérdida de conectividad;
   – información con errores;
   – información autorreplicada intencionalmente;
   – inserción errónea de datos [UIT-T Y.1730].

10) Las funciones OAM serán compatibles con las versiones anteriores. Las NGN podrán activar con transparencia las funciones OAM, sin perturbar el tráfico de usuario o provocar acciones innecesarias.

11) Las funciones OAM operarán confiablemente, aun en condiciones degradadas de transmisión, por ejemplo, cuando haya eventos con errores.

12) Las evaluaciones del estado de conectividad serán independientes del comportamiento dinámico del tráfico de usuario [UIT-T Y.1710], [UIT-T Y.1730].

13) Se soportarán las relaciones OAM de capa cliente-servidor entre capas inferiores y superiores (por ejemplo, fallo de señal/degradación de señal), cuando se trate de redes multicapa.

14) En el caso de redes multicapa, un defecto en determinada red de capa de servidor no podrá provocar alarmas múltiples, ni tampoco acciones correctivas innecesarias, en ninguna capa superior de cliente. Se recomienda que las redes de capa de cliente soporten la supresión de alarma para defectos originados en la capa de servidor, cuya presencia haya sido comunicada empleando la indicación de defecto hacia adelante. Las redes de capa de cliente han de soportarán la capacidad de indicación de defecto hacia adelante [UIT-T Y.1710], [UIT-T Y.1730].

15) En el caso de redes multicapa, las funciones OAM en una red de capa determinada no podrán depender de ninguna red específica de capa superior o inferior. Esto es fundamental desde el punto de vista de la arquitectura, con el fin de garantizar que la evolución de las redes de capa, su supresión o adición, no afecte las demás redes de capa.

16) En el caso de redes multicapa, las funciones OAM en una red de capa determinada serán lo suficientemente independientes de todo plano de control específico, de manera que cualquier modificación a éste no imponga cambios en el plano de usuario OAM (incluido el caso en que no hay plano de control). Esto es fundamental desde el punto de vista de la arquitectura, con el fin de garantizar que la evolución del plano de usuario y la del plano de control no se influencien entre sí.

17) En los entornos en los que hay varios proveedores de red o de servicio, se soportarán las funciones OAM.

18) Cuando se prestan servicios NGN en entornos de múltiples servicios o proveedores de red, es requisito detectar e informar cuál proveedor de servicio o de red es responsable de determinado defecto, con lo cual se puede actuar prontamente. Además, se informará del fallo de servicio al proveedor de servicio o de red que ofrece el servicio al usuario, aunque

el fallo y el punto de detección se encuentren en la red de otro proveedor de servicio o de red.

19) Las NGN dispondrán de mecanismos que garanticen que los flujos OAM del proveedor de servicio o de red, destinados a uso interno, se mantengan confinados dentro de sus redes y no lleguen a otros usuarios o proveedores de servicio o de red.

20) Con el fin de poder utilizar funciones OAM en redes híbridas, de manera que se puedan prestar servicios a lo largo de un trayecto extremo a extremo que contenga una combinación de redes NGN y otras que no lo sean, se soportarán las funciones OAM en los casos de interfuncionamiento (cláusula 18.3).

21) Para que se pueda gestionar separadamente una porción de red que depende de un proveedor y permitir una definición flexible de las entidades de mantenimiento, se soportarán tanto las funciones OAM "de segmento" como las "extremo a extremo".

NOTA 2 – Por segmento se entiende una parte de una conexión extremo a extremo, que se define a los efectos de la explotación y el mantenimiento.

22) Se soportará el registro del tiempo de indisponibilidad de servicio, con el fin de efectuar mediciones de la calidad de funcionamiento y de la disponibilidad.

23) Se gestionará la información producida por las funciones OAM de manera que se suministren al personal de mantenimiento las indicaciones adecuadas para conservar el nivel de calidad de servicio ofrecido a los usuarios [UIT-T I.610].

24) Se soportarán las capacidades de supervisión de calidad de funcionamiento.

16.4 Gestión de política

La gestión de políticas se puede emplear en las NGN para:

1) Garantizar la coherencia de servicio a través de una variedad de teconologías de red de acceso y red troncal. Esto también se puede lograr con redes de varios proveedores de servicio.

NOTA 1 – La política en vigor para cada red es función de las tecnologías de red y se puede opcionalmente especificar para cada tecnología.

2) Proporcionar control de admisión, con relación a la utilización, por parte de los servicios y las aplicaciones, de las capacidades y los recursos de red.

3) Proporcionar un registro de utilización de recursos de red.

NOTA 2 – Esto puede entenderse como la función que produce información que puede ser utilizada por otras capacidaes, como las de contabilidad y de tasación.

4) Lograr que los servicios y las aplicaciones sean independientes de los intrincados detalles de implementración de red.

NOTA 3 – El control de política puede ser útil a las aplicaciones, aunque no conozca las tecnologías de red empleadas.

Los puntos anteriores aunados a la conectividad, la QoS y la seguridad hacen que se puedan tomar muchas medidas en el entorno de gestión de política, benéficas para los servicios NGN. Por ejemplo, la gestión de política puede servir para:

– el alta de servicio;
– la configuración de servicio;
– la autorización (es decir, los derechos de acceso);
– la prestación de servicio;
– la contabilidad y la tasación.

En la gestión de política se pueden invocar reglas, cuya complejidad es función de la utilización prevista, con el fin de producir resultados fiables, coherentes y determinísticos, denominados decisiones políticas.

NOTA 4 – Se pueden ver las capacidades de gestión de QoS, por ejemplo el control de recursos y de admisión (cláusula 9), como parte del conjunto general de capacidades de gestión de política.

Los requisitos generales de gestión de política para las NGN son:

1) Se soportarán las capacidades de gestión de política con el fin de garantizar el acceso, la configuración y la gestión de servicio.
2) Las capacidades de gestión de política funcionarán en servicios específicos, y dentro de dominios específicos de proveedor o entre varios de dichos dominios.
3) Las capacidades de gestión de política rechazarán peticiones no autorizadas o no responderán a ellas, y responderán a las autorizadas.

16.5 Requisitos de supervivencia

Las funciones de supervivencia son indispensables cuando se trate de redes altamente fiables.

16.5.1 Conmutación de protección

Con el fin de poder contar con funciones de supervivencia rápidas y determinísticas en todos los trayectos de tráfico, las NGN soportarán las capacidades de conmutación de protección.

Los requisitos generales para la conmutación de protección de transporte NGN son:

1) Se soportarán las capacidades necesarias para impedir que un defecto de capa superior active la conmutación de protección en una capa inferior.
2) Cuando más de una capa participe en la conmutación de protección, las capas inferiores tendrán prioridad (esto se conoce como la estrategia de transferencia ascendente (o "escalación") entre capas).
3) Se recomienda que haya conmutación de protección 1+1 y 1:n.
4) Se pueden opcionalmente emplear los recursos de protección de transporte no utilizados para transportar tráfico sin garantías.
5) Se recomienda minimizar los efectos sobre la calidad de funcionamiento de red (por ejemplo, el retardo adicional, la variación de retardo, los errores de bits, las pérdidas de paquetes, etc.) causados por la conmutación de protección.
6) Se soportarán las funciones de control de operador, como la de exclusión de la protección, y las instrucciones de conmutación manual y forzada.

En otras Recomendaciones, por ejemplo la [UIT-T G.808.1], se describen los requisitos específicos para determinadas tecnologías.

16.5.2 Reencaminamiento

Cuando haya accidentes graves o eventos especiales, es posible que se presente, en el peor de los casos, una degradación o un fallo de red. Siendo así, se necesitan capacidades como la de reencaminamiento, aunque probablemente se produzca una disminución de la calidad de funcionamiento o de la de servicio, por lo que también se ha de disponer de mecanismos de control de tráfico.

NOTA – Dichas capacidades también pueden entenderse como parte de las funciones de integridad de red.

Los requisitos generales de reencaminamiento NGN son:

1) Cuando más de una capa participe en el reencaminamiento, las capas inferiores pueden opcionalmente tener prioridad (esto se conoce como la estrategia de transferencia ascendente entre capas).

2) El mecanismo de reencaminamiento deberá poder encontrar, en un tiempo razonable, un camino alternativo.

3) Se recomienda minimizar los efectos sobre la calidad de funcionamiento de red (por ejemplo, el retardo adicional, la variación de retardo, los errores de bits, las pérdidas de paquetes, etc.) causados por el reencaminamiento.

4) No se excluirá el control de operador.

5) Se podrá efectuar una reoptimización de red, si fuere necesaria, tras la restauración del tráfico defectuoso.

6) Después de recuperarse de una condición de degradación o fallo, se restaurarán los niveles de calidad de funcionamiento y de servicio existentes antes de la condición de degradación o de fallo.

16.5.3 Resiliencia de servicio

Las condiciones de resiliencia dependen del tipo de servicio, por lo cual es necesario describirlas para cada servicio, cuando corresponda.

Los requisitos generales de resiliencia de servicio (SR, *service resiliency*) son:

1) Se podrán atribuir independientemente diferentes niveles de SR a diferentes servicios.

2) Se podrán atribuir independientemente diferentes niveles de SR a diferentes servicios, flujo por flujo.

3) En función del nivel atribuido de SR, los servicios podrán gozar del mismo nivel de calidad de servicio que tenían antes del evento de fallo.

4) Los terminales de usuario no estarán obligados a señalar a la NGN los niveles de SR.

5) Se podrá atribuir y soportar la SR desde el punto de ingreso hasta el de egreso de la red del proveedor de servicio.

6) Se podrá distinguir entre los flujos con SR del plano de usuario y los del plano de control.

7) Se podrá notificar a la aplicación o al usuario, cuando la NGN no pueda garantizar el nivel requerido de SR.

17 Redes de usuario, incluidas las redes de empresa

17.1 Requisitos generales para el acceso a las NGN a través de redes de usuario

A continuación se presentan los requisitos generales para el acceso a las NGN a través de redes de usuario:

1) Las NGN aceptarán soluciones de acceso a las NGN a través de una red de usuario, con NAT/NAPT y cortafuegos, en entornos en los que la red de usuario pueda atribuir direcciones IP a equipos de usuario. Es probable que no se pueda establecer un camino hacia esas direcciones desde la red pública internet.

2) Las soluciones de acceso a las NGN a través de las redes de usuario habrán de tener un efecto mínimo en las redes de usuario existentes.

3) Las soluciones de acceso a las NGN a través de las redes de usuario soportarán las siguientes configuraciones:

   – con conectividad directa e interacción entre los terminales y la NG;

   – con conectividad indirecta e interacción entre los terminales y la NGN (por ejemplo, mediante redes domésticas y redes de empresa).

Se recomienda que las NGN permitan la utilización simultánea de varios tipos de funciones de transporte de acceso por parte de un solo terminal, aunque no es requisito coordinar la comunicación entre ellos. Es posible, entonces, que dichos terminales parezcan, desde la óptica de la red, ser dos o más terminales distintos.

NOTA – Si bien los requisitos indicados en esta Recomendación no se refieren a los equipos, no se pretende prohibir la conexión de equipos de usuario que faciliten la adaptación de la interfaz a otros requisitos de usuario, incluidos los de las personas discapacitadas, útiles para la conexión con dispositivos tradicionales de interfaz de usuario.

17.2 Requisitos generales para las redes de usuario

Los requisitos de alto nivel para las redes de usuario conectadas a las NGN son los siguientes:

– Se recomienda que las redes de usuario conectadas a las NGN permitan a los usuarios acceder:
  1) a los servicios facilitados por las NGN;
  2) a los servicios facilitados por las redes de usuario mismas (a nivel local y mediante las NGN interconectadas);
  3) como usuarios de empresa y como usuarios domésticos.

– Se recomienda que las redes de usuario conectadas a las NGN soporten:
  1) la seguridad, la gestión y la QoS para las redes domésticas;
  2) la configuración de dispositivos y servicios (terminales de usuario, pasarelas de red de usuario), incluido el acceso a distancia.

17.3 Redes de empresa

17.3.1 Introducción

En esta cláusula se especifican los requisitos de alto nivel para las comunicaciones de empresa a fin de:

1) soportar la conexión e interfuncionamiento de las capacidades de comunicación de empresa (en una red empresarial de la próxima generación (NGCN) o una NGN) con las NGN;
2) soportar la conexión e interfuncionamiento de las capacidades de comunicación de empresa con otras capacidades de comunicación de empresa (en una NGCN o una NGN);
3) soportar la conexión e interfuncionamiento de las capacidades de comunicación de empresa con otras capacidades de comunicación de empresa ubicadas en la RDSI y la RTPC o conectadas a ellas;
4) soportar los servicios de empresa en una NGN.

NOTA 1 – En esta Recomendación se especifican los requisitos de red para soportar la conexión de una NGCN directamente a una NGN, así como los requisitos de red para la comunicación entre capacidades de una NGCN (incluido el equipo de usuario) con otras capacidades de una NGCN de la misma empresa a través de la NGN (por ejemplo, geográficamente separadas).

NOTA 2 – Se supone que los requisitos de servicio heredados existentes se aplican en caso de conexión de PBX heredadas a las NGN.

17.3.2 Tipos de tráfico de empresa

El tráfico generado o recibido por una NGCN (o en su nombre) puede ser:

– Tráfico enviado a la NGN para su procesamiento de acuerdo con las normas habituales de la NGN. Este tipo de tráfico se conoce como tráfico de red pública.

– Tráfico enviado a la NGN para su procesamiento de acuerdo con un conjunto acordado de reglas específicas a la empresa. Este tipo de tráfico se conoce como tráfico de red privada. El tráfico de red privada pertenece normalmente a una única empresa, pero también puede existir entre dos empresas distintas, si ello no es objeto de prohibiciones reglamentarias.

NOTA – Una red de empresa puede establecer una distinción entre las comunicaciones de red privada que se originan en las NGN y las comunicaciones de red privada que se originan en la empresa. Este punto queda fuera del alcance de esta Recomendación.

Las NGN han de distinguir entre el tráfico de red pública y el tráfico de red privada.

Las NGN han de distinguir entre el tráfico de red privada que pertenece a una empresa y el tráfico que pertenece a otra empresa.

El tráfico de red privada puede necesitar un tratamiento en las NGN diferente del que recibe el tráfico de red pública.

Excepto cuando las leyes y reglamentos nacionales lo impiden, las NGN habrán de dar el mismo tratamiento al tráfico entre empresas y al tráfico de red pública. En estos casos, como parte de las capacidades ofrecidas a la empresa, las NGN pueden ofrecer capacidades de ingreso y/o egreso en nombre de cada empresa.

En el caso del tráfico de red privada, las NGN han de ser transparentes a los mecanismos de señalización, excepto cuando se necesita específicamente que las NGN intervengan para entregar el servicio solicitado por los clientes de empresa.

17.3.3 Capacidades de comunicación de empresa

Las NGN han de permitir la utilización de cualquier tipo de medio IP durante las comunicaciones de empresa, en función de la disponibilidad de recursos y de los acuerdos contractuales.

Excepto cuando esté autorizado por acuerdo explícito con una NGCN (por señalización o contrato), o a fin de ajustarse a los requisitos jurídicos formales, las NGN no han de intervenir en los medios que transportan.

NOTA 1 – Como ejemplos de motivos para la intervención acordada pueden citarse la transcodificación, la traducción y el puenteo. La no intervención por defecto tiene por objetivo evitar problemas indebidos de calidad de funcionamiento (en particular en lo que respecta a los datos de telemedida en tiempo real, el audio y el vídeo bidireccional) y para salvaguardar la confidencialidad percibida de los medios.

Se recomienda que las NGN permitan el transporte de la señalización misma mientras que otras redes se ocupan del transporte de los medios.

NOTA 2 – Por ejemplo, en la comunicación entre dos redes de empresa, las NGN pueden participar en la señalización (para asistir al encaminamiento entre la primera empresa y la segunda), pero el tráfico de medios puede fluir directamente por otras redes IP.

Las NGN puede opcionalmente ofrecer a una empresa las siguientes capacidades:

a) Línea arrendada virtual, cuando los sitios NGCN están interconectados por una NGN. Las NGN no ofrecen capacidades adicionales.

b) Aplicación de enlace empresarial, cuando la NGN es anfitriona de capacidades de tránsito entre NGCN, capacidades de ingreso de la NGN hacia la NGCN y capacidades de egreso desde la NGCN a la NGN. Una aplicación de enlace empresarial también puede ser anfitriona de otras capacidades además de las de ingreso, egreso y tránsito básicas hacia las NGCN. Normalmente no habrá equipos terminales de red conectados directamente a la NGN.

c) Servicios de empresa acogidos (HES), cuando una NGN sea anfitriona de las capacidades de comunicación de empresa de origen y/o terminación para las comunicaciones de empresa entre usuario directamente conectados a una NGN y que están abonados a estos servicios en tal NGN.

17.3.4 Gestión de la ubicación

Las NGN han de facilitar información de ubicación geográfica de un usuario de la NGCN a la NGCN. Este punto puede estar sujeto a requisitos de privacidad.

NOTA 1 – Una NGCN puede emplear la información de ubicación geográfica para, por ejemplo, prestar servicios basados en la ubicación al usuario NGCN.

NOTA 2 – El origen de la información de ubicación geográfica puede ser un usuario NGN o un usuario NGCN.

17.3.5 Señalización

Las NGN han de ofrecer una señalización normalizada para la interfaz con una NGCN.

17.3.6 Encaminamiento

17.3.6.1 Encaminamiento a un usuario NGCN

Las NGN han de soportar el encaminamiento a usuarios NGCN que no estén abonados al servicio NGN, pero a los que se pueda acceder a través de un sitio NGCN que tienen un acuerdo de enlace empresarial con una NGN.

NOTA – En este caso, el sitio NGCN está abonado al servicio NGN y los usuarios de la red empresarial de la NGCN no necesitan estar abonados al servicio NGN por sí mismos, pues pertenecen a la NGCN que los gestiona. Lo que se consigue con este requisito es que se pueda acceder a tales usuarios de la red empresarial desde la parte pública de la NGN utilizando una dirección pública para acceder directamente a ellos.

17.3.6.2 Encaminamiento basado en una gama de números

Para poder realizar el encaminamiento a usuarios de la red empresarial en una NGCN, se recomienda que las NGN soporten el encaminamiento únicamente a partir de una gama de números [UIT-T E.164] específica asignada a tal NGCN.

17.3.7 Control de QoS

Las NGN han de soportar el control de admisión de comunicación por sitios NGCN.

NOTA 1 – El proveedor NGN define el conjunto de reglas o políticas en función de las cuales se recomienda este punto, y se recomienda que el proveedor NGCN pueda configurar la capacidad siguiendo tales reglas y políticas.

Se ha de permitir fijar los siguientes umbrales por cada dirección (es decir, para comunicaciones entrantes y salientes):

1) número máximo de comunicaciones de sesión simultáneas;

2) número máximo de trenes simultáneos por comunicación.

Se podrán aceptar o rechazar las comunicaciones que superen los umbrales permitidos.

NOTA 2 – La empresa podrá seleccionar valores para el control de admisión de comunicación que correspondan al acuerdo de nivel de servicio (SLA) entre la empresa y el proveedor NGN. En este caso, las comunicaciones que superen el umbral permitido y que se acepten podrán someterse a reglas de tasación específicas.

17.3.8 Identificación

17.3.8.1 Identificación del sitio NGCN

Las NGN han de soportar la identificación de un sitio NGN con fines de autentificación y autorización.

NOTA 1 – La identificación del sitio NGCN es necesaria para que la NGN pueda determinar desde que sitio NGCN se está originando la comunicación.

NOTA 2 – Una NGCN puede tener más de un sitio NGCN y, por tanto, más de un identificador de sitio NGCN asociado.

17.3.8.2 Identificación de usuario de red de empresa

Además de los requisitos de denominación, numeración y direccionamiento de la cláusula 16, las NGN han de ofrecer la capacidad de identificar exclusivamente a los usuarios de la NGCN. Los identificadores de usuario NGCN serán asignados por la NGCN.

NOTA 1 – Esto no impide que una organización que ejerza de proveedor NGN pueda, ejerciendo otra función, administrar la NGCN de una empresa en nombre de la misma.

NOTA 2 – Este requisito garantiza que, en una comunicación entre un usuario NGCN y un usuario NGN, el servicio OIP (presentación de identidad de origen) del usuario NGN pueda presentar el identificador correcto del usuario NGCN llamante.

NOTA 3 – Este requisito garantiza que, en una comunicación entre un usuario NGN y un usuario NGCN, el servicio TIP (presentación de identidad de terminación) del usuario NGN pueda presentar el identificador correcto del usuario NGCN llamado.

NOTA 4 – Este requisito garantiza que los usuarios NGN puedan llamar a usuarios NGCN cuyos identificadores pertenezcan al grupo de identificadores disponibles para tal NGCN en virtud del acuerdo de enlace empresarial de esa NGCN.

No se recomienda que las NGN impidan a una NGCN asignar nuevos identificadores de usuario dentro de su dominio sin acuerdo previo con la NGN.

Se recomienda que las NGN soporten los identificadores de usuario NGNC que correspondan a números UIT-T E.164.

No se recomienda que las NGN impidan a una NGCN modificar las correspondencias entre identificadores de usuario dentro de su dominio y números UIT-T E.164 sin acuerdo previo con la NGN.

NOTA 5 – Esto implica que, para una comunicación entre la RTPC/RDSI y la NGCN, la NGN debe poder determinar que el número UIT-T E.164 llamado se encuentra dentro del dominio NGCN y, por tanto, encamine la comunicación a la NGCN indicando como destino el número UIT-T E.164 llamado o un identificador NGCN descubierto obtenido a partir de la información publicada por la NGCN (por ejemplo, DNS).

Se recomienda que las NGN soporten los identificadores de usuario NGCN que no correspondan a números UIT-T E.164.

NOTA 6 – Aunque no se pueda acceder directamente a los identificadores de usuario NGCN que no correspondan a números UIT-T E.164 desde la RTPC/RDSI, deberá ser posible acceder a ellos desde otros usuarios NGCN o NGN.

No se recomienda que las NGN impidan la entrega de llamadas e identificadores de usuario conectados de la NGCN, en función de la disponibilidad y no habiendo requisitos privados o reglamentarios que impidan tal entrega.

No se recomienda que las NGN impidan la aplicación de privacidad a las llamadas e identificadores de usuario conectados de una NGCN de manera permanente o por cada comunicación, de manera que tales identificadores no se divulguen a otras partes.

NOTA 7 – Esto significa que, en tales circunstancias, una NGN no debe entregar a otras partes un identificador facilitado por la NGCN (y marcado como privado) o un identificador por defecto asignado por la NGN a la NGCN.

17.3.9 Autentificación

La autentificación en el marco de una conexión entre una NGCN y una NGN habrá de cumplir los requisitos especificados en esta cláusula y en la cláusula 10.3.

17.3.10 Seguridad

La seguridad en el marco de una conexión entre una NGCN y una NGN habrá de cumplir los requisitos especificados en la cláusula 10.

17.3.11 Gestión de la movilidad

En esta cláusula se especifican los requisitos de itinerancia en el contexto de las comunicaciones de empresa.

Para la itinerancia en el contexto de las comunicaciones de empresa, se recomienda el soporte del nomadismo tanto para la movilidad de terminales como de personas.

En concreto, se recomienda que un usuario NGCN pueda registrarse y recibir servicios de su NGCN mientras esté en itinerancia hacia:

a) otro sitio NGCN de la misma NGCN interconectados por las NGN;

b) una NGN a la que esté directamente conectada la NGCN;

c) una NGN a la que esté indirectamente conectada la NGCN a través de otra NGN.

Por encima de todas las capacidades de itinerancia que han de facilitarse a los usuario NGN en virtud de esta cláusula, se recomienda que, de acuerdo con los acuerdos contraídos con la NGCN, un usuario NGN pueda registrarse y recibir servicios de su NGN mientras esté en itinerancia hacia:

a) una NGCN conectada a la NGN;

b) una NGCN indirectamente conectada a la NGN.

17.3.12 Contabilidad

Una empresa puede contabilizar el tráfico de sus capacidades de comunicación de empresa, ya pertenezcan a una NGCN o una NGN.

Para el tráfico de red pública se aplican los requisitos de [UIT-T Y.2201] y [UIT-T Y.2233].

Para el tráfico de red pública, la empresa y el proveedor NGN han de poder identificarse mutuamente a través de cualquier interfaz de interconexión, incluidas las interfaces intra-NGN hacia las capacidades de comunicación de empresa acogidas.

Para el tráfico de red privada, todas las empresas involucradas tendrán que poder identificarse mutuamente a través de cualquier interfaz de interconexión entre sus capacidades de comunicación de empresa.

Todas las capacidades de comunicación de empresa que residan en una NGN habrán de ser capaces de contabilizar el tráfico de red privada hacia la empresa del mismo modo que un proveedor NGN contabiliza su propio tráfico.

Además, en lo que respecta al tráfico de red privada, la empresa y el proveedor NGN habrán de poder identificarse mutuamente a través de cualquier interfaz de interconexión.

18 Interconexión e interfuncionamiento

La compatibilidad y el interfuncionamiento son dos funciones distintas que se definen, respectivamente, en [UIT-T Y.101] y en la serie de Recomendaciones UIT-T Y.1400.

18.1 Requisitos de interconexión

Se conocen dos tipos de interconexión entre las NGN, a saber:

– "La interconexión orientada a la conectividad": la que se basa en la conectividad IP sin importar los niveles de interoperabilidad que existan.

  NOTA 1 – Una interconexión de este tipo no reconoce el servicio específico extremo a extremo y, por ende, no es seguro que se puedan garantizar la calidad de funcionamiento específica del servicio, la QoS ni los requisitos de seguridad.

– "La interconexión orientada al servicio": la que permite a los operadores y proveedores de servicio ofrecer servicios con niveles de interoperabilidad definidos.

NOTA 2 – Por ejemplo, éste es el caso de los servicios UIT-T G.711 en una interconexión IP. Los niveles de interoperabilidad definidos son función del servicio, de la QoS, de la seguridad, etc.

NOTA 3 – Sólo la interconexión orientada al servicio satisface plenamente los requisitos de compatibilidad de las NGN.

Los requisitos para la interconexión son:

1) Se ha de soportar el tipo de interconexión orientada a la conectividad entre las NGN.

   Se ha de soportar este tipo de interconexión entre NGN utilizando distintas versiones del IP.

2) Se ha de soportar la interconexión orientada al servicio entre las NGN.

   Se ha de soportar este tipo de interconexión entre NGN utilizando distintas versiones del IP.

3) Se ha de soportar la interconexión orientada al servicio entre las NGN y las NGCN, cuando la NGN acoja los servicios de empresa.

   Se ha de soportar este tipo de interconexión entre NGN y NGCN utilizando distintas versiones del IP.

18.1.1 Interconexión orientada al servicio entre NGN basadas en IMS

Los requisitos para la interconexión orientada al servicio entre NGN basadas en IMS son:

1) El enlace lógico de interconexión entre proveedores NGN ha de "conocer" los servicios NGN específicos. Puede ser un enlace físico o lógico que transporte datos y portadoras de señalización. Las NGN han de ofrecer una interfaz normalizada de interconexión con otra NGN.
2) El enlace de interconexión ha de disponer del control de recursos a fin de tratar las distintas características de los datos y portadoras de señalización de los distintos servicios.
3) Han de tenerse en cuenta las características de seguridad y contabilidad.

Quedan en estudio otros requisitos concretos de la interconexión orientada al servicio (por ejemplo, los aspectos de señalización, códec, encaminamiento, seguridad, tasación y contabilidad, recursos, QoS y SLA).

18.2 Requisitos de compatibilidad

Con el fin de poder prestar ciertos servicios a través de un trayecto extremo a extremo que abarque una o varias NGN:

1) los componentes de servicio apropiados de una sola red NGN deberán ser compatibles entre ellos;
2) no se prohíbe la compatibilidad de NGN interconectadas que posean conjuntos idénticos de capacidades de servicio.

18.3 Requisitos de interfuncionamiento

Con el fin de poder prestar ciertos servicios, las NGN tendrán que interfuncionar con diversos tipos de redes. Los servicios de los que trata este interfuncionamiento se deberán prestar sin interrupción en la infraestructura de uno o varios proveedores de red. En la versión 1 de las NGN se suministran capacidades, incluidas, entre otras, la de seguridad, la OAM, la resiliencia, la QoS y, cuando fuere necesario, la transcodificación de medios, para el soporte de los diferentes casos de interconexión con otras redes que no sean NGN, a fin de garantizar un funcionamiento extremo a extremo sin interrupciones.

Para que se puedan prestar ciertos servicios en un trayecto extremo a extremo que abarque una combinación de redes NGN y otras que no pertenezcan a esa categoría:

– Las NGN deberán poder interfuncionar con redes que no lo sean.

– Se recomienda que las NGN tengan como fin el soporte de las siguientes capacidades de interfuncionamiento:

  - el encaminamiento;
  - el interfuncionamiento de señalización;
  - el interfuncionamiento de numeración, denominación o direccionamiento;
  - el intercambio de información relativa a la contabilidad y la tasación;
  - el interfuncionamiento de seguridad;
  - el interfuncionamiento de QoS;
  - el intercambio de información de perfil de usuario y de terminal;
  - el interfuncionamiento de medios;
  - el interfuncionamiento de gestión;
  - la gestión de política (por ejemplo, dependiendo de la política aplicable entre dominios, tal vez haya que esconder o suprimir alguna información interna de un dominio de confianza, incluyendo información relacionada con el usuario, del flujo de información intercambiado en la interfaz entre el dominio de confianza y otro que no lo es), incluida la resolución de diferencias relacionadas con las políticas en vigor.

  NOTA – Lo anterior no implica que haya interfuncionamiento entre todos los servicios o características de servicio. Puede ocurrir que estos requisitos sólo valgan para el interfuncionamiento entre ciertos servicios o características de servicio específicos (que muy probablemente serán similares o idénticos).

18.3.1 Interfuncionamiento con la RTPC/RDSI

Para interfuncionar correctamente con RTPC/RDSI, es necesario cumplir los siguientes requisitos:

1) Interfuncionamiento entre la RTPC/RDSI y los servicios de emulación RTPC/RDSI. Se ha de proporcionar un alto nivel de interoperabilidad con los servicios de la RTPC/RDSI que están siendo emulados. Es potestad de los operadores, y en algunos casos de los reguladores nacionales, determinar cuánta interoperabilidad de servicio se ha de suministrar.

2) Interfuncionamiento entre la RTPC/RDSI y los servicios de simulación RTPC/RDSI. Se debe aceptar la interoperabilidad de los servicios de simulación RTPC/RDSI con los servicios suplementarios RTPC/RDSI, aunque con ello se pueda limitar la capacidad de servicio.

3) Interfuncionamiento entre la RTPC/RDSI y los servicios multimedios IP NGN, aunque con ello se pueda limitar la capacidad de servicio.

NOTA 1 – Lo anterior no implica que todos los servicios o las características de servicio NGN puedan interfuncionar con la RTPC/RDSI y viceversa. Puede ocurrir que estos requisitos sólo valgan para el interfuncionamiento entre ciertos servicios o características de servicio específicos (que muy probablemente serán similares o idénticos) ofrecidos tanto por la NGN como por la RTPC/RDSI.

NOTA 2 – En la versión 1 se soportan las redes de empresas basadas en circuitos, cuando se conectan a las NGN a través de una RTPC/RDSI o cuando se emula la RTPC/RDSI, gracias a una pasarela de interfuncionamiento.

18.3.2 Interfuncionamiento con otras redes

1) Las NGN proveerán la capacidad de interconexión directa para redes basadas en circuitos, entre las cuales se cuentan, como mínimo, las de difusión y las móviles terrestres públicas. Los requisitos de interfuncionamiento para todas las redes basadas en circuitos son idénticos a los del interfuncionamiento con la RTPC/RDSI.

   Las NGN permitirán la capacidad de interconexión orientada a la conectividad con redes basadas en el IP que no sean NGN.

Las NGN permitirán la capacidad de interconexión orientada a la conectividad con redes basadas en IP que no sean NGN utilizando distintas versiones del IP.

Las NGN no impedirán la capacidad de interconexión orientada al servicio con redes basadas en el IP que no sean NGN.

Siempre y cuando la red interconectada provea todas las capacidades de interfuncionamiento, con arreglo a la cláusula 18.3, una determinada implementación tal vez pueda soportar dichas interconexiones de red. Las características y la funcionalidad de las redes basadas en el IP que no son NGN son tan diversas y abundantes que en la versión 1 no ha sido posible establecer claramente sus requisitos de interconexión.

2) Las NGN no excluirán deliberadamente la interconexión con redes no NGN basadas en el IP.

NOTA – En la cláusula 10.6 se describen los requisitos de seguridad para este caso.

18.4 No divulgación de información en las interfaces NNI y ANI

Cuando se requiera, por ejemplo, por reglamentación, por ley, por condiciones nacionales o regionales, las NGN podrán:

– evitar la divulgación de información interna o información de los usuarios del servicio a otras entidades a través de las interfaces NNI;

– evitar la divulgación de información interna de la red, así como de información de los usuarios de la red a otras entidades a través de las interfaces NNI;

– evitar la divulgación de información interna o información de los usuarios del servicio a otras entidades a través de las interfaces ANI;

– evitar la divulgación de información interna de la red, así como de información de los usuarios de la red a otras entidades a través de las interfaces ANI.

18.5 Intercambio entre proveedores de información sobre los usuarios

Cuando se requiera, por ejemplo, por reglamentación, por ley, por condiciones nacionales o regionales, las NGN tendrán que soportar mecanismos para el intercambio de información sobre los usuarios entre NGN con fines de compatibilidad de servicio.

19 Requisitos de servicio específicos

19.1 Emulación RTPC/RDSI

La evolución de las redes hacia las NGN es función de las decisiones que tomen y de las necesidades que tengan los operadores. El derrotero que han de seguir depende de cuáles sean sus recursos, y sus planes y estrategias comerciales, con lo cual puede haber una amplia gama de tecnologías y su periodo de implantación puede opcionalmente variar.

A los efectos del periodo de transición de las RTPC/RDSI a las NGN, estas últimas deben poseer las siguientes capacidades:

1) Emulación RTPC/RDSI.

2) Simulación RTPC/RDSI.

A continuación se describen los requisitos correspondientes.

19.1.1 Requisitos generales

Una red NGN deberá soportar un servicio de emulación RTPC/RNIS con un nivel de servicio que ofrezca capacidades iguales o superiores a aquellas ofrecidas por la red de conmutación de servicios.

19.1.2 Terminales

Las NGN soportarán los terminales tradicionales (por ejemplo, teléfonos RTPC, teléfonos de texto, telefaxes y otros tipos existentes de terminales RTPC/RDSI) que no estás sujetos a una interfaz UNI NGN, pero por una interfaz UNI de tipo RTPC/RDSI.

NOTA – Puede ocurrir que la emulación del conjunto completo de servicios RTPC/RDSI no sea posible y que el soporte del servicio se restrinja a determinados tipos de terminal, es decir a terminales tradicionales o a equipos de usuario que se comporten como terminales tradicionales.

19.1.3 Servicios

Los requisitos de servicio para la emulación RTPC/RDSI son:

1) Las NGN soportarán la emulación, por parte de los proveedores que ofrecen servicios RTPC/RDSI, de uno o varios de dichos servicios.

2) Las NGN soportarán definiciones de capacidad heredadas de la especificación RTPC/RDSI existente.

NOTA – Puede ocurrir que una determinada NGN no soporte todas las posibles capacidades e interfaces que existen en la RTPC/RDSI.

19.2 Servicios conversacionales multimedios en tiempo real, incluida la simulación RTPC/RDSI

19.2.1 Requisitos generales

Las NGN soportarán los servicios de simulación RTPC/RDSI que permiten al usuario sentirse como en un entorno RTPC/RDSI.

19.2.2 Terminales

Las NGN soportarán terminales no tradicionales para los servicios de simulación RTPC/RDSI. También pueden soportar dispositivos de adaptación, para que los terminales tradicionales (por ejemplo, los teléfonos clásicos, los teléfonos de texto y los telefaxes) puedan conectarse a las NGN.

19.2.3 Servicios

Los requisitos de servicio para la simulación RTPC/RDSI son:

1) Las NGN soportarán capacidades de servicio del tipo RTPC/RDSI, mediante el control de sesión a través de interfaces e infraestructura IP.

2) Se recomienda que las NGN permitan que un proveedor de servicio simule servicios RTPC/RDSI.

3) Las NGN no están obligadas a prestar servicios idénticos a los de la RTPC/RDSI.

NOTA – Se supone que los servicios de simulación RTPC/RDSI no emplean modelos de llamada o protocolos de señalización RTPC/RDSI.

19.3 Servicios TVIP

Los servicios TVIP ofrecidos por las NGN se definen de la siguiente manera.

Esta Recomendación contiene los requisitos de alto nivel aplicables a las NGN para el soporte de los servicios TVIP.

A fin de soportar los servicios TVIP, las capacidades NGN en principio han de soportar los requisitos descritos en [UIT-T Y.1901], sustituyéndose en su formulación "la arquitectura TVIP" por "el entorno NGN". Quedan en estudio consideraciones específicas, como qué capacidades NGN concretas soportan los requisitos identificados en [UIT-T Y.1901] y si se aplican por igual a todos los servicios o aplicaciones TVIP.

19.3.1 Oferta de servicio

La arquitectura NGN ha de soportar mecanismos para servicios TVIP a la carta (incluido el vídeo a la carta sin solicitud previa del usuario [UIT-T Y.1901]), los servicios de retransmisión de radiodifusión [UIT-T Y.1901] (incluida la TV lineal [UIT-T Y.1901]) y los servicios interactivos. Se recomienda que la arquitectura NGN soporte mecanismos para cPVR [UIT-T Y.1901] y nPVR [UIT-T Y.1901]. Se recomienda el soporte de la funcionalidad modo truco [UIT-T Y.1901] para la implementación de algunos servicios TVIP.

Se recomienda que la arquitectura NGN soporte mecanismos mediante los cuales los usuarios extremos puedan poder a disposición de otros usuarios extremos los contenidos producidos/creados por ellos.

La arquitectura NGN ha de soportar que el usuario extremo tenga la capacidad de elegir una opción idiomática preferida (audio, subtítulos [UIT-T Y.1901], comentarios [UIT-T Y.1901], contenidos suplementarios [UIT-T Y.1901] y descripciones en audio [UIT-T Y.1901]) entre varios idiomas predefinidos por el proveedor de contenido y ofrecidos por el proveedor de servicio.

NOTA – Puede encontrarse más información sobre los "servicios a la carta" en [b-UIT-T Y-Sup.5].

19.3.2 Transporte y movilidad

Para el soporte de los servicios TVIP son aplicables los requisitos de transporte de la cláusula 6, incluido el soporte de multidifusión.

Para el soporte de los servicios TVIP, son aplicables los requisitos de tratamiento de la movilidad de la cláusula 12.

19.3.3 Activadores de servicio

La arquitectura NGN ha de soportar las capacidades de descubrimiento y selección, así como la de navegación para los contenidos y servicios TVIP.

Se recomienda que la arquitectura NGN soporte el rastreo de datos del espectador, al tiempo que se protege debidamente la privacidad del usuario.

Se recomienda que la arquitectura NGN permita la recopilación de estadísticas de utilización de contenido y el rastreo del mismo.

Se recomienda que la arquitectura NGN disponga de medios para que sólo los espectadores correspondientes puedan ver el contenido, en función de la zona geográfica, el control parental y los grupos específicos. En concreto, la arquitectura NGN ha de soportar mecanismos para bloquear la transmisión de contenido a zonas geográficas específicas, siempre y cuando se apliquen los requisitos de bloqueo.

19.3.4 Middleware y metadatos

Se prohíbe que la arquitectura NGN impida la utilización de middleware y metadatos especificados para los servicios TVIP.

19.3.5 QoS

Las redes que soportan la TVIP han de soportar las clases de QoS IP y satisfacer los correspondientes requisitos de calidad de funcionamiento especificados en [UIT-T Y.1541], lo que incluye el mantenimiento de un exacto control temporal de la sincronización, por ejemplo, sincronización con el movimiento de los labios. Se recomienda que la arquitectura NGN soporte medios para ofrecer tiempos de cambio de canal [UIT-T Y.1901] con suficiente calidad percibida (QoE).

Las NGN han de soportar un marco que identifique los componentes y puntos de medición (incluido el dispositivo de usuario extremo) para la medición de la calidad de servicio (QoSM).

19.3.6 Seguridad

La arquitectura NGN ha de soportar la protección de servicios y contenido.

19.3.7 Gestión

Se recomienda que la arquitectura NGN soporte la actualización y descarga de software (a distancia) para los dispositivos TVIP.

19.3.8 Medios

La arquitectura NGN no podrá impedir la utilización de cualquier formato de vídeo y audio (incluidas las resoluciones de vídeo, relaciones de aspecto de vídeo, velocidades de muestreo de audio y profundidades de bits de audio) especificados para los servicios TVIP.

La arquitectura NGN no podrá impedir la utilización de ningún códec de vídeo y audio especificado por los servicios TVIP.

Se habrá de evitar, siempre que sea posible, la transcodificación durante la entrega de contenidos TVIP en la arquitectura NGN.

19.3.9 Tasación

La arquitectura NGN habrá de soportar mecanismos para recopilación de datos con fines de contabilidad e información, acuerdos de asociación y reconciliación de utilización por parte del usuario extremo, como los abonos al servicio, las compras y las transacciones a fin de soportar opciones de tasación como el pago por visión [UIT-T Y.1901].

19.3.10 Aspectos relativos al terminal

Un dispositivo terminal que soporte servicios TVIP habrá de poder seleccionar, recibir y entregar múltiples informaciones de audio, vídeo y de control asociadas.

Se recomienda que la arquitectura NGN soporte tales capacidades de terminal y adquiera las capacidades necesarias para ajustarse a la configuración del servicio.

19.3.11 Interfuncionamiento

Quedan en estudio los requisitos de soporte del interfuncionamiento de los servicios TVIP.

19.3.12 Interés público

La arquitectura NGN ha de soportar los dispositivos terminales para los servicios TVIP, que estén constantemente a la escucha de mensajes de notificación de alertas de emergencia (EAN).

La arquitectura NGN ha de soportar la disponibilidad de características de accesibilidad (subtitulados, comentarios, audio descriptivo y múltiples trenes de vídeo, como para el lenguaje de signos) y su sincronización con el contenido principal cuando se efectúe una reproducción normal.

Se recomienda que la arquitectura NGN soporte la transmisión de vídeo o datos con suficiente calidad para la percepción de la interpretación a lenguaje de signos, incluida la lectura labial. Para ello se requiere la transmisión de un número suficiente de tramas por segundo y suficiente resolución espacial para reproducir con detalle las manos, cara, labios, ojos y cuerpo de la persona que habla por signos [b-UIT-T H-Sup.1]

19.4 Servicios de empresa

19.4.1 Servicio de línea arrendada virtual

En esta Recomendación no se identifican requisitos específicos del servicio.

19.4.2 Aplicación de enlace empresarial

En esta Recomendación no se identifican requisitos específicos del servicio.

19.4.3 Servicios de empresa propios

Cuando las NGN ofrecen servicios de empresa propios, han de:

– Soportar las comunicaciones de empresa en las que participan tanto usuarios de la NGCN como usuarios del HES, incluidas las comunicaciones entre un usuario de la NGCN y un usuario del HES.
– Permitir a un usuario de empresa trasladarse entre una ubicación de la NGCN y una ubicación del HES sin necesidad de que la otra parte en la comunicación esté al tanto del cambio.
– Permitir a un usuario de empresa trasladar su terminal de una ubicación de la NGCN a una ubicación del HES con una reconfiguración mínima.

19.5 Aplicaciones y servicios utilizando la identificación por etiquetas

Cuando las NGN ofrezcan aplicaciones y servicios que utilizan la identificación por etiquetas [UIT-T Y.2213], definirán los requisitos de servicio específicos correspondientes.

19.6 Servicios de entrega gestionados

Cuando las NGN ofrezcan servicios de entrega gestionados [UIT-T Y.2212], definirán los requisitos de servicio específicos correspondientes.

19.7 Servicios de vigilancia visual

El servicio de vigilancia visual de terminal a terminal permite que un terminal reciba y controle la información multimedios producida por el otro terminal (fuente), así como que controle a distancia el dispositivo fuente.

El servicio de vigilancia visual de servidor a terminal permite a múltiples terminales recibir y controlar la misma información multimedios producida por un único servidor fuente.

El servicio de vigilancia visual de terminal a servidor permite a un servidor recopilar múltiples partes o un conjunto de partes de la información multimedios producida por múltiples terminales (fuentes).

Cuando las NGN ofrecen servicios de vigilancia visual, han de soportar:

– El servicio de vigilancia visual de terminal a terminal (incluido de uno a uno y de uno a muchos) (por ejemplo, servicio de vigilancia visual para la supervisión de seguridad doméstica).
– El servicio de vigilancia visual de servidor a terminal (incluido de uno a uno y de uno a muchos) (por ejemplo, servicio de vigilancia visual para la supervisión del tráfico público).

Quedan en estudio los requisitos relativos al servicio de vigilancia visual de terminal a servidor.

19.7.1 Servicio de vigilancia visual de servidor a terminal

Las NGN han de soportar las capacidades de descubrimiento y selección, así como la de navegación para el servicio de vigilancia visual de servidor a terminal.

Se recomienda que las NGN permitan la realización de estadísticas de utilización de contenido y el rastreo del mismo.

Se recomienda que la arquitectura NGN disponga de medios para que sólo los espectadores correspondientes puedan ver el contenido, en función de la zona geográfica, el control parental y los grupos específicos. En concreto, la arquitectura NGN ha de soportar mecanismos para bloquear la transmisión de contenido a zonas geográficas específicas, siempre y cuando se apliquen los requisitos de bloqueo.

Las NGN han de soportar la protección de servicios y contenido.

Se recomienda que las NGN soporten la actualización y descarga de software (a distancia) para los dispositivos de vigilancia visual de servidor a terminal.

19.7.2 Servicio de vigilancia visual de terminal a terminal

Para soportar el servicio de vigilancia visual de terminal a terminal, las NGN han de cumplir los requisitos expuestos en las siguientes subcláusulas.

19.7.2.1 Tratamiento de sesión

Las NGN han de soportar el control de admisión de sesión con información relativa a la vigilancia visual.

Las NGN han de soportar el tratamiento de sesión con información relativa a la vigilancia visual (por ejemplo, datos específicos del servicio, como control a distancia).

19.7.2.2 Encaminamiento

Las NGN han de soportar el encaminamiento basado en las capacidades del terminal de origen y/o de terminación (por ejemplo, soporte de medios).

19.7.2.3 Códecs

La arquitectura NGN ha de permitir la utilización de todos los códecs de vídeo y audio especificados para el servicio de vigilancia visual.

La arquitectura NGN evitará, siempre que sea posible, la transcodificación durante la entrega de información de vigilancia visual.

19.8 Aplicaciones y servicios de red de sensor ubicua (USN)

Quedan en estudio los requisitos específicos del servicio.

19.9 Servicios de centros de comunicaciones multimedios

Quedan en estudio los requisitos específicos del servicio.

19.10 Servicios VPN en las NGN

Cuando las NGN ofrezcan servicios VPN [UIT-T Y.2215], definirán los requisitos de servicio específicos correspondientes.

20 Interés público

Las NGN ofrecerán las capacidades necesarias para la prestación de los servicios de interés general requeridos por la reglamentación o las leyes de autoridades regionales o nacionales, o conforme a tratados internacionales. Entre dichos servicios se pueden contar los que se describen en esta cláusula.

20.1 La interceptación legal

1) Un proveedor de transporte o de servicio NGN cumplirá con las exigencias de interceptación legal. Por tanto, las NGN proporcionarán los mecanismos que hagan posible dicha interceptación cuando una tal posibilidad esté requerida por los reglamentos o la ley de un país en la zona de aplicación.

2) Gracias a los mecanismos de interceptación legal, las autoridades podrán acceder al contenido de la comunicación e interceptar la información pertinente con arreglo a los requisitos de las administraciones y conforme a los tratados internacionales.

Tratándose de un aspecto que depende de las costumbres y de las leyes de cada país o región, los requisitos que ha de cumplir la interceptación legal son función del entorno reglamentario en cuestión.

20.2 Identificación de comunicaciones malintencionadas

Las NGN contarán con la capacidad de identificar el origen de una comunicación malintencionada, por ejemplo, a través de la obtención de la identidad del terminal involucrado o de quien origina la comunicación.

20.2.1 Identificación de comunicaciones malignas para empresas

Una comunicación identificada como tráfico de red pública habrá de tratarse de conformidad con los requisitos de identificación de comunicaciones malignas de las NGN.

La identificación de comunicaciones malignas en el tráfico de red privada queda fuera del alcance de esta Recomendación. Se prohíbe que las NGN traten tales comunicaciones. Lo mismo se aplica a una capacidad NGCN propia.

NOTA – Pueden aplicarse requisitos reglamentarios distintos al tráfico de red privada.

20.3 Comunicaciones no solicitadas

Las NGN dispondrán de las capacidades necesarias para impedir las comunicaciones no solicitadas (UC).

Las NGN han de ofrecer la capacidad de tratar intentos de comunicación detectados y marcados a fin de poder reaccionar contra ellos (por ejemplo, redireccionamiento de la comunicación a un buzón de correo, buzón vocal o correo no deseado).

Se recomienda que las NGN dispongan de mecanismos para contrarrestar las UC (por ejemplo, lista negra/blanca, sistema de reputación, ocultación de dirección, filtrado de contenido).

NOTA 1 – Puede encontrarse más información sobre estos mecanismos en [b-UIT-T X.1244]

Se recomienda que las NGN dispongan de un mecanismo para la información de UC por parte de los usuarios de las NGN.

Se recomienda que las NGN dispongan de un mecanismo para auditar los informes de UC presentados por los usuarios de las NGN.

Se recomienda que las NGN:

- Ofrezcan la capacidad necesaria para que un usuario afectado por una UC solicite el marcado de UC (clasificación).
- Ofrezcan la capacidad necesaria para que un usuario afectado por una UC modifique el marcado de UC.

NOTA 2 – Puede encontrarse más información sobre la clasificación de UC en [b-ETSI TS 187 009].

20.4 Telecomunicaciones de emergencia

Las telecomunicaciones de emergencia (incluido el soporte de la advertencia temprana) son:

– las telecomunicaciones de una persona hacia la autoridad, por ejemplo, llamadas a los proveedores de servicios de emergencia;

– las telecomunicaciones de una autoridad hacia otra, por ejemplo, el servicio de telecomunicaciones de socorro (TDR, *telecommunications for disaster relief*);

– las telecomunicaciones de una autoridad hacia las personas, por ejemplo, servicios de información comunal.

NOTA – Además de ser utilizados en las telecomunicaciones de una autoridad hacia otra, el TDR y el servicio de telecomunicaciones de emergencia (ETS, *emergency telecommunications service*) también pueden servir en el marco de las telecomunicaciones de las autoridades hacia las personas.

Las Recomendaciones [UIT-T Y.1271], [UIT-T E.106] y [UIT-T E.107] proporcionan, respectivamente, los "Requisitos y capacidades de red generales necesarios para soportar telecomunicaciones de emergencia en redes evolutivas con conmutación de circuitos y conmutación de paquetes", un "Plan internacional de preferencias en situaciones de emergencia para actuaciones frente a desastres" y un "Servicio de telecomunicaciones de emergencia y un marco de interconexión para las implementaciones nacionales del ETS".

Las NGN pondrán las capacidades de red a disposición de las aplicaciones que requieren un aviso oportuno, por ejemplo, el suministro de información de ubicación geográfica necesaria para que los mensajes de alerta lleguen sólo a quienes están en peligro de sufrir los efectos de un desastre inminente.

El soporte de las telecomunicaciones de emergencia y de los avisos oportunos hace necesario que las NGN sean resistentes en su funcionamiento y altamente disponibles.

Las NGN:

1) Dispondrán, en los niveles de transporte y de servicio, de capacidades que permitan dar curso a las telecomunicaciones de emergencia conforme a esquemas de prioridad o preferenciales. El control de llamada o de sesión de las telecomunicaciones de emergencia y el tráfico de dichas telecomunicaciones tendrán un tratamiento prioritario en condiciones de congestión o de fallo.
2) Suministrarán, si fuere necesario, el interfuncionamiento y la correspondencia de mecanismos de prioridad entre los diversos componentes de las NGN (por ejemplo, entre las redes de acceso y troncal, y entre los estratos de servicio y de transporte) y entre las NGN propiamente dichas (por ejemplo, entre dos redes troncales de proveedores de servicios), garantizando así telecomunicaciones adecuadas, prioritarias o preferenciales, de extremo a extremo.
3) Aceptarán los servicios de telecomunicaciones existentes, incluido uno equivalente a todos los servicios existentes de telecomunicaciones de emergencia RTPC/RDSI, aun cuando una o varias de las entidades que se comunican estén conectadas a una NGN y una o varias más a la RTPC/RDSI.
4) Crearán nuevos medios de telecomunicaciones de emergencia (por ejemplo, de mensajería instantánea) que han de ser soportados en futuros entornos establecidos por las autoridades (por ejemplo, proveedores de servicios de emergencia).
5) Proveerán un interfuncionamiento sin interrupciones de las telecomunicaciones de emergencia en las redes públicas, dentro de un dominio (de emergencia) administrativo.
6) Encaminarán las telecomunicaciones de emergencia hasta las autoridades competentes.
7) Encaminarán las telecomunicaciones de emergencia desde las autoridades hasta las personas.
8) Garantizarán, de ser posible, la continuidad de las telecomunicaciones de emergencia entre las autoridades y las personas, hasta que las autoridades terminen la sesión, aun en el caso de que las personas la interrumpan.
9) Suministrarán a las autoridades información relativa a la ubicación geográfica de los individuos, así como su identidad, con arreglo a los requisitos reglamentarios nacionales o regionales en vigor. Siempre que la reglamentación o la ley así lo exijan, la autoridad puede obtener esta información aunque la persona haya solicitado su confidencialidad.

10) Proporcionarán la capacidad de acceder, con o sin autenticación, a los servicios de telecomunicaciones de emergencia, de acuerdo con los requisitos reglamentarios nacionales o regionales en vigor. Por ejemplo, las NGN permitirán autenticar usuarios con el fin de acceder a las telecomunicaciones ETS/TDR.

11) Aceptarán que se eximan los servicios de telecomunicaciones de emergencia de las restricciones que imponen ciertas funciones de gestión de red.

12) Soportarán las telecomunicaciones de emergencia con medios alternativos y medios múltiples, cuando se requieran (por ejemplo, por reglamentación o por ley). El vídeo, el texto, la voz, y cualquier combinación de ellos, al igual que diversas formas de mensajería, son fundamentales para las telecomunicaciones de personas discapacitadas con los servicios de emergencia.

13) Proporcionarán capacidades que garanticen que sólo se distribuyan los mensajes de alerta oportuna autorizados.

14) Proporcionarán capacidades para evitar el envío de mensajes de tipo alerta oportuna que no estén destinados específicamente a los receptores y que no sean indispensables.

20.4.1 Telecomunicaciones de emergencia para empresas

Tanto el tráfico de red pública como el tráfico de red privada pueden transportar telecomunicaciones de emergencia para empresas.

1) Una telecomunicación de emergencia para empresa identificada como tráfico de red pública se tratará de conformidad con los requisitos de telecomunicaciones de emergencia de las NGN.

2) En caso de telecomunicación de emergencia para empresa de tráfico de red pública, las NGN habrán de remitir la información de ubicación geográfica recibida de la NGCN y, posiblemente, utilizarla para su encaminamiento a las autoridades correspondientes. Este punto puede estar sometido a requisitos reglamentarios y de privacidad.

3) El encaminamiento de comunicaciones identificadas como telecomunicaciones de emergencia de tráfico de red privada queda fuera del alcance de los documentos relativos a las NGN. Las NGN no han de tratar tales comunicaciones. Esto mismo se aplica a una capacidad NGCN propia.

4) De conformidad con los reglamentos y leyes nacionales, los planes privados de numeración o marcación empleados dentro de una empresa pueden reutilizar los números nacionales de emergencia para otros fines y pueden emplear un número distinto para las llamadas de emergencia.

5) De conformidad con los reglamentos y leyes nacionales, cuando una empresa privada explote un PSAP privado, las NGN podrán soportar el encaminamiento de las telecomunicaciones de emergencia para empresas del tráfico de red pública al PSAP privado (o a uno de varios PSAP privados) o a un PSAP público, en función de las circunstancias. Por ejemplo, para un llamante físicamente ubicado en un sitio de empresa concreto, se puede exigir el encaminamiento al PSAP privado de ese sitio, mientras que para los llamantes físicamente ubicados en otros lugares, se puede exigir el encaminamiento a un PSAP público.

20.5 Presentación y privacidad de la identidad de usuario

1) Las NGN habrán de presentar la identidad de la parte que origina.

2) Las NGN habrán de presentar la identidad de la parte que termina.

3) Las NGN habrán de suprimir la presentación de la identidad de la parte que origina.

4) Las NGN habrán de suprimir la presentación de la identidad de la parte que termina.

NOTA – Es posible que los requisitos que han de cumplirse para el soporte de las telecomunicaciones de emergencia impidan la supresión.

20.6 Selección de proveedor de red o de servicio

Las NGN soportarán la capacidad de selección de proveedor, cuando así se requiera (por ejemplo, por reglamentación o por ley).

20.7 Usuarios discapacitados

Estos usuarios necesitan, en general, medios para controlar y utilizar terminales y servicios en formas y modos específicos, que abarcan una gama de capacidades y preferencias. La mejor manera de satisfacer dichos requisitos consiste en tenerlos en cuenta en el diseño mismo de terminales y servicios.

1) Las NGN proveerán los medios necesarios para la invocación de servicios de retransmisión, que son los que traducen servicios entre varios modos de comunicación útiles para las personas discapacitadas (por ejemplo, el lenguaje de signos, la lectura de los labios, el texto, la voz). La invocación de servicios de retransmisión se puede basar en las preferencias del usuario, la resolución de direcciones o las instrucciones de usuario.
2) Las NGN permitirán que cualquiera de las dos partes involucradas en una telecomunicación de emergencia invoque los servicios de retransmisión.

NOTA 1 – En la cláusula 20.4 se tratan otras necesidades de los usuarios discapacitados de los servicios de telecomunicaciones de emergencia.

NOTA 2 – Véase también en [b-ITU-T Accesibilidad] y [b-ITU-T F.790].

20.8 Portabilidad de número

La portabilidad de número es una capacidad de red de la RTPC/RDSI.

La capacidad NGN equivalente es la portabilidad de identidad (cláusula 10.2). La emulación RTPC/RDSI no impone nuevos requisitos de soporte de la portabilidad de número, puesto que los servicios emulados se heredan de la RTPC/RDSI (véase la cláusula 19.1.3).

20.9 Desagregación (*unbundling*) de servicios

En muchas jurisdicciones nacionales se requiere que los proveedores de servicios "desglosen" sus ofertas, para que los usuarios puedan escoger diferentes proveedores para diferentes servicios, y que los proveedores puedan prestar competitivamente sus servicios a los usuarios.

Cuando se requiera, por ejemplo, por reglamentación o por ley, las NGN tendrán que soportar mecanismos para desglosar los servicios.

20.10 Rechazo de comunicaciones anónimas

Las NGN han de ofrecer un mecanismo que permita a un usuario rechazar comunicaciones entrantes cuando el llamante es anónimo.

20.10.1 Rechazo de comunicaciones anónimas para empresas

Una comunicación identificada como tráfico de red pública habrá de tratarse de conformidad con los requisitos de rechazo de comunicaciones anónimas de las NGN.

Los requisitos de tratamiento de comunicaciones anónimas de tráfico de red privada quedan fuera del alcance de esta Recomendación. Las NGN no han de tratar tales comunicaciones. Esto mismo se aplica a una capacidad NGCN propia.

NOTA – Pueden aplicarse requisitos reglamentarios distintos al tráfico de red privada.

Apéndice I

Principales diferencias, en términos de capacidades y requisitos de alto nivel, entre la presente versión de la Recomendación UIT-T Y.2201 (Y.2201 Rev.1) y la anterior versión de la Recomendación UIT-T Y.2201 (2007)

(Este apéndice no es parte integrante de esta Recomendación)

En este apéndice se enumeran las principales diferencias, en términos de capacidades y requisitos de alto nivel, entre la presente Recomendación y UIT-T Y.2201 (04/07) [UIT-T Y.2201].

NOTA – Queda en estudio la compleción de este apéndice.

Capacidad en UIT-T Y.2201 Rev.1	Cláusula en esta Recomendación	Cláusula en UIT-T Y.2201 (2007) (si procede)	Mejoras con respecto a Y.2201 (2007)	Nueva capacidad
OAM			Ninguna	–
Movilidad			Soporte de traspaso	–
Conocimiento del contexto		–	–	X

Apéndice II

Correspondencia entre servicios y habilitadores de servicio

(Este apéndice no es parte integrante de esta Recomendación)

NOTA – Queda en estudio la compleción del presente apéndice.

En este apéndice se presenta un ejemplo de correspondencia entre algunos servicios y sus habilitadores (cláusula 7.2). Esta correspondencia no es exhaustiva ni representa requisitos de servicio.

Cuadro II.1 – Correspondencia ilustrativa entre servicios y habilitadores de servicio

Servicios/Habilitadores de servicio	Presencia	Gestión de la ubicación	Gestión de grupo	Tratamiento de mensajes	Soporte de multidifusión	"Push"	Tratamiento de sesión	Gestión de información personal	Gestión de dispositivo	Soporte de aplicaciones web	Sincronización de datos
Servicios vocales conversacionales en tiempo real							X				
Servicios conversacionales multimedios en tiempo real							X				
Texto en tiempo real							X				
Servicios de mensajería	X		X	X			X				
Solicitud de conversación en las NGN	X		X				X				
Servicios multimedios interactivos punto a punto			X				X				
Servicios de comunicación interactivos colaborativos		X	X				X				
Servicios "push"		X				X					
Servicios de difusión o multidifusión					X						
Servicios de información	X	X				X					
Servicios de presencia y notificación general	X	X	X								

Cuadro II.1 – Correspondencia ilustrativa entre servicios y habilitadores de servicio

Servicios/Habilitadores de servicio	Presencia	Gestión de la ubicación	Gestión de grupo	Tratamiento de mensajes	Soporte de multidifusión	"Push"	Tratamiento de sesión	Gestión de información personal	Gestión de dispositivo	Soporte de aplicaciones web	Sincronización de datos
Versión 6 de 3GPP y versión A 3GPP2 de servicios basados en OSA	X	X	X	X	X	X	X				
Aplicaciones de recuperación de datos	X					X					
Servicios VPN			X		X						
Aplicaciones y servicios que utilizan identificación por etiquetas					X				X		
Servicios de vigilancia visual							X		X		
Servicios TVIP											
Servicios de empresa: servicio de línea arrendada virtual											
Servicios de empresa: aplicación de enlace empresarial											
Servicios de empresa: servicios propios para empresas											
Servicios de entrega gestionados											

Bibliografía

Los siguientes documentos contienen información que puede ser útil al lector de la presente Recomendación. En ellos se suministra información adicional acerca de tópicos que si bien son tratados en ella, no son básicos para entenderla.

Recomendaciones del UIT-T

[b-UIT-T E.351] Recomendación UIT-T E.351 (2000*), Encaminamiento de conexiones multimedios a través de redes con multiplexión por división en el tiempo, modo de transferencia asíncrono o basados en el protocolo Internet.*

[b-UIT-T F.703] Recomendación UIT-T F.703 (2000), *Servicios multimedios conversacionales.*

[b-UIT-T F.724] Recomendación UIT-T F.724 (2005), *Requisitos y descripción de los servicios de videotelefonía por las redes con protocolo Internet.*

[b-UIT-T F.733] Recomendación UIT-T F.733 (2005), *Requisitos y descripción del servicio de conferencia multimedia por las redes con protocolo Internet.*

[b-UIT-T F.741] Recomendación UIT-T F.741 (2005), *Descripción de servicio y requisitos de los servicios audiovisuales a la carta.*

[b-UIT-T F.742] Recomendación UIT-T F.742 (2005), *Descripción de servicio y requisitos para servicios de aprendizaje a distancia.*

[b-UIT-T F.790] Recomendación UIT-T F.790 (2007), *Directrices sobre accesibilidad para ancianos y discapacitados.*

[b-UIT-T Climate] Las TIC y el cambio climático, UIT-T, (2009), *Deliverable 2, Gap Analysis and Standards Roadmap*.

[b-UIT-T G.729A] Recomendación UIT-T G.729 Anexo A (1996), *Codificador de la voz mediante predicción lineal con excitación por código algebraico de estructura conjugada a 8 kbit/s de complejidad reducida.*

[b-UIT-T G.780] Recomendación UIT-T G.780/Y.1351 (2004), *Términos y definiciones para las redes de jerarquía digital síncrona.*

[b-UIT-T G.799.1] Recomendación UIT-T G.799.1/Y.1451.1 (2004), *Especificaciones de funcionalidad e interfaces para equipos de la red de transporte de la red telefónica general conmutada (RTGC) para la interconexión entre redes RTGC e IP.*

[b-UIT-T G.805] Recomendación UIT-T G.805 (2000), *Arquitectura funcional genérica de las redes de transporte.*

[b-UIT-T G.809] Recomendación UIT-T G.809 (2003), *Arquitectura funcional de las redes de capa sin conexión.*

[b-UIT-T G.1000] Recomendación UIT-T G.1000 (2001), *Calidad de servicio de las comunicaciones: Marco y definiciones.*

[b-UIT-T G.1010] Recomendación UIT-T G.1010 (2001*), Categorías de calidad de servicio para los usuarios de extremo de servicios multimedios.*

[b-UIT-T H.510] Recomendación UIT-T H.510 (2002), *Movilidad para sistemas y servicios multimedios H.323.*

[b-UIT-T H-Sup.1] Suplemento 1 a la serie H (1999), *Perfil de aplicación – Utilización de la comunicación en vídeo a baja velocidad binaria para la conversación en tiempo real mediante el lenguaje de signos y la lectura labial.*

[b-UIT-T I.230] Recomendación UIT-T I.230 (1988), *Definición de las categorías de servicios portadores.*

[b-UIT-T I.250] Recomendación UIT-T I.250 (1988), *Definición de servicios suplementarios.*

[b-UIT-T I.570] Recomendación UIT-T I.570 (1993), *Interfuncionamiento entre RDSI pública y privada.*

[b-UIT-T M.3017] Recomendación UIT-T M.3017 (2003), *Marco para la gestión integrada de redes híbridas de circuitos y paquetes.*

[b-UIT-T Q.833.1] Recomendación UIT-T Q.833.1 (2001), *Línea de abonado digital asimétrica – Gestión de elementos de red: Modelo de protocolo común de información de gestión.*

[b-UIT-T Q.1200] Recomendación UIT-T Q.1200 Series (1997), *Estructura general de la serie de Recomendaciones sobre la red inteligente.*

[b-UIT-T Q.1236] Recomendación UIT-T Q.1236 (1999), *Conjunto de capacidades 3 de red inteligente – Requisitos del modelo de información de gestión y metodología.*

[b-UIT-T Q.1702] Recomendación UIT-T Q.1702 (2002), *Visión a largo plazo de las características de las redes de sistemas posteriores a los sistemas de las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[b-UIT-T Q.1741.1] Recomendación UIT-T Q.1741.1 (2002), *Referencias de IMT-2000 a la publicación de 1999 del sistema global para comunicaciones móviles que ha evolucionado hacia la red medular del sistema de telecomunicaciones móviles universales con la red de acceso de la red terrenal de acceso radioeléctrico del sistema de telecomunicaciones móviles universales*.

[b-UIT-T Q.1741.2] Recomendación UIT-T Q.1741.2 (2002), *Referencias de las IMT-2000 a la versión 4 de la red medular del sistema de telecomunicaciones móviles universales derivada del sistema global para comunicaciones móviles con red terrenal de acceso radioeléctrico universal.*

[b-UIT-T Q.1741.3] Recomendación UIT-T Q.1741.3 (2003), *Referencias de las IMT-2000 a la versión 5 de la red medular del sistema de telecomunicaciones móviles universales derivada del sistema global para comunicaciones móviles.*

[b-UIT-T Q.1741.4] Recomendación UIT-T Q.1741.4 (2005), *Referencias de las IMT-2000 a la versión 6 de la red medular del sistema de telecomunicaciones móviles universales derivada del sistema global para comunicaciones móviles.*

[b-UIT-T Q.1742.4] Recomendación UIT-T Q.1742.4 (2005), *Referencias IMT-2000 (aprobadas el 30 de junio de 2004) a la red medular desarrollada ANSI-41 con red de acceso cdma2000.*

[b-UIT-T Q.1761] Recomendación UIT-T Q.1761 (2004), *Principios y requisitos para la convergencia de los sistemas fijos y los sistemas IMT-2000 existentes.*

[b-UIT-T T.140] Recomendación UIT-T T.140 (1998), *Protocolo de conversación mediante texto para aplicaciones multimedios.*

[b-UIT-T X.501] Recomendación UIT-T X.501 (2008) | ISO/CEI 9594-2:2008, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos.*

[b-UIT-T X.509] Recomendación UIT-T X.509 (2008) | ISO/CEI 9594-8:2008, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

[b-UIT-T X.511] Recomendación UIT-T X.511 (2008) | ISO/CEI 9594-3:2008, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Definición de servicio abstracto.*

[b-UIT-T X.1244] Recomendación UIT-T X.1244 (2008), *Aspectos globales para contrarrestar el correo basura en las aplicaciones multimedios en las redes IP.*

[b-UIT-T Y.1411] Recomendación UIT-T Y.1411 (2003), *Interfuncionamiento de redes con conmutación por etiquetas multiprotocolo y modo de transferencia asíncrono – Interfuncionamiento en el plano de usuario en modo célula.*

[b-UIT-T Y.2052] Recomendación UIT-T Y.2052 (2008), *Marco para el multidireccionamiento en las NGN IPv6.*

[b-UIT-T Y.2053] Recomendación UIT-T Y.2053 (2008), *Requisitos funcionales para la transición a IPv6 de las NGN.*

[b-UIT-T Y.2054] Recomendación UIT-T Y.2054 (2008), *Marco para el soporte de la señalización en las NGN IPv6.*

[b-UIT-T Y-Sup.1] Recomendaciones UIT-T de la serie Y.2000 Suplemento 1 (2006), *Alcance de la versión 1 de las NGN.*

[b-UIT-T Y-Sup.5] Recomendaciones UIT-T de la serie Y.1900 – *Suplemento sobre casos de uso del servicio TVIP (2008)*.

[b-UIT-T Y-Sup.7] Recomendaciones UIT-T de la serie Y Suplemento 7 (2008), *Alcance de la versión 2 de las NGN.*

[b-UIT-R M.1645] Recomendación UIT-R M.1645 (2003*), Marco y objetivos generales del desarrollo futuro de los sistemas IMT-2000 y de los sistemas posteriores.*

Directrices del UIT-T

[b-UIT-T Accessibility] Documento técnico del UIT-T (2006), *FSTP-TACL Telecommunications Accessibility Checklist.*

Especificaciones técnicas del ETSI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

American National Standards Institute (ANSI) standards

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

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

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

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

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

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

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

IETF specifications

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

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

Open Mobile Alliance specifications

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

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

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

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

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

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

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

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

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

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

Open Service Access (OSA)

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

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

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

IN services

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

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

UDDI specifications

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

SOA specifications

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

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, 2010