

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2201

(04/2007)

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 de las redes de la próxima generación, versión 1

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
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
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899

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

Requisitos de las redes de la próxima generación, versión 1

Resumen

En esta 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*), versión 1.

Orígenes

La Recomendación UIT-T Y.2201 fue aprobada el 27 de abril de 2007 por la Comisión de Estudio 13 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

Palabras clave

Autenticación, autorización, capacidades, contabilidad, denominación, direccionamiento, emulación RTPC/RDSI, entorno de servicio abierto, facilitador de servicios, gestión, identificación, interfuncionamiento, interoperabilidad, movilidad, numeración, OAM, perfil, política, privacidad, QoS, requisitos de capacidades, seguridad, simulación RTPC/RDSI, tasación, versión 1 de las NGN.

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/>.

© UIT 2008

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

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones.....	3
3.1 Términos definidos en otro sitio.....	3
3.2 Términos definidos en la presente Recomendación	5
4 Siglas y acrónimos	5
5 Convenios	7
6 Requisitos de capacidad, versión 1 de las NGN	7
6.1 Conectividad de transporte	7
6.2 Modos de comunicación.....	7
6.3 Gestión de recursos de medios	8
6.4 Códex	8
6.5 Red de acceso y conexión de red.....	9
6.6 Redes de usuario.....	9
6.7 Interconexión, interoperabilidad e interfuncionamiento	10
6.8 Encaminamiento	12
6.9 Calidad de servicio	12
6.10 Contabilidad y tasación	14
6.11 Numeración, denominación y direccionamiento.....	14
6.12 Identificación, autenticación y autorización.....	16
6.13 Seguridad.....	20
6.14 Gestión de la movilidad.....	20
6.15 OAM.....	21
6.16 Supervivencia	23
6.17 Gestión.....	24
6.18 Entorno de servicio abierto.....	25
6.19 Gestión de perfil	29
6.20 Gestión de políticas	30
6.21 Activadores de servicio	31
6.22 Emulación y simulación RTPC/RDSI.....	37
6.23 Asuntos de interés público.....	38
6.24 Protección de infraestructuras clave.....	41
6.25 Confidencialidad de la información en las interfaces.....	41
6.26 Intercambio entre proveedores de información relativa al usuario	41
Apéndice I – Correspondencia entre servicios y habilitadores de servicio.....	42
Bibliografía	43

Recomendación UIT-T Y.2201

Requisitos de las redes de la próxima generación, versión 1

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 versión 1 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 la versión 1 de las NGN conforme a [b-ITU-T Y-Sup.1]. Las NGN tendrán que prestar por lo menos un nivel de servicio que ofrezca capacidades similares a las suministradas por las redes con conmutación de circuitos o mejores que ellas.

No pretende esta Recomendación indicar requisitos más detallados ni requisitos específicos de determinado tipo de servicio. Si bien los requisitos aplicables a los equipos de usuario están fuera del alcance de este documento, los correspondientes a los acuerdos de acceso sí se tratan en él.

Se acepta que es posible que una determinada NGN esté constituida por un conjunto (o superconjunto) arbitrario de servicios conformes a la versión 1 de las NGN, y por capacidades especificadas en esta Recomendación.

Es probable que las administraciones conminen a los operadores y proveedores de servicios a conformarse a sus marcos reglamentarios y políticos nacionales al aplicar esta Recomendación.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

- [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 (2004), *Plan de identificación internacional para terminales y usuarios de servicios móviles.*
- [UIT-T G.711] Recomendación UIT-T G.711 (1988), *Modulación por impulsos codificados (MIC) de frecuencias vocales.*
- [UIT-T G.780] Recomendación UIT-T G.780/Y.1351 (2004), *Términos y definiciones para las redes de jerarquía digital síncrona.*
- [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 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 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.*
- [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.*
- [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.*
- [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.*
- [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.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.*
- [UIT-T Y.2091] Recomendación UIT-T Y.2091 (2007), *Términos y definiciones aplicables a las redes de la próxima generación.*
- [UIT-T Y.2701] Recomendación UIT-T Y.2701 (2007), *Requisitos de seguridad de la red de próxima generación.*
- [UIT-T Z.100] Recomendación UIT-T Z.100 (2002), *Lenguaje de especificación y descripción.*

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).

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 Abonado.

3.1.9 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.

3.1.10 red propia [UIT-T E.212]: La red asociada con el operador o el proveedor de servicio al que está abonado el usuario.

3.1.11 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).

3.1.12 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.

3.1.13 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.

3.1.14 gestión de la movilidad [UIT-T Q.1706]: Conjunto de funciones que se utilizan para permitir la movilidad.

NOTA – 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.

3.1.15 nomadismo [UIT-T Q.1706]: Capacidad del usuario para cambiar su punto de acceso a la red después de haberse desplazado; 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.

3.1.16 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.

3.1.17 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.

3.1.18 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.

3.1.19 servicio [UIT-T Z.100]: Conjunto de funciones y facilidades ofrecido a un usuario por un proveedor.

3.1.20 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.

3.1.21 abonado [UIT-T M.3050.1]: Persona u organización responsable de la firma de contratos para los servicios suscritos y del pago de dichos servicios.

3.1.22 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.

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

3.1.24 red visitada [UIT-T Q.1706]: Red local en caso de itinerancia.

3.2 Términos definidos en la presente Recomendación

La presente Recomendación define los términos siguientes.

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

3.2.2 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.

3.2.3 señalización de prioridad: Parte del mecanismo de activación de la prioridad que utiliza señalización.

3.2.4 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.

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

3.2.6 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.

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

3.2.8 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:

ANI	Interfaz aplicación-red (<i>application network interface</i>)
API	Interfaz de programación de aplicaciones (<i>application programming interface</i>)
ATM	Modo de transferencia asíncrono (<i>asynchronous transfer mode</i>)
B2B	De empresa a empresa (<i>business to business</i>)
CC	Contenido de la comunicación (<i>content of communication</i>)
CD/DVD	Disco compacto/disco vídeo digital (<i>compact disk/digital versatile disk</i>)
DNS	Sistema de nombres de dominio (<i>domain name system</i>)
DTMF	Multifrecuencia bitono (<i>dual tone multi frequency</i>)
ENUM	Correspondencia de números telefónicos (<i>telephone number mapping</i>)
ETS	Servicio de telecomunicaciones de emergencia (<i>emergency telecommunications services</i>)

IEPS	Plan internacional de preferencias en situaciones de emergencia (<i>international emergency preference scheme</i>)
IM	Mensajería instantánea (<i>instant messaging</i>)
IMS	Subsistema multimedios IP (<i>IP multimedia subsystem</i>)
IN (o RI)	Red inteligente (<i>intelligent network</i>)
IP	Protocolo internet (<i>internet protocol</i>)
IP-CAN	Red de acceso de conectividad IP (<i>IP connectivity access network</i>)
IPv4	Versión 4 del IP (<i>internet protocol version 4</i>)
IPv6	Versión 6 del IP (<i>internet protocol version 6</i>)
IRI	Información relativa a la interceptación (<i>intercept related information</i>)
IT	Tecnología de la información (<i>information technology</i>)
LEA	Organismos encargados de hacer cumplir la ley (<i>law enforcement agencies</i>)
MMS	Servicio de mensajería multimedia (<i>multimedia messaging service</i>)
MPLS	Conmutación por etiquetas multiprotocolo (<i>multi-protocol label switching</i>)
NAI	Identificador de acceso de red (<i>network access identifier</i>)
NAPT	Traducción de puerto de direcciones de red (<i>network address port translation</i>)
NAT	Traducción de dirección de red (<i>network address translation</i>)
NGN	Redes de próxima generación (<i>next generation network</i>)
NNI	Interfaz red-red (<i>network-network interface</i>)
OAM	Operaciones, administración, mantenimiento (<i>operations, administration and maintenance</i>)
OS	Sistema operativo (<i>operating system</i>)
OSA	Acceso de servicio abierto (<i>open service access</i>)
OTN	Red óptica de transporte (<i>optical transport network</i>)
QoS	Calidad de servicio (<i>quality of service</i>)
PBX	Centralita privada (<i>private branch exchange</i>)
PC	Computador personal (<i>personal computer</i>)
PDA	Agenda digital (<i>personal digital assistant</i>)
POTS	Servicio telefónico tradicional (<i>plain old telephone service</i>)
RMTP	Red móvil terrestre pública
RACF	Funciones de control de recursos y admisión (<i>resource and admission control functions</i>)
RDSI	Red digital de servicios integrados
RTPC	Red telefónica pública conmutada
SIP	Protocolo de iniciación de sesión (<i>session initiation protocol</i>)
SLA	Acuerdo de nivel de servicio (<i>service level agreement</i>)
SMS	Servicio de mensajes cortos (<i>short message service</i>)
SR	Resiliencia de servicio (<i>service resiliency</i>)

TDR	Servicio de telecomunicaciones de socorro (<i>telecommunications for disaster relief</i>)
TE	Equipo terminal (<i>terminal equipment</i>)
UDDI	Descubrimiento, descripción e integración universales (<i>universal discovery, description and integration</i>)
UMTS	Sistema de telecomunicaciones móviles universales (<i>universal mobile telecommunications system</i>)
UNI	Interfaz usuario-red (<i>user to network interface</i>)
URI	Identificador de recurso unificado (<i>uniform resource identifier</i>)
VPN	Red privada virtual (<i>virtual private network</i>)
xDSL	Diversos tipos de línea digital de abonado (<i>digital subscriber line</i>)

5 Convenios

Ninguno.

6 Requisitos de capacidad, versión 1 de las NGN

En esta cláusula se describen los requisitos principales y las capacidades correspondientes necesarios para garantizar los objetivos de servicio de la versión 1 de las NGN [b-UIT-T Y-Sup.1].

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.

No pretende esta Recomendación indicar requisitos más detallados ni requisitos específicos de servicio.

En esta Recomendación sólo se tratan las capacidades de red necesarias para las NGN. Si bien los requisitos aplicables a los equipos de usuario están fuera del alcance de este documento, los correspondientes a los acuerdos de acceso sí se tratan en él.

6.1 Conectividad de transporte

El estrato de transporte NGN, versión 1 [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 (p. ej., 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 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 son:

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

6.4 Códecs

Los requisitos generales que han de cumplir los códecs son:

- 1) Siempre que sea posible, se debería 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 (p. ej., 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.

NOTA 1 – Conviene que el equipo de usuario NGN utilice un códec de audio de banda ancha.

- 3) Con el fin de facilitar el interfuncionamiento entre las NGN y otras redes (incluidas las RTPC/RDSI, RMTP y otras NGN), las NGN tendrán la capacidad de aceptar y presentar voz codificada conforme a G.711 [UIT-T G.711] cuando se conecten con otra red.
- 4) 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 debería emplear un tamaño de empaquetado de voz de muestras de 10 ms para la voz G.711 [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 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 2 – Cuando se escoge un tamaño de empaquetado por negociación de códec entre terminales y/o elementos de red, el presente documento no impone ningún requisito al valor seleccionado.

NOTA 3 – En los casos en los que la negociación extremo a extremo no resulte en una selección de códec, se puede utilizar la transcodificación. Por ejemplo, las pasarelas residenciales o las domésticas ubicadas en los locales del cliente, o las pasarelas de acceso, de medios o de interconexión de red, podrían efectuarla, dependiendo de la configuración de comunicación.

NOTA 4 – Los requisitos mencionados no obligan a los terminales a soportar ningún códec, ni tampoco a que las NGN soporten la transcodificación entre un códec de audio (cualquiera que sea), y la G.711 [UIT-T G.711].

6.5 Red de acceso y conexión de red

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

- 1) Las NGN soportarán varias tecnologías de función de transporte de acceso.
- 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.
- 4) 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.
- 5) El perfil de usuario contendrá información de autenticación de acceso e información relacionada con la configuración de acceso de red requerida.
- 6) 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. Es posible que los servicios dependan de uno o varios de los siguientes factores: el dispositivo de usuario, la red de acceso y los acuerdos (p. ej., 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.
- 7) 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.
- 8) 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 (p. ej., el mecanismo de identificador de conexión de red (NAI, *network attachment identifier*) especificado en [b-RFC2486]).

6.6 Redes de usuario

A continuación se enumeran los requisitos generales para el acceso a las 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 NGN.
 - Con conectividad indirecta e interacción entre los terminales y la NGN (p. ej., mediante PBX IP).

Aunque en la versión 1 de las NGN se debería permitir la utilización simultánea de varios tipos de funciones de transporte de acceso por parte de un solo terminal, 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.

6.7 Interconexión, interoperabilidad e interfuncionamiento

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

6.7.1 Interconexión

Se conocen dos tipos de interconexión entre las NGN, versión 1, 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 G.711 en una interconexión IP. Los niveles de interoperabilidad definidos son función del servicio, de la QoS, de la seguridad, etc.

Los requisitos para la interconexión son:

- 1) Se ha de soportar el tipo de interconexión orientada a la conectividad entre las NGN.
- 2) No se prohíbe la utilización del tipo de interconexión orientada al servicio entre las NGN.

6.7.2 Interoperabilidad

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 interoperar entre ellos.
- 2) No se prohíbe la interoperabilidad de NGN interconectadas que posean conjuntos idénticos de capacidades de servicio.

6.7.3 Interfuncionamiento con redes que no son NGN

Con el fin de poder prestar ciertos servicios, las NGN de la versión 1 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.
- Las NGN deberían tener 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 (p. ej., 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).

6.7.3.1 Interfuncionamiento con RTPC/RDSI

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

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

6.7.3.2 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 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 6.7.3, 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 6.13 se describen los requisitos de seguridad para este caso.

6.8 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.

6.9 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. 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.

6.9.1 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 (p. ej., abonamiento/configuración, invocación, supervisión).
- 3) Aceptar diferentes capacidades de los CPE (p. ej., 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.
- 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.

- 7) Admitir requisitos de QoS orientados a la aplicación.

6.9.2 Clases de QoS de red

- 1) Las NGN deberían tener en cuenta la calidad de funcionamiento de red en el estrato de transporte.
- 2) Las NGN deberían soportar clases de QoS NGN basadas en [UIT-T Y.1541].

6.9.3 Prioridad de servicio o de aplicación

Las NGN deberían tener 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 y la NNI.
- 3) Mecanismos de activación de prioridad que ejecuten la acción de prioridad deseada.

6.9.4 Control de QoS

Las NGN deberían soportar:

- 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, ha de ser 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.

6.9.5 Señalización de QoS

Las NGN deberían utilizar 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.

6.9.6 Medición y gestión de la calidad de funcionamiento

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

Las mediciones de la calidad de funcionamiento y su gestión admitirán:

- 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, p. ej., 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.

6.9.7 Gestión de sobrecarga 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, la versión 1 de las NGN proveerá 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.

Las NGN dispondrán de mecanismos de control de sobrecarga que:

- 1) Indiquen a otras redes las condiciones y el grado de sobrecarga.
- 2) Optimicen el caudal efectivo (p. ej., 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.

6.10 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 (p. ej., 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 (p. ej., 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.

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.

6.11 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.

6.11.1 Requisitos generales para la numeración, la denominación y el direccionamiento

- 1) Se admitirán los modos de atribución de direcciones dinámico y fijo.
- 2) Las capacidades de numeración, denominación y direccionamiento se podrán 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 varias capas pueden cambiar dinámicamente dependiendo de la ubicación del terminal).

6.11.2 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 E.164 (números mundiales).
- 4) Las NGN deberían aceptar numeración que no sea E.164 (números locales).
- 5) Las NGN deberían aceptar números cortos en los planes nacionales de marcación.
- 6) Las NGN deberían aceptar la numeración privada y empresarial (véase la cláusula 6.6).
- 7) Cuando se empleen números que no son 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 distinguirán entre los números telefónicos y los identificadores alfanuméricos que sólo tengan números, y como tales los considerará a los efectos del encaminamiento.

6.11.3 Esquemas de numeración, denominación y direccionamiento

- 1) En el estrato de transporte, las NGN aceptarán esquemas de direccionamiento IP basados en el IPv4, el IPv6 o en ambos.
NOTA 1 – Conviene 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 operadores NGN pueden 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 E.164 (URI Tel, *telephone uniform resource identifiers*), p. ej., tel:+4412345678, y los identificadores uniformes de recursos SIP (URI SIP), p. ej., sip:my.name@company.org. Para el caso de los URI Tel:
 - se aceptarán los números mundiales;
 - se deberían aceptar los números locales.

- 4) En algunas situaciones de servicio, p. ej., 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 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.

6.11.4 Resolución de nombre o dirección

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: las NGN deberían ser 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 emplear bases de datos internas o externas a la NGN (p. ej., una base de datos del DNS de Internet). 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.

6.11.5 Interfuncionamiento de numeración, denominación y direccionamiento

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, sin que ello afecte al 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, sin que ello afecte el servicio prestado a los usuarios.

6.12 Identificación, autenticación y autorización

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

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

6.12.1 Requisitos generales

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 1 – Algunas veces se ha empleado la expresión "proveedor de servicio" para referirse al proveedor de servicios del estrato de transporte. En esta subcláusula, 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) Deberían procesarse 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 serán visibles para los otros usuarios siempre que no participen intermediarios.
- 16) Un proveedor de servicio puede 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 sólo procedimiento de abonado.
- 18) Puede ser posible emplear una sola autenticación y autorización de usuario para varios servicios (firma única).

NOTA 2 – 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 la versión 1 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 de la versión 1.

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

6.12.2 Requisitos de identificación

En la versión 1 de 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 (p. ej., para los procedimientos de autenticación y autorización).

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 (p. ej., 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 debería 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 (p. ej., 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 asociar con una entidad de usuario.
- 5) **Soporte de condiciones de atributo**
Un proveedor de atributo (p. ej., red, usuario principal, usuario extremo) puede asociar a la identidad de usuario las condiciones (p. ej., 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 (p. ej., la validez de la identidad).

- 7) Soporte de la programación de abonado
Las NGN soportarán la programación por parte del abonado de varios permisos para diferente información de atributo, p. ej., 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 (p. ej., terminal en el punto de venta).

6.12.3 Requisitos de autenticación

La autenticación 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 autenticación de red y autenticación de servicio. Para un usuario, por su parte, una NGN puede distinguir entre autenticación de usuario y de equipo terminal. La autenticación 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 autenticación 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 autenticar 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 autenticar e identificar un proveedor de servicio.

La NGN debe asegurar 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 autenticación.

Los requisitos que debe cumplir la capacidad de autenticación son:

- 1) Las NGN admitirán la utilización de varios mecanismos de autenticación de red, conforme a las tecnologías subyacentes de red de acceso.
- 2) La autenticación de servicio debería ser independiente de la tecnología de red de acceso NGN y mantener un mecanismo coherente de autenticación de servicio.
- 3) Las NGN podrán solicitar al usuario o al equipo terminal que suministren información de autenticación, de manera explícita o implícita.
- 4) Las NGN deberían admitir mecanismos de autenticación basados en soporte lógico físico.
- 5) Se aceptará la autenticación de equipo terminal mediante información de perfil de dispositivo.
- 6) Las NGN deberían proveer capacidades de autenticación mutua entre el proveedor de servicio y el usuario.
- 7) Una red NGN debe proveer capacidades de autenticación recíproca entre el proveedor de red de transporte y el usuario.

6.12.4 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) La autorización de servicio debería ser independiente de las tecnologías de red de acceso NGN.
- 3) La capacidad de autorización debería soportar los casos de movilidad especificados en la versión 1 de las NGN, cuando corresponda.

6.13 Seguridad

La versión 1 de las NGN incluirá 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, p. ej., 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 la cantidad de ataques de la red, desde el exterior o desde el interior.
- 10) Protección contra la cibercriminalidad permitiendo al utilizador de identificar al proveedor de la red de transporte y al proveedor de servicio.

6.14 Gestión de la movilidad

La gestión de la movilidad incluye la capacidad que tienen los entes móviles, p. ej., los usuarios, los terminales y las redes, de pasar de una red a otra (itinerancia), sean estas últimas NGN o no. En la versión 1 de las NGN, se tratan dos tipos de movilidad, a saber la movilidad personal y la de terminal [UIT-T Q.1706].

En dicha versión 1, 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 la versión 1 de 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 de la versión 1 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, la versión 1 deberá:

- 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.

6.15 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].

La versión 1 de 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 – Las capacidades OAM de que trata esta subcláusula son complementarias con las descritas en la cláusula 6.17.

6.15.1 Requisitos generales de OAM

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, p. ej., 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 (p. ej., 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. Las redes de capa de cliente deberían soportar 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 6.7.3).
- 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 – 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.

6.16 Supervivencia

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

6.16.1 Requisitos de 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) Habrá conmutación de protección 1+1 y 1: n.
- 4) Se podrán emplear los recursos de protección de transporte no utilizados para transportar tráfico sin garantías.
- 5) Se deberían minimizar los efectos sobre la calidad de funcionamiento de red (p. ej., 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.

6.16.2 Requisitos de 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 tendrán 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 deberían minimizar los efectos sobre la calidad de funcionamiento de red (p. ej., 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.

6.16.3 Requisitos de 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.

6.17 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 (p. ej., 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 (p. ej., 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 (p. ej., 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 también los requisitos de la subcláusula 6.10, "Contabilidad y tasación".

6.18 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 deberían 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 portables o reutilizables a través de las redes.
- Las ANI abiertas y normalizadas permitirán interacciones entre entidades y aplicaciones NGN (p. ej., 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 (p. ej., un tercero), todas las funciones de servicio que le correspondan. Es posible 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 6.13.

En las siguientes subcláusulas se especifican las capacidades del entorno abierto de servicio.

6.18.1 Coordinación de servicio

Los requisitos que debe cumplir la coordinación de servicio en el entorno abierto de servicio son:

- 1) Las NGN ofrecerán la coordinación de las aplicaciones y servicios con las capacidades.
- 2) Se debería guardar registro de las capacidades o componentes de servicio NGN de varios proveedores de servicio, y la relación entre dichas capacidades o componentes de servicio.
- 3) Se debería suministrar a las aplicaciones y a los servicios información sobre los cambios de estado de capacidades o componentes de servicio (debidos, por ejemplo, a actualizaciones).

6.18.2 Interfuncionamiento con entornos de creación de servicio

- 1) El entorno abierto de servicio NGN permitirá el interfuncionamiento entre entornos de creación de servicio y entidades de red, con miras a crear y configurar aplicaciones y servicios.
- 2) La versión 1 de las NGN debería soportar las 3 clases siguientes de entornos de creación de servicio:
 - entorno abierto de creación de servicio; ejemplos de esta clase de entorno, que utiliza las ANI: OSA/Parlay, Parlay X, y OMA;
 - entorno de creación de servicio basado en el subsistema multimedios IP (IMS, *IP multimedia subsystem*) [UIT-T Q.1741.x];
 - entorno de creación de servicio basado en redes inteligentes (IN, *intelligent network*): algunos ejemplos de protocolos de interfaz que vienen al caso para esta clase de entorno son el protocolo de aplicación IN (INAP, *IN application protocol*), las aplicaciones personalizadas de la lógica mejorada de red móvil (CAMEL, *customized application for mobile network enhanced logic*) y la red inteligente inalámbrica (WIN, *wireless intelligent network*).

6.18.3 Descubrimiento de servicio

Éste suele ser el primer paso cuando se desea ubicar capacidades, y/o servicios y aplicaciones. Contar con una capacidad de descubrimiento de servicio es esencial en muchos casos, por ejemplo en los de movilidad (con el fin de ubicar los servicios en una red visitada) y en el de acceso a servicios independiente del dispositivo de usuario.

Así, por ejemplo, cuando se implementa esta capacidad en servicios web, se pueden emplear los registros públicos de servicios web (p. ej., el registro universal de descubrimiento, descripción e integración (UDDI, *universal discovery, description and integration*)) para implementar el descubrimiento de servicio y permitir el acceso a los servicios.

Los requisitos para el descubrimiento de servicio son:

- 1) Las NGN soportarán una capacidad de descubrimiento de servicio que permita a los usuarios y sus dispositivos descubrir los servicios que les interesen, con cualquier tecnología de red subyacente.
- 2) Los mecanismos de descubrimiento de servicio serán independientes de la tecnología de red subyacente, permitiendo así la utilización de tecnologías de red heterogéneas y en constante evolución.
- 3) La capacidad de descubrimiento de servicio permitirá a los usuarios descubrir los servicios que puedan ser de interés para ellos y otros que lo sean para los dispositivos:
 - Los servicios de interés para los usuarios pueden ser utilizados directamente por éstos. Son ejemplos los servicios de directorio, los de traducción y los de facilidades compartidas (p. ej., de información de ayuda relativa a las TI).
 - Los servicios de interés para los dispositivos son aquellos a los que pueden acceder directamente los dispositivos (p. ej., microteléfonos móviles o PC portátiles). Por ejemplo, las impresoras, los dispositivos de salvaguarda de información, los grabadores CD/DVD, los servidores de autenticación y los servidores de atribución de dirección IP. Es posible que estos servicios y la información de red no puedan ser utilizados directamente por personas.
- 4) Los mecanismos de descubrimiento de servicio no deberían limitarse a las tecnologías tradicionales basadas en el modelo cliente-servidor.

NOTA – Pueden también implementarse cuando se emplean tecnologías par-par o una combinación de tecnologías cliente-servidor y par-par.

- 5) La capacidad de descubrimiento de servicio debería soportar varios criterios de determinación de alcance (p. ej., ubicación y costo) con el fin de lograr la adecuada utilización de escalas.
- 6) La capacidad de descubrimiento de servicio debería soportar los mecanismos apropiados para garantizar la seguridad y preservar la privacidad.
- 7) La capacidad de descubrimiento de servicio se utilizará teniendo en cuenta la escalabilidad (p. ej., conviene evitar los mecanismos de difusión).

6.18.4 Registro de servicio

Esta capacidad permite el registro de otras capacidades, servicios y aplicaciones, en directorios del entorno abierto de servicio que sean accesibles a ellos. Así, por ejemplo, se puede poner en funcionamiento la capacidad de registro en los servicios web cuando se desee hacer propaganda a un servicio web: se pueden inscribir en "registros" públicos de servicios web (es decir, directorios especiales en los que los usuarios no sólo encuentran recursos, sino que también pueden inscribir servicios).

El requisito para el registro de servicio es:

- 1) El entorno abierto de servicio proveerá los medios para gestionar el registro de capacidades, servicios y aplicaciones. Se escogerá una tecnología que garantice las funciones necesarias para el registro de servicios y su anulación, incluidas las de configuración, activación y publicación.

6.18.5 Soporte de desarrollo

Éste es un aspecto clave de la cadena de prestación de servicio, ya sea que se trate del proveedor de servicios o de terceros que estén facultados para mejorar el conjunto de capacidades y ampliar la oferta general de servicios. Quienes desarrollan aplicaciones han de contar con la adecuada recolección y publicación de la información, además de disponer de medios para coordinar y especificar sus necesidades, e identificar las interfaces a los efectos del desarrollo.

Las NGN suministrarán un soporte eficiente de desarrollo para:

- 1) La construcción de aplicaciones.
- 2) La prueba de aplicaciones (p. ej., rastreo y depuración).
- 3) La puesta en funcionamiento de aplicaciones.
- 4) La supresión de aplicaciones.

El soporte de desarrollo debería incluir:

- 1) La reutilización e intercambiabilidad de componentes (de *software*).
- 2) La capacidad de mezclar y hacer corresponder componentes, a través de la gestión de interfaces y contando con una semántica coherente de datos/esquema compartidos en dichos componentes.
- 3) La capacidad de abarcar toda la vida útil de los componentes, desde la instalación, pasando por la configuración, la administración, la publicación, la creación de versiones y el mantenimiento, hasta la supresión.
- 4) Admitir el diseño de aplicaciones independientes de su utilización final, con el fin de que puedan servir sin que haya que rediseñarlas para cada caso particular.
- 5) La identificación de la dependencia entre componentes.

6.19 Gestión de perfil

6.19.1 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, o en bases de datos coubicadas.

Los requisitos generales del perfil de usuario son:

- 1) Habrá un perfil de usuario para cada usuario, que podrá estar formado por varios "componentes".
- 2) Dichos componentes pueden 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 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. Dichos requisitos deberían abarcar los siguientes aspectos.

6.19.2 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 contienen 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, o en bases de datos coubicadas.

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 podrá estar formado por varios "componentes".
- 2) Dichos componentes pueden estar distribuidos en la red local y en el entorno de terceros proveedores de servicio.
- 3) Dentro de la red local, los componentes pueden 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 deberán 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 usuario, 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. Dichos requisitos deberían abarcar los siguientes aspectos.

6.20 Gestión de políticas

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

- 1) Garantizar la coherencia de servicio a través de una variedad de tecnologías 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 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 capacidades, como las de contabilidad y de tasación.

- 4) Lograr que los servicios y las aplicaciones sean independientes de los intrincados detalles de implementación 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 6.9), como parte del conjunto general de capacidades de gestión de política.

Los requisitos generales de gestión de política para la versión 1 de 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.

6.21 Activadores de servicio

La categoría de "activadores 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.

6.21.1 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 deberían protegerse con relación a los otros usuarios. Las NGN deberían gestionar este tipo de grupos y proporcionar 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.

6.21.2 Gestión de la 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 (p. ej., según las redes de acceso disponibles), de preferencias de medios, especificada por el usuario, etc. Esta información es suministrada por las aplicaciones (p. ej., 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.

Debería protegerse la información gestionada por esta capacidad. Conviene proveer soporte para los diferentes contextos de comunicación, a los efectos de permitir la movilidad.

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

- 1) Se puede 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) La capacidad de gestión de la información personal debería soportar diferentes contextos de comunicación.

6.21.3 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 (p. ej., el aislamiento de grandes volúmenes de telecomunicación no solicitada).

6.21.4 Soporte de la multidifusión

Estas capacidades permiten a las aplicaciones suministrar contenidos a varios usuarios simultáneamente, empleando mecanismos de multidifusión.

Con el fin de utilizar eficientemente los recursos de red, además de la unidifusión se deberían soportar mecanismos de multidifusión.

A los efectos de prestar servicios de difusión/multidifusión, tanto el estrato de transporte como el de servicio deberían proveer las capacidades correspondientes.

Los requisitos generales son:

- 1) Las NGN deberían soportar capacidades de multidifusión para poder entregar la información de una manera eficiente y escalable.
- 2) Las NGN deberían ofrecer capacidades para realizar servicios de difusión/multidifusión en una sola NGN o entre varias.

6.21.5 Información de 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 (p. ej., 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 -p. ej., 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-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, p. ej., 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.

Distribución de información de presencia:

- 3) Las NGN proveerán una capacidad para habilitar una entidad, p. ej., 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.

Gestión de información de presencia:

- 4) Las NGN tendrán gestión de presencia, el conjunto de capacidades necesarias para gestionar la información de presencia recolectada.
- 5) 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.
- 6) 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.
- 7) 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, p. ej., para aceptar o rechazar peticiones según de cuál observador provengan.

6.21.6 Gestión de la ubicación

Capacidad que permite prestar servicios y aplicaciones basados en la ubicación de los usuarios y en la de los dispositivos en la red. Si se trata de la posición física real, se 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 debería implementarse 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.

6.21.7 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, p. ej., 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 requiere el acuerdo del usuario.

6.21.8 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 suministrar funciones de registro, gestión y actualización de información de dispositivo.
- 5) La gestión de dispositivo puede 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.

6.21.9 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 (p. ej., 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.
- 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 varios tipos de servicios (p. ej., voz, texto y vídeo).
- 6) Si hay uno o dos participantes en la sesión, la red terminará la sesión en cualquier momento a petición de cualquiera de los usuarios de la sesión. La red puede terminar por sí misma una sesión en cualquier momento de ésta (p. ej., en condiciones de fallo).
- 7) Si hay más de dos participantes en la sesión la red puede terminar la sesión en cualquier momento a petición de cualquiera de los usuarios de la sesión. La red puede terminar por sí misma una sesión en cualquier momento de ésta (p. ej., en condiciones de fallo).

6.21.10 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 entorno 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.

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

- 5) La reutilización de las tecnologías existentes y de los componentes NGN (p. ej., 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 la versión 1 de las NGN sea limitada en lo que tiene que ver con las capacidades de soporte de aplicaciones basadas en la web.

6.21.11 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.

Las NGN soportarán 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) La capacidad de sincronización de datos debería conocer las limitaciones de recursos de los terminales.

6.22 Emulación y simulación 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 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.

6.22.1 Requisitos de emulación RTPC/RDSI

6.22.1.1 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.

6.22.1.2 Requisitos de terminal para la emulación RTPC/RDSI

Las NGN soportarán los terminales tradicionales (p. ej., teléfonos RTPC, teléfonos de texto, telefaxes y otros tipos existentes de terminales RTPC/RDSI) que no están 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.

6.22.1.3 Requisitos de servicio para la emulación RTPC/RDSI

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.

6.22.2 Requisitos de simulación RTPC/RDSI

6.22.2.1 Requisitos generales para la simulación RTPC/RDSI

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

6.22.2.2 Requisitos de terminal para la simulación RTPC/RDSI

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

6.22.2.3 Requisitos de servicio para la simulación RTPC/RDSI

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) Las NGN deberían permitir 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.

6.23 Asuntos de 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 cuentan los que se describen en las subcláusulas siguientes.

6.23.1 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.

6.23.2 Identificación de comunicaciones malintencionadas

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

6.23.3 Grandes volúmenes de comunicaciones no solicitados

Las NGN dispondrán de las capacidades necesarias para impedir este tipo de comunicaciones.

6.23.4 Telecomunicaciones de emergencia

Las telecomunicaciones de emergencia (incluido el soporte de la advertencia temprana) son:

- Las telecomunicaciones de una persona hacia la autoridad, p. ej., llamadas a los proveedores de servicios de emergencia.
- Las telecomunicaciones de una autoridad hacia otra, p. ej., el servicio de telecomunicaciones de socorro (TDR, *telecommunications for disaster relief*).
- Las telecomunicaciones de una autoridad hacia las personas, p. ej., 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, p. ej., 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 (p. ej., entre las redes de acceso y troncal, y entre los estratos de servicio y de transporte) y entre las NGN propiamente dichas (p. ej., 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 (p. ej., 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 (p. ej., 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.

6.23.5 Presentación y privacidad de la identidad de usuario

- 1) Las NGN podrán presentar la identidad de la parte que origina.
- 2) Las NGN podrán presentar la identidad de la parte que termina.
- 3) Las NGN podrán suprimir la presentación de la identidad de la parte que origina.
- 4) Las NGN podrán 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.

6.23.6 Selección de proveedor de red o de servicio

Las NGN soportarán la capacidad de selección de proveedor, cuando así se requiera (p. ej., por reglamentación o por ley).

6.23.7 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 (p. ej., 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 6.23.4 se tratan otras necesidades de los usuarios discapacitados de los servicios de telecomunicaciones de emergencia.

NOTA 2 – Véase también en la Bibliografía [b-ITU-T P. TALL] y [b-ITU-T F.790].

6.23.8 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 6.12.2). 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 6.22.1.3).

6.23.9 Separación (*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, p. ej., por reglamentación o por ley, las NGN tendrán que soportar mecanismos para desglosar los servicios.

6.24 Protección de infraestructuras clave

Los proveedores de servicio deberían disponer 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 incluye 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 6.13 se presentan los requisitos de seguridad.

6.25 Confidencialidad de la información en las interfaces

Cuando se requiera, p. ej., por reglamentación, por ley, por condiciones nacionales o regionales, las NGN podrán:

- habilitar a los proveedores de servicio para que impidan que otras entidades descubran la información interna o de los usuarios del servicio a través de la interfaz NNI;
- habilitar a los proveedores de red para que impidan que otras entidades descubran la información interna a través de la interfaz NNI.

6.26 Intercambio entre proveedores de información relativa al usuario

Cuando se requiera, p. ej., por reglamentación o por ley, las NGN soportarán mecanismos para intercambiar información relativa al usuario entre diferentes NGN, a los efectos de la interoperabilidad de servicio.

Apéndice I

Correspondencia entre servicios y habilitadores de servicio

(Este apéndice no es parte integrante de esta Recomendación)

En este apéndice se presenta un ejemplo de correspondencia entre algunos servicios y sus habilitadores (cláusula 6.21). Esta correspondencia no es exhaustiva ni representa requisitos de servicio.

Cuadro I.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
Servicios vocales conversacionales 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 de entrega de contenidos		X				X	
Servicios "push"		X				X	
Servicios de difusión o multidifusión					X		
Servicios propios y de tránsito para empresas			X				X
Servicios de información	X	X				X	
Servicios de presencia y notificación general	X	X	X				
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		

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-R M.1645] Recomendación UIT-R M.1645 (2003), *Marco y objetivos generales del desarrollo futuro de las IMT-2000 y de los sistemas posteriores.*
- [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 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.*
- [b-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.*
- [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 multimedia.*
- [b-UIT-T H.263] Recomendación UIT-T H.263 (2005), *Codificación de vídeo para comunicación a baja velocidad binaria.*
- [b-UIT-T H.264] Recomendación UIT-T H.264 (2005), *Codificación de vídeo avanzada para los servicios audiovisuales genéricos.*
- [b-UIT-T H.510] Recomendación UIT-T H.510 (2002), *Movilidad para sistemas y servicios multimedia H.323.*
- [b-UIT-T H-suppl1] 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 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.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 multimedia.*
- [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.2111] Recomendación UIT-T Y.2111(2006), *Funciones de control de recursos y admisión en las redes de la próxima generación.*
- [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.*

Directrices del UIT-T

- [b-ITU-T TP.TACL] Las directrices, *Accessibility checklist for use in ITU-T standardization work (2006)* se encuentran en <http://www.itu.int/ITU-T/studygroups/com16/accessibility/docs/tacl.pdf>

Especificaciones técnicas del ETSI

- [b-101.331] ETSI TS 101 331 V1.2.1 (2006-06), *Requirements of Law Enforcement Agencies*.
- [b-102.71] 3GPP TS 22.071 3rd Generation Partnership Project; Technical specification Group Services and System Aspects; *Location Services (LCS); Service description; Stage 1* (Release 1999).
- [b-121.905] ETSI TR 121 905 V7.3.0 (2007-03), *Vocabulary for 3GPP Specifications*.
- [b-122.057] ETSI TS 122 057 V6.0.0 (2005-01), *Mobile Execution Environment (MExE) service description; Stage 1*.
- [b-122.127] ETSI TS 122 127 V7.1.0 (2006-03), *Service requirement for the Open Services Access (OSA); Stage 1*.
- [b-122.140] ETSI TS 122 140 V6.7.0 (2005-03), *Multimedia Messaging Service (MMS); Stage 1*.
- [b-122.146] ETSI TS 122 146 V7.2.0 (2006-09), *Multimedia Broadcast/Multicast Service (MBMS); Stage 1*.
- [b-122.174] ETSI TS 122 174 V6.2.0 (2005-01), *Push service; Stage 1*.
- [b-122.240] ETSI TS 122 240 V6.5.0 (2005-01), *Service requirements for 3GPP Generic User Profile (GUP); Stage 1*.
- [b-122.250] ETSI TS 122 250 V6.0.0 (2005-01), *IP Multimedia Subsystem (IMS) Group Management; Stage 1*.
- [b-122.708] ETSI TS 122 078 V7.6.0 (2005-12), *Customized Applications for Mobile network Enhanced Logic (CAMEL); Service description*.
- [b-123.141] ETSI TS 123 141 V7.2.0 (2006-09), *Presence service; Architecture and functional description; Stage 2*.
- [b-123.228] ETSI TS 123 228 V7.7.0 (2007-03), *IP Multimedia Subsystem (IMS); Stage 2*.
- [b-126.235] ETSI TS 126 235 V6.4.0 (2005-03), *Packet switched conversational multimedia applications; Default codecs*.
- [b-133.106] ETSI TS 133 106 V7.0.1 (2006-01), *Lawful interception requirements*.
- [b-142.033] ETSI TS 142 033 V7.0.0 (2007-06), *Lawful interception – Stage 1*.
- [b-181.005] ETSI TS 181 005 V1.1.1 (2006-03), *Services and Capabilities Requirements*.

Instituto nacional de normas de los Estados Unidos

- [b-JSTD025] ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance (CALEA)*.
- [b-T1.678] ANSI ATIS 1000678-2006, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks*.
- [b-T1.724] ANSI T1.724-2004, *UMTS Handover Interface for Lawful Interception, March, 2004*.
- [b-TIA-1066] TIA-1066 (2006), *Lawfully Authorized Surveillance (LAES) for cdma2000 Voice Over IP (VoIP)*.

- [b-TIA-1072] TIA-1072 (2006), *LAES for cdma2000 push-to-talk over cellular*.
- [b-TIA-1016-A] *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB), Service Options 62 and 63 for Spread Spectrum Systems (TIA-1016-A-2006)*.
- [b-TIA-127-A] *Enhanced Variable Rate Codec Speech Service Option 3 for Wideband Spread Spectrum Digital Systems (ANSI/TIA-127-A-2004)*.

Especificaciones del IETF

- [b-RFC 2486] IETF RFC 2486 (1999), *The Network Access Identifier*.
- [b-RFC 4594] IETF RFC 4594 (2006), *Configuration guidelines for DiffServ Service Classes*.

Especificaciones de la "Open Mobile Alliance"

- [b-OMA-DS] OMA Data Synchronization V1.2 – **Status:** Approved Enabler – **Release Date:** 2006-07-10.
- [b-OMA-DM] OMA Device Management V1.2 – **Status:** Approved Enabler – **Release Date:** 2007-02-09.
- [b-OMA-OSE] OMA Service Environment V1.0 – **Status:** Candidate Release – **Release Date:** 2007-03-13.
- [b-OMA-PoC] OMA Push to talk over Cellular V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-PS] OMA Presence Simple V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-WS] OMA Web Services V1.1 – **Status:** Approved Enabler – **Release Date:** 2006-03-28.
- [b-OMA-XML] OMA XML Document Management V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-LS] OMA Mobile Location Service V1.1 – **Status:** Candidate Enabler – **Release Date:** 2006-10-20.
- [b-OMA-XDM] OMA XML Document Management V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-Push] OMA Push V2.1 – **Status:** Candidate Enabler – **Release Date:** 2005-11-22.

Open Service Access (OSA)

- [b-OSA-Parlay-X] *Open Service Access (OSA), Parlay X Web Services, Parts 1-14, ETSI ES 202 391-[1-14] V1.1.1 (2006-12)*.
- [b-OSA-Parlay-4] *Open Service Access (OSA), Application Programming Interface (API), Parts 1-14, ETSI ES 202 915-[1-14] V1.3.1 (2006-12)*.
- [b-OSA-Parlay-5] *Open Service Access (OSA), Application Programming Interface (API), Parts 1-15, ETSI ES 203 915-[1-15] V1.1.1 (2007-01)*.

Servicios IN

- [b-TIA-771] TIA/EIA/IS 771-1 (1999), *Wireless Intelligent Network – Addendum 1 (2001)*.
- [b-TIA-873] TIA/EIA 873.002 (2003), *All IP Core Network Multimedia Domain – IP Multimedia Subsystem – Stage-2*.

Especificaciones de la UDDI

[b-UDDI] UDDI Specification Technical committee, *UDDI Specification*,
Version 3.0.2.

Especificaciones de la SOA

[b-OASIS-SOA] *OASIS, Reference Model for Service Oriented Architecture 1.0*, Committee
Specification 1. 2 August 2006.

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	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
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