Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.261

(10/2009)

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIA

IPCablecom

Marco para la prestación de servicios de telecomunicaciones preferentes en redes IPCablecom e IPCablecom2

Recomendación UIT-T J.261

Recomendación UIT-T J.261

Marco para la prestación de servicios de telecomunicaciones preferentes en redes IPCablecom e IPCablecom2

Resumen

La Recomendación UIT-T J.261 define un marco para la implementación de capacidades preferentes en redes IPCablecom e IPCablecom2.

El método adoptado por esta Recomendación consiste en definir un marco para las capacidades que pueden utilizarse con el fin de cumplir los requisitos estipulados en la Recomendación UIT-T J.260 y sentar las bases para la elaboración de Recomendaciones detalladas basadas en IPCablecom e IPCablecom2 sobre telecomunicaciones preferentes.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T J.261	2009-10-30	9

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Introducción

Las telecomunicaciones en caso de emergencia/catástrofes para los usuarios autorizados son de vital importancia para la salud, la seguridad y el bienestar de los ciudadanos de todos los países. Por lo general, para facilitar cualquier tipo de operación de emergencia/socorro se recurre a capacidades que garanticen unas telecomunicaciones de emergencia fáciles de utilizar y que puedan materializarse adoptando las correspondientes soluciones técnicas y/o políticas administrativas. La infraestructura IPCablecom e IPCablecom2 constituye un importante recurso para ofrecer servicios de telecomunicaciones preferentes.

Los dos aspectos esenciales de las telecomunicaciones preferentes por redes de cable que se tratan en la presente Recomendación son la autentificación y la prioridad. Estos aspectos constituyen las funciones de red esenciales para obtener acceso a los recursos de las redes de cable cuando se requiere un trato preferente. Otros aspectos, como los relativos a políticas, ingeniería de tráfico, encaminamiento alternativo, capacidad de restablecimiento, etc., quedan fuera del alcance de la presente Recomendación o no se abordan en esta versión.

Dada la naturaleza evolutiva de las redes de comunicaciones en general y de las redes de cable en particular, es preciso adoptar un método por fases en el trato preferente. En dicho método se ha de tomar en consideración la evolución de las Recomendaciones relativas a IPCablecom, es decir, el conjunto inicial de Recomendaciones sobre IPCablecom, las versiones revisadas en 2005 y el conjunto de Recomendaciones relativas a IPCablecom2.

Recomendación UIT-T J.261

Marco para la prestación de servicios de telecomunicaciones preferentes en redes IPCablecom e IPCablecom2

1 Alcance

El objetivo de la presente Recomendación es proporcionar un marco para la prestación de servicios de telecomunicaciones preferentes en redes de cable, como se describe en [UIT-T J.160] y [UIT-T J.360]. Este marco es uno de la serie de Recomendaciones que versan sobre estos servicios.

Los dos aspectos fundamentales de los servicios de telecomunicaciones preferentes que se tratan en este marco son la prioridad y la autentificación. Las diferencias arquitectónicas entre estos dos aspectos se indican mediante las entidades lógicas funcionales definidas en [UIT-T J.160] y [UIT-T J.360], respectivamente.

En esta versión del marco se abordan estos dos aspectos fundamentales, a saber, la prioridad y la autentificación necesarias para poder dar un trato preferente en los servicios de telecomunicaciones, mientras que otros aspectos tales como la política, la ingeniería de tráfico, el encaminamiento alternativo, la configuración, etc., quedan fuera del alcance de la misma o se estudiarán en un futuro. Por ejemplo, en futuras versiones se prevé abordar el tema de la prestación de servicios preferentes a determinados usuarios y/o dispositivos (adaptadores terminales de medios) que se encuentren en un lugar específico.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T J.160] Recomendación UIT-T J.160 (2005), *Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable*.

[UIT-T J.163] Recomendación UIT-T J.163 (2007), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable*.

[UIT-T J.170] Recomendación UIT-T J.170 (2005), *Especificación de la seguridad de IPCablecom*.

[UIT-T J.179] Recomendación UIT-T J.179 (2005), *Soporte de IPCablecom para multimedia*.

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

[UIT-T J.360] Recomendación UIT-T J.360 (2006), *Arquitectura general IPCablecom2*.

[UIT-T J.368] Recomendación UIT-T J.368 (2008), *IPCablecom 2: Especificación de la calidad del servicio*.

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

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

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos.

3.1.1 capacidades garantizadas [UIT-T J.260]: Capacidades que sean muy dignas de confianza o garantizan la disponibilidad y fiabilidad de las comunicaciones mínimas necesarias.

3.1.2 autentificación [UIT-T J.260]: Acción o método utilizado para verificar la identidad supuesta.

3.1.3 autorización [UIT-T J.260]: Acto de determinar que un privilegio particular, como el acceso a algún tipo de recurso, puede concederse tras la presentación de una credencial a dicho efecto.

3.1.4 módem de cable [UIT-T J.160]: Un módem de cable es un dispositivo terminal de capa 2 que termina el extremo cliente de la conexión DOCSIS.

3.1.5 situación de emergencia [UIT-T J.260]: Situación de naturaleza grave que ocurre súbita e inesperadamente. Para restaurar un estado de normalidad y evitar mayores riesgos para las personas o las propiedades puede ser necesario llevar a cabo inmediatamente actividades a gran escala, con ayuda de las comunicaciones. Si la situación se agrava, puede transformarse en crisis y/o catástrofes.

3.1.6 situación de emergencia internacional [UIT-T J.260]: Situación de emergencia que traspasa las fronteras nacionales y afecta a más de un país.

3.1.7 IPCablecom [UIT-T J.160]: Proyecto del UIT-T consistente en una arquitectura y una serie de Recomendaciones que permiten la entrega de servicios en tiempo real por las redes de televisión por cable empleando módems de cable.

3.1.8 etiqueta [UIT-T J.260]: Identificador inherente o adjunto a elementos de datos. En el marco de las telecomunicaciones preferentes es una indicación de prioridad. Este identificador se puede utilizar como mecanismo de correspondencia entre diversos niveles de prioridad de red.

3.1.9 red IP gestionada [UIT-T J.160]: Una red IP gestionada por una sola entidad y que se utiliza para transportar señalización IPCablecom y paquetes de medios.

3.1.10 preferente [UIT-T J.260]: Capacidad que presenta ventajas con respecto a las capacidades normales.

3.1.11 capacidades de tratamiento prioritario [UIT-T J.260]: Capacidades que proporcionan acceso prioritario a los recursos de redes de telecomunicaciones y/o su utilización.

3.1.12 abonado [UIT-T J.360]: Una entidad (que incluye a uno o más usuarios) que tiene una suscripción con un proveedor de servicio.

3.1.13 agente de usuario (AU) [UIT-T J.360]: Un agente de usuario SIP tal como se define en [IETF RFC 3261].

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se define el siguiente término:

3.2.1 equipo de usuario: Todo dispositivo que utiliza directamente un usuario para comunicarse.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

AKA Acuerdo de autentificación y claves (*authentication and key agreement*)

ATM Cajero automático (*automatic teller machine*)

AVP Par atributo-valor (*attribute value pair*)

CM Módem de cable (*cable modem*)

CMS Servidor de gestión de llamadas (*call management server*)

CMTS Sistema de terminación de módem de cable (*cable modem termination system*)

DQoS Calidad de servicio dinámica (*dynamic quality of service*)

E-DVA Adaptador de voz digital integrado (*embedded digital voice adapter*)

E-MTA Adaptador terminal de medios integrado (*embedded media terminal adapter*)

IPSec Seguridad del protocolo Internet (*Internet protocol security*)

KDC Centro de distribución de claves (*key distribution centre*)

MGC Controlador de pasarela de medios (*media gateway controller*)

MTA Adaptador terminal de medios (*media terminal adapter*)

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

P-CSCF Función intermedia de control de sesión de llamada (*proxy call session control function*)

PKI Infraestructura de clave pública (*public key infrastructure*)

PKINIT Criptografía de clave pública para autentificación inicial (*public key cryptography for initial authentication*)

QoS Calidad de servicio (*quality of service*)

RTP Protocolo de transporte en tiempo real (*real time transport protocol*)

RTPC Red telefónica pública conmutada

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

TGT Billete de concesión de billete (*ticket granting ticket*)

TLS Seguridad de la capa de transporte (*transport layer security*)

UE Equipo de usuario (*user equipment*)

5 Convenios

Ninguno.

6 Marco común para la prioridad

En [UIT-T J.260] se enumeran una serie de requisitos para garantizar el trato prioritario en las redes IPCablecom e IPCablecom2. Aunque existen diferencias en la arquitectura de IPCablecom (que se describe en [UIT-T J.160]) y la de IPCablecom2 en ([UIT-T J.360]), en la presente cláusula se describe el marco aplicable a los dos tipos de red. Al abordar el tema del trato prioritario para la prestación de servicios de telecomunicaciones preferentes es necesario tomar en consideración tres aspectos, a saber, la clasificación o etiquetado de la llamada o sesión que requiere un trato prioritario, la señalización de la prioridad y los mecanismos para conferir la prioridad solicitada.

La selección de los mecanismos y las políticas, así como su correspondiente puesta en práctica, quedan fuera del alcance de la presente Recomendación.

En el cuadro 1 se clasifican los requisitos en tres categorías con arreglo a estos tres aspectos, es decir, la clasificación, la señalización y los mecanismos. Algunos de los requisitos pertenecen a más de una categoría, por cuanto la clasificación de la prioridad de la llamada se mantiene, mientras que los mecanismos concretos para preservar dicha clasificación pueden variar.

Cuadro 1 – Relación entre los requisitos y los aspectos relativos a la prioridad

Requisito de [UIT-T J.260]	Categoría
Acceso prioritario a las redes IPCablecom e IPCablecom2 (1a)	Clasificación
Activación de la llamada y características de la misma (1b)	Señalización
Atribución de recursos de red (1c)	Mecanismos
Trato prioritario a las llamadas etiquetadas en las pasarelas (1d)	Señalización y mecanismos
Asignación de etiquetas en el origen de la llamada (2)	Clasificación
Trato prioritario a las llamadas etiquetadas en las redes IPCablecom e IPCablecom2 (3)	Mecanismos
Correspondencia entre las etiquetas utilizadas de la red de cable al dispositivo de la pasarela de red de conexión, y viceversa (4 y 5)	Mecanismos
Mantenimiento de la prioridad a través de las redes de cable (6)	Señalización y mecanismos
Tratamiento de las llamadas prioritarias que circulan por la red de cable con arreglo a las capacidades de ésta (7)	Clasificación y mecanismos
Número de niveles de prioridad: mínimo 1 y posibilidad de otros niveles en función de las opciones nacionales (8)	Clasificación
Trato prioritario en la red de cable a las llamadas con etiqueta de prioridad procedentes de una red fiable (9)	Mecanismos

Por prioridad en el caso de una llamada/sesión se entiende que ésta adquiere mayor probabilidad de llevarse a buen término. Dicho de otro modo, una vez que se ha determinado que el tráfico corresponde a un servicio de telecomunicaciones preferente, se le ha de conferir mayor probabilidad de completarse que en el caso de la admisión de llamadas, encaminamiento y transmisión de tráfico. Esta capacidad debe estar integrada en el enlace de acceso y se ha de propagar por todas las entidades de red pertinentes, tales como los servidores de gestión de llamadas (CMS, *call management servers*) y los controladores de pasarela de medios (MGC, *media gateway controller*) o las entidades de la infraestructura del protocolo de inicio de sesión (SIP, *session initiation protocol*).

Si bien los mecanismos de activación de la prioridad y asignación de la QoS no son idénticos, en IPCablecom puede recurrirse a las clases de sesión DQoS para asignar el trato prioritario a una sesión. Uno de los requisitos para atribuir recursos que puedan emplearse en las redes IPCablecom es el concepto de puertas multimedios descrito en [UIT-T J.163] y [UIT-T J.179]. La [UIT-T J.163] es específica de IPCablecom y se describe a continuación. Las puertas sirven para controlar el acceso de un flujo IP a la QoS mejorada desde la red DOCSIS y se instalan en los sistemas terminales del módem de cable (CMTS) para permitir la creación de flujos de servicio con un nivel de QoS garantizado gracias a la reserva de los recursos necesarios. El control de admisión en el CMTS se emplea para asegurarse de que el número de recursos disponibles es mayor que el de los comprometidos y reservados. En el caso de una red IPCablecom que utilice la [UIT-T J.163], el cliente, por ejemplo el adaptador terminal de medios integrado (E-MTA), inicia la reserva y activación de recursos, mientras que cuando se emplea la [UIT-T J.179] para multimedios es un intermediario quien efectúa estas tareas en nombre del cliente situado en el extremo.

La señalización de la prioridad se describe por separado en IPCablecom e IPCablecom2 debido a las diferencias en los métodos utilizados por el E-MTA o el UE para conectarse a la red de acceso.

El protocolo de transporte de medios para paquetes de audio y vídeo en IPCablecom e IPcablecom2 es el protocolo de transporte en tiempo real (RTP). Según se indicó en [b-IETF RFC 4190], el RTP no dispone de marcas para indicar la prioridad del paquete en la etiqueta. Se examinan diversos métodos en los que se define, entre otras cosas, un nuevo comportamiento por tramo para el tráfico preferente, un nuevo protocolo de capa de conversión por IP o el marcado de un paquete en la capa de aplicación.

7 Marco común para la autentificación

La autentificación en las redes IPCablecom e IPCablecom2 requiere que se proporcionen de algún modo credenciales, las cuales utiliza el sistema para verificar la integridad del identificador mostrado por un determinado usuario del sistema. La gestión de estas credenciales reviste una importancia considerable al considerar el tipo de mecanismos de autentificación utilizados en las redes de cable. Asimismo, es preciso examinar los mecanismos de autentificación existentes (para, por ejemplo, los abonados), y la aceptabilidad y utilidad de cualquier mecanismo de autentificación empleado para las telecomunicaciones preferentes en otras redes. Las dos formas disponibles de autentificación son las siguientes:

- autentificación basada en las credenciales del usuario, en el que el usuario preferente tiene que facilitar o introducir información en el dispositivo (por ejemplo, el E-MTA);
- autentificación basada en el equipo, en el que el sistema de la red de cable reconoce el equipo del usuario preferente.

7.1 Autentificación basada en las credenciales del usuario

La autentificación basada en las credenciales del usuario consiste en recurrir a una función integrada en el dispositivo o la red que acepta algún tipo de parámetro mediante el cual el usuario preferente puede autentificar su identidad. El dispositivo interactúa con un servidor de autentificación que forma parte de la infraestructura para validar el identificador que permite activar el servicio preferente. Una forma de realizar este tipo de autentificación consiste en que el usuario llame a un número especial y marque su número de identificación personal (NIP). Para ello puede utilizarse cualquier equipo de usuario de IPCablecom e IPCablecom2 que disponga de un teclado numérico normal de 12 teclas. Este método basado en el NIP resulta útil dada su simplicidad y su compatibilidad con las capacidades del servicio preferente en las redes existentes.

7.2 Autentificación basada en el equipo

Este tipo de autentificación consiste en que el sistema IPCablecom o IPCablecom2 reconozca el equipo de telecomunicaciones del usuario preferente. Es decir, se utiliza la identidad del equipo (por ejemplo, el certificado digital del dispositivo) para la identificación total o parcial de los usuarios de telecomunicaciones preferentes. Esta autentificación sólo estará disponible en determinadas partes del equipo (por ejemplo, teléfonos, E-MTA) y quizá resulte necesario recurrir a otros mecanismos (por ejemplo, tarjetas inteligentes, testigos y/o NIP) además de los de seguridad física del equipo.

7.3 Mecanismos básicos de autentificación

Si bien los mecanismos basados en el NIP son los más sencillos y accesibles en las actuales redes IPCablecom, en el futuro pudiera ser necesario disponer de métodos más seguro para algunas aplicaciones. En esta cláusula se describen estos métodos.

Una forma de llevar a cabo este tipo de autentificación consiste en que el usuario llame a un número especial y marque su número de identificación personal (NIP). Para ello puede utilizarse cualquier equipo de usuario de IPCablecom e IPCablecom2 que disponga de un teclado numérico normal

de 12 teclas. Este método basado en el NIP resulta útil dada su simplicidad y su compatibilidad con las capacidades de servicio preferente en las redes existentes. Sin embargo, este en método basado en NIP se recurre a un sólo factor (algo que sabe la persona) en lugar de una combinación de factores (en lugar de "un objeto que posee" o "algo único que lo caracteriza"). Con el aumento de la dependencia en las comunicaciones por paquetes, el método generalizado consiste en recurrir a dos factores, por ejemplo:

- conocer un NIP y disponer de una tarjeta de banda magnética (por ejemplo, como las que se utilizan en los cajeros automáticos de los bancos);
- conocer una contraseña y disponer de un dispositivo electrónico de validez limitada (por ejemplo, como los que se emplean para realizar operaciones bancarias y financieras en línea).

Ahora bien, muchos de estos métodos alternativos sólo sirven si el dispositivo dispone de otras capacidades entrada/salida además del teclado numérico de 12 botones.

Existen pocos mecanismos de autentificación (o combinaciones de mecanismos) que puedan emplearse en las redes de cable y que no se basen en el NIP. Una alternativa sería, por ejemplo, utilizar frases contraseña (suponiendo que la función de reconocimiento vocal tenga una tasa baja de "falsos positivos" y "falsos negativos"). Aunque existen otros muchos mecanismos de autentificación (por ejemplo, contraseñas, tarjetas inteligentes, analizadores biométricos, etc.), la arquitectura de las redes de cable no permite utilizarlos fácilmente (por ejemplo, los E-MTA no disponen de unidades de lectura de tarjetas inteligentes).

En el caso de servicios multimedios que requieren una determinada QoS, IPCablecom define interfaces en las que se utiliza la autentificación basada en RADIUS y DIAMETER: RADIUS entre el servidor de gestión de llamadas y el sistema de registro y DIAMETER entre la P-CSCF y la función de datos de tasación. A continuación se indican posibles mecanismos que no están definidos en las Recomendaciones sobre IPCablecom y que cabría considerar para la autentificación del usuario de los servicios de trato preferente:

- contraseñas junto con una infraestructura de autentificación basada en RADIUS;
- contraseñas junto con una infraestructura de autentificación basada en Diameter;
- contraseñas junto con un centro de distribución de claves (KDC), como Kerberos;
- frases contraseña junto con una tarjeta inteligente; y
- frases contraseña junto con una tarjeta inteligente e infraestructura de clave pública (PKI).

Cada uno de estos mecanismos difiere en el grado de garantía que ofrece respecto a la validez de la identidad alegada que presenta un usuario autorizado del sistema. También difieren en su magnitud de despliegue, capacidad operativa y complejidad. Los métodos antes citados se habrán de examinar en mayor profundidad para determinan su capacidad de autentificación relativa, el grado de escalabilidad, el rendimiento, la compatibilidad entre dominios y con los mecanismos de autentificación tradicionales o existentes.

En el caso de la autentificación de trato preferente de determinadas llamadas/sesiones en redes IPCablecom, el nivel de seguridad debe ser alto. Ahora bien, la facilidad con la que un usuario obtiene autentificación también debe ser alta por cuanto en algunos casos el usuario puede encontrarse en una situación de emergencia. Así pues, siempre que sea posible se seleccionará una combinación de mecanismos que sea fácil de utilizar y ofrezca un alto grado de seguridad.

7.4 Mecanismos de gestión de credenciales

La gestión de credenciales es importante para garantizar que el sistema utiliza credenciales actualizadas y precisas para la autentificación del usuario. La gestión de credenciales comprende lo siguiente: actualización, revocación e intercambio de credenciales a través de los dominios de distintos proveedores de servicio.

La gestión de credenciales depende de las propias credenciales, tales como bases de datos de contraseñas, servidores RADIUS/Diameter, servidores KDC, tarjetas inteligentes y raíz PKI, etc. Cada uno de estos tipos de mecanismo varía en cuanto al grado de protección de la integridad y confidencialidad de los datos que ofrecen las credenciales. También difieren en la magnitud del despliegue, la capacidad operativa y la complejidad.

8 Autentificación y prioridad en redes IPCablecom

8.1 Autentificación en redes IPCablecom

En [UIT-T J.160] y [UIT-T J.170] se describen los mecanismos utilizados para autentificar el cliente que solicita el servicio. El protocolo utilizado para ello es Kerberos con ampliación de la criptografía de clave pública para la autentificación inicial (PKINIT). Para crear una asociación segura entre el servidor de gestión de llamadas (CMS) y el MTA (cliente) se recurre a la seguridad del protocolo Internet (IPSec) con Kerberos. Se describen tres fases. En la primera fase, el cliente envía el certificado del dispositivo al centro de distribución de claves (KDC) para obtener un billete de concesión de billete (TGT, *ticket granting ticket*) que le permite obtener un billete (ticket) del KDC para un determinado servidor, como por ejemplo el CMS. El cliente puede saltarse la primera fase y proporcionar al KDC su certificado del dispositivo con el fin de obtener directamente un billete para un determinado servidor. En la tercera fase, se definen un par de parámetros de seguridad con el servidor de aplicaciones que se utilizan para enviar y recibir datos protegidos por IPSec.

8.2 Prioridad en las redes IPCablecom

Los usuarios preferentes reciben un trato prioritario. Para ello se emplea el método definido en [UIT-T J.163].

La reserva de recursos en IPCablecom se realiza utilizando dos componentes. El primero en la capa de enlace de datos y consiste en lograr que los flujos del servicio DOCSIS estén más pronto disponibles para las puertas de ciertas clases de sesión. El segundo se aplica en la capa de sesión y consiste en describir el estado de la prioridad de una llamada de forma que la información pueda propagarse a todas las entidades de la red que corresponda.

En el enlace del acceso por cable, la prioridad puede establecerse asociando en primer lugar puertas de calidad de servicio dinámica (DQoS) con una determinada clase de sesión reservada especialmente para este fin y luego, como resultado, exigir al CMTS que tome las medidas adecuadas. Dependiendo del valor de la clase de sesión se aplica un control de admisión diferente a la solicitud de recursos resultante. Por ejemplo, podría definirse una clase de sesión para las comunicaciones de voz normales y una clase de sesión solapada para las llamadas de telecomunicaciones preferentes con el fin de permitir la atribución, respectivamente, del 50% y el 70% del total de recursos en sentido ascendente, y reservar el 30-50% restante para otros servicios, posiblemente de menor prioridad.

En [b-UIT-T J.162] se describe la señalización de llamadas basada en la red que utiliza IPCablecom entre el E-MTA y el agente de llamadas para crear y suprimir conexiones. Si bien el agente de llamadas proporciona el identificador de la puerta (GateID) al MTA durante el establecimiento de la llamada, deberá emplearse para la sesión un mecanismo, aún no disponible, que permita comunicar al MTA la prioridad del tráfico DOCSIS deseada. El CMTS utiliza dicha información para establecer la prioridad del tráfico durante los periodos de congestión. Es necesario estudiar con mayor profundidad este tema en el contexto de las telecomunicaciones preferentes.

9 Autentificación y prioridad en redes IPCablecom2

9.1 Autentificación en redes IPCablecom2

IPCablecom2 admite dos tipos de equipos de usuario (EU), integrados e independientes. Éstos se materializan en software y pueden disponer de capacidades para conectar un dispositivo físico seguro, por ejemplo una tarjeta inteligente. Se prevé que los mecanismos de autentificación disponibles en las redes IPCablecom2 sean más versátiles y que pronto dispondrán de un tipo de autentificación adecuada.

En el apéndice III de [UIT-T J.360] se describen tres mecanismos de autentificación que pueden utilizarse en la arquitectura de IPCablecom2: Autenticación y acuerdo de clave (AKA) del subsistema multimedios IP (IMS), autentificación *Digest* del protocolo de inicio de sesión (SIP) y autentificación basada en certificados. Los requisitos de los diversos componentes de las redes IPCablecom2 se especifican en función del mecanismo utilizado para la autentificación. Por ejemplo, para poder emplear la autentificación *Digest*, es necesario almacenar de manera segura los nombres y contraseñas del usuario.

La señalización entre el EU y la P-CSCF se protege utilizando IPSec o TLS. En [UIT-T J.360] se exige que el EU pueda negociar la utilización de TLS. Se han definido dos modelos para la seguridad a través de TLS, a saber: la autentificación mutua, en la que tanto el EU como el servidor (por ejemplo, la P-CSCF) validan los certificados entre sí, y la autentificación en el servidor, en la que sólo el servidor puede certificar para establecer la seguridad de la señalización. El primero ofrece mayor nivel de seguridad; IPCablecom2 requiere la autentificación en el servidor. Convendría considerar la posibilidad de realizar la autentificación mutua de los equipos de usuario que se utilizan para iniciar servicios de trato preferente.

La red IPcablecom2 requiere que el abonado afirme su identidad mediante la P-CSCF para transmitir la autenticidad del usuario a los demás elementos de red en una red fiable y para suprimir la identidad cuando se comunica a elementos de redes no fiables. El hecho de afirmar y suprimir la identidad garantiza que los servicios de telecomunicaciones preferentes los inicie un usuario autorizado.

En [b-UIT-T J.262] se definen los requisitos.

9.2 Prioridad en las redes IPCablecom2

La arquitectura de IPCablecom2, que se describe en [UIT-T J.360], se basa en la infraestructura IMS de 3GPP. La prioridad se establece en tres lugares: en la señalización IMS, en el mecanismo de activación y en el etiquetado de los paquetes.

9.2.1 Señalización de la prioridad

A nivel de la señalización IMS se utilizan dos nuevos encabezamientos SIP, a saber *Resource-Priority* (prioridad del recurso (R-P)) y el *Accept-Resource-Priority* (prioridad del recurso aceptada) definidos en [IETF RFC 4412]. Al añadir estos encabezamientos en los mensajes de petición y respuesta, respectivamente, los servidores intermediarios y los agentes de usuario (AU) del SIP pueden conferir trato prioritario a las peticiones.

Para solicitar acceso prioritario a los recursos se incluye en los mensajes de petición SIP el encabezamiento *Resource-Priority* (R-P), definido en [IETF RFC 4412]. Para indicar que el agente de usuario SIP acepta la prioridad, en la respuesta se incluye el encabezamiento *Accept-Resource-Priority*, indicando los valores R-P. Estos valores se registran en la IANA (*autoridad* de asignación de números Internet) y el encabezamiento es un campo opcional. IANA registra cinco espacios de nombres que se incluyen en la RFC. En la presente Recomendación no se propone la utilización de un espacio de nombres en concreto. Además, los espacios de nombres adicionales que pudieran necesitarse para los servicios de telecomunicaciones preferentes podrían registrarse con arreglo a

los procedimientos definidos en [IETF RFC 4412]. La utilización del encabezamiento R-P permite la señalización de la prioridad.

Cabe señalar que estos encabezamientos no influyen directamente la forma en que efectúan la retransmisión los encaminadores IP. Dicha funcionalidad, es decir, en la capa de red o en la capa 3, se está estudiando. En [IETF RFC 3690] se definen los requisitos generales del sistema para dar soporte a los servicios preferentes en el ámbito general de la telefonía IP considerada como un servicio de extremo a extremo. Es útil considerar estos requisitos en el contexto de IPCablecom2 para el trato preferente.

9.2.2 Mecanismos de activación

A nivel de la red de acceso, pueden utilizarse los parámetros par de valor de atributo (AVP, *attribute value pair*) del encabezamiento *Reservation-Priority* (prioridad de la reserva) para indicar la prioridad al solicitar recursos de la red de acceso. Para definir las especificaciones de puerta para la reserva de recursos, la P-CSCF interactúa con el gerente de aplicaciones de IPCablecom2 utilizando para ello la interfaz Rx definida en el IMS de 3GPP. Esta interfaz emplea el protocolo Diameter con una serie de nuevos parámetros AVP definidos en las especificaciones de la QoS en [UIT-T J.368].

Los mensajes GateSpec utilizados para solicitar y activar recursos de la red de acceso consta, entre otros, de un ID de clase de sesión que define el nivel de prioridad de la solicitud. Si bien el agente de llamada facilita el GateID al adaptador de voz digital integrado (E-DVA, *embedded digital voice adapter*) durante el establecimiento de llamada, deberá utilizarse en la sesión un mecanismo, aún no disponible, para comunicar la prioridad deseada del tráfico DOCSIS al E-DVA. El CMTS utiliza esta prioridad del tráfico DOCSIS para establecer la prioridad del tráfico durante los periodos de congestión. Es preciso estudiar con más profundidad este tema.

En la red de acceso DOCSIS, puede asignarse prioridad del tráfico con el fin de dar un trato prioritario en los diversos tipos de flujo de servicio.

La definición de los valores específicos que habrán de utilizarse para especificar los niveles de prioridad para el servicio de telecomunicaciones preferentes queda fuera del alcance de la presente Recomendación.

Si bien existen mecanismos para emplear el encaminamiento prioritario en la red medular de paquetes IP, tales como la señalización SIP y los paquetes de portador RTP, su definición no se incluye en la presente Recomendación.

9.2.3 Etiquetado

Actualmente el RTP, que es el protocolo de transferencia de medios utilizado en IPCablecom2, no permite realizar un etiquetado de la prioridad.

En [b-UIT-T J.263] se definen en detalle los requisitos.

Bibliografía

[b-UIT-T E.106] Recomendación UIT-T E.106 (2003), *Plan internacional de preferencias en situaciones de emergencia para actuaciones frente a desastres*.

[b-UIT-T J.162] Recomendación UIT-T J.162 (2007), *Protocolo de señalización de llamada de red para la prestación de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable*.

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

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

[b-UIT-T Q-Sup.57] Suplemento 57 a la serie Q de Recomendaciones UIT-T (2008), *Requisitos de señalización para el soporte del servicio de telecomunicaciones de emergencia (ETS) en las redes IP*.

[b-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*.

[b-UIT-T Y.2205] Recomendación UIT-T Y.2205 (2008), *Redes de la próxima generación – Telecomunicaciones de emergencia – Consideraciones técnicas*.

[b-UIT-T Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autentificación y autorización en las redes de próxima generación versión 1*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3689] IETF RFC 3689 (2004), *General Requirements for Emergency Telecommunication Service (ETS)*.

[b-IETF RFC 3690] IETF RFC 3690 (2004), *IP Telephony Requirements for Emergency Telecommunication Service (ETS)*.

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

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2010