Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.360

(11/2006)

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

IPCablecom

Arquitectura general de IPCablecom2

Recomendación UIT-T J.360

UIT-T

ITU Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.360

Arquitectura general de IPCablecom2

Resumen

Esta Recomendación UIT-T J.360 relativa a la arquitectura general ofrece una visión general de carácter técnico de la ampliación de IPCablecom al contexto multimedia.

Orígenes

La Recomendación UIT-T J.360 fue aprobada el 29 de noviembre de 2006 por la Comisión de Estudio 9 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

			Página
1	Alcance y visión general		1
	1.1	Alcance	1
	1.2	Visión general de IPCablecom2	1
2	Referencias		2
	2.1	Referencias normativas	2
	2.2	Referencias informativas	2
3	Términos y definiciones		3
4	Abreviaturas, siglas o acrónimos		4
5	IPCablecom2		6
	5.1	Relación con el IMS del 3GPP	6
	5.2	Visión general	7
	5.3	Versiones y organización de IPCablecom	11
	5.4	Consideraciones de diseño de IPCablecom2	14
6	Componentes funcionales de IPCablecom		17
	6.1	Red local	17
	6.2	Red de acceso	18
	6.3	Borde	18
	6.4	Núcleo	19
	6.5	Multimedia de IPCablecom	21
	6.6	Aplicación	21
	6.7	Interconexión	22
	6.8	Sistemas de soporte de las operaciones	23
7	Interfaces de protocolo y puntos de referencia		24
	7.1	Señalización y control del servicio	24
	7.2	Datos de abonado	26
	7.3	Calidad de servicio	27
	7.4	Tránsito del traductor de direcciones de red (NAT, *network address translation*) y de la barrera contrafuegos	29
	7.5	Codificación de medios y transporte	31
	7.6	Provisión, activación, configuración y gestión (PACM)	32
	7.7	Contabilización y utilización de la red	34
	7.8	Seguridad	35
	7.9	Interceptación legal	38
	7.10	Descubrimiento del punto de control	40
Apéndice I – Visión general de la señalización SIP			41
	I.1	Introducción y objetivo	41
	I.2	Referencias	43
	I.3	Términos y definiciones	43

Página

I.4 Abreviaturas y acrónimos 44
I.5 Señalización SIP de IPCablecom2 44
I.6 Requisitos del IMS para IPCablecom2 52
Apéndice II – Visión general técnica de la arquitectura de calidad de servicio 73
II.1 Introducción 73
II.2 Referencias 73
II.3 Términos y definiciones 74
II.4 Abreviaturas, siglas o acrónimos 74
II.5 Requisitos y alcance de la calidad de servicio 74
II.6 Marco de la arquitectura para calidad de servicio 75
II.7 Descripción de la arquitectura 79
II.8 Ejemplos de procedimientos 82
Apéndice III – Visión general de la seguridad de IPCablecom2 85
III.1 Introducción 85
III.2 Referencias 85
III.3 Términos y definiciones 86
III.4 Abreviaturas, siglas o acrónimos 86
III.5 Seguridad de IPCablecom2 87
III.6 Requisitos de seguridad de IPCablecom 98
Apéndice IV – Visión general del servidor de abonado de la red de origen en IPCablecom2 (HSS, *home subscriber server*) 113
Apéndice V – Visión general del tránsito del NAT y de la barrera contrafuego en IPCablecom2 114
V.1 Introducción 114
V.2 Referencias 114
V.3 Términos y definiciones 114
V.4 Abreviaturas, siglas o acrónimos 115
V.5 Requisitos y campo de aplicación del nat de IPCablecom2 115
V.6 Aspectos básicos del NAT 116
V.7 Arquitectura del NAT de IPCablecom2 119
V.8 Descripción de la arquitectura 122
Apéndice VI – Visión general de la estrategia IPv6 e IPv4 de IPCablecom2 128

Recomendación UIT-T J.360

Arquitectura general de IPCablecom2

1 Alcance y visión general

1.1 Alcance

La versión inicial de IPCablecom [UIT-T J.160-178] fue concebida para la telefonía. El sistema IPCablecom para multimedia [UIT-T J.179] crea un puente que permite la extensión de IPCablecom a una amplia gama de servicios multimedia. Esta Recomendación proporciona la arquitectura, las bases técnicas y la organización del proyecto para la segunda versión de la familia de recomendaciones relativas a IPCablecom destinadas a su extensión al ámbito multimedia.

1.2 Visión general de IPCablecom2

IPCablecom2 es un esfuerzo de la industria del cable destinada a permitir la convergencia de las tecnologías de voz, video, datos y movilidad. Existen decenas de millones de clientes de banda ancha por cable, y cada vez es mayor la capacidad de la red para ofrecer servicios innovadores adicionales al acceso a Internet de banda ancha. En particular, los servicios de comunicaciones en tiempo real basados en los protocolos IP, como por ejemplo, la voz sobre IP (VoIP), están evolucionando rápidamente y los clientes están adoptando y una amplia gama de dispositivos de cliente y de tipos de medios. Es previsible que las nuevas tecnologías, tales como video sobre IP y la representación de las notificaciones de mensajes de voz y de correo en el equipo de TV, cambien la forma en la que se ofrecen los servicios de comunicación y de entretenimiento. Estas tecnologías avanzadas permitirán a los operadores de cable presentar a los consumidores una oferta de servicios de alto valor y eficiente en términos de costes.

IPCablecom2 define una arquitectura y un conjunto de interfaces abiertas para aprovechar tecnologías emergentes de comunicaciones, tales como el protocolo de inicio de sesión (SIP, *session initiation protocol*) de [IETF RFC 3261], con el objetivo de conseguir la rápida introducción en las redes por cable de nuevos servicios basados en IP. Un enfoque modular permite a los operadores desplegar de forma flexible las capacidades de red necesarias en función de los servicios ofrecidos, manteniendo la interoperabilidad entre dispositivos de distintos suministradores. Dicha plataforma, que intencionadamente se ha diseñado como no específica para servicios en particular, proporcionaría las capacidades básicas necesarias para que los operadores puedan ofrecer servicios en los ámbitos de:

- Comunicaciones residenciales de VoIP y de video basado en IP mejoradas – Capacidades para la videotelefonía, el tratamiento de llamadas en función de la presencia, la capacidad de los dispositivos o la identidad, junto con funcionalidades como la de "hacer click para marcar";
- Integración de prestaciones de distintas plataformas – Capacidades tales como la presentación del nombre del llamante e identificación del número en la TV y el tratamiento de las llamadas desde el propio equipo de TV;
- Servicios con movilidad e integración con redes celulares e inalámbricas – Funcionalidades tales como el traspaso de llamadas y la itinerancia entre VoIP de IPCablecom sobre WiFi y redes inalámbricas – celulares; integración del correo de voz; número único E.164 (es decir, el número telefónico);
- Aplicaciones multimedia – Capacidad para establecer trenes de video y audio con calidad de servicio (QoS);

- Ampliación de servicios comerciales – Funcionalidades tales como centralitas (PBX), servicios Centrex IP para pequeñas y medianas empresas y enlaces basados en VoIP para la unión de centralitas privadas IP (IP-PBX);
- Ampliación de la telefonía SIP en el ámbito residencial – Funcionalidades propias de la telefonía tradicional (por ejemplo, llamada en espera, ID del llamante), servicios a través de operadora y servicios de emergencia.

Tal como se ha señalado anteriormente, la arquitectura está diseñada para soportar una amplia gama de servicios. El conjunto de recomendaciones de IPCablecom2 define una arquitectura básica y los componentes y requisitos genéricos necesarios para un amplio número de servicios y aplicaciones. Los servicios y aplicaciones específicas descansan sobre esta arquitectura básica, pero se especifican en diversas ediciones de la misma. Las especificaciones base deberían poder acomodar distintos servicios y aplicaciones con muy pocos cambios o ninguno.

Esta versión de IPCablecom se basa en la versión 6 del susbsistema multimedia IP (IMS) desarrollado por el 3GPP. El IMS es una arquitectura basada en SIP para la provisión de servicios multimedia. IPCablecom2 define mejoras del IMS para garantizar se satisfacen requisitos de IPCablecom que aún no recoge el IMS.

Un objetivo importante de este trabajo es asegurar la interoperabilidad entre el IPCablecom 2.0 y el IMS del 3GPP. Aunque IPCablecom2 está basado en el IMS del 3GPP, incluye funcionalidades adicionales para satisfacer los requisitos de los operadores de cable. El hecho de reconocer y favorecer el desarrollo de soluciones convergentes para sistemas inalámbricos, de líneas fijas y de cable permitirá continuar el desarrollo de IPCablecom 2.0, contribuyendo al desarrollo del IMS del 3GPP con el objetivo de alinear el desarrollo del IMS del 3GPP y de IPCablecom 2.0.

IPCablecom2 aprovecha normas abiertas y especificaciones existentes siempre que ello es posible.

2 Referencias

2.1 Referencias normativas

Ninguna.

2.2 Referencias informativas

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

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

[UIT-T J.171.1] Recomendacón UIT-T J.171.1 (2005), *Protocolo de control de pasarela de circuitos troncales IPCablecom Perfil 1*.

[UIT-T J.178] Recomendación UIT-T J.178 (2005), *Señalización entre servidores de gestión de llamadas IPCablecom*.

[UIT-T J.179 Ap.I] Recomendación UIT-T J.179 (2005), *Soporte de IPCablecom para multimedia*. Apéndice I: *Información general*.

[UIT-T J.361] Recomendación UIT-T J.361 (2006), *Códec de medios IPCablecom2*.

[UIT-T J.362] Recomendación UIT-T J.362 (2006), *Detección de punto de control IPCablecom2*.

[UIT-T J.363] Recomendación UIT-T J.363 (2006), *Registro de información IPCablecom2 a los fines de contabilidad*.

[UIT-T J.364] Recomendación UIT-T J.364 (2006), *Alta, configuración, activación y gestión de IPCablecom2*.

[UIT-T J.365] Recomendación UIT-T J.365 (2006), *Interfaz de gestor de aplicación IPCablecom2*.

[ES-DCI] PacketCable Electronic Surveillance – *Delivery Function to Collection Function Interface Specification*, PKT-SP-ES-DCI-I01-060914 (2006), Cable Television Laboratories, Inc.

[ES-INF] PacketCable Electronic Surveillance – *Intra-Network Functions Specification*, PKT-SP-ES-INF-I01-060406, 6 April 2006, Cable Television Laboratories, Inc.

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

[TS 23.002] 3GPP 23.002 v6.10.0, *Network Architecture*, December 2005.

3 Términos y definiciones

En esta Recomendación se utilizan los términos y definiciones siguientes:

3.1 dirección de contacto: La URI de un agente de usuario en la red. Las direcciones de contacto, en el contexto de IPCablecom son a menudo, pero no siempre, direcciones utilizadas para hacer llegar peticiones a un agente de usuario específico.

3.2 E.164: E.164 es una Recomendación del UIT-T que define el plan de numeración de las telecomunicaciones públicas internacionales utilizado en la RTPC y en otras redes de datos.

3.3 cabecera: Ubicación central de la red de cable que es responsable de la inyección de los canales de difusión de video y de otras señales en sentido descendente.

3.4 especificaciones complementarias a IMS: Conjunto de especificaciones del IMS del 3GPP modificadas para reflejar los aspectos complementarios necesarios para la conformidad con IPCablecom.

3.5 IPCablecom Multimedia: Una arquitectura con calidad de servicio (QoS) y agnóstica con respecto a las aplicaciones para servicios prestados sobre redes DOCSIS.

3.6 identidad privada: Véase Identidad privada de usuario.

3.7 identidad privada de usuario: Utilizada, por ejemplo, con objetivos de registro, autorización, administración y contabilización. Una identidad privada de usuario se asocia con una o más Identidades públicas de usuario.

3.8 identidad pública: Véase Identidad pública de usuario.

3.9 identidad pública de usuario: Utilizada por cualquier usuario para solicitar comunicaciones con otros usuarios.

3.10 agente de usuario SIP: Véase "agente de usuario".

3.11 servidor: Elemento de red que recibe peticiones que da servicio y a las que responde. Son ejemplo de servidores los intermediarios (proxies), los servidores de agentes de usuario, los servidores de redireccionamiento y los registradores.

3.12 abonado: Una entidad (que incluye a uno o más usuario) que tiene una suscripción con un proveedor de servicio.

3.13 suscripción: Un contrato de servicio o servicios entre un usuario y un proveedor de servicio.

3.14 usuario: Una persona que, en el contexto de este documento, utiliza un servicio dado o invoca una funcionalidad de un agente de usuario (UA).

3.15 agente de usuario (UA): Un agente de usuario SIP tal como se define en [IETF RFC 3261].

3.16 sesión multimedia: Un conjunto de emisores y receptores multimedia y los flujos de datos entre emisores y receptores. La conferencia multimedia es un ejemplo de sesión multimedia.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

3GPP	Proyecto asociado de tercera generación (*3rd generation partnership project*)
ALG	Pasarela de capa de aplicación (*application layer gateway*)
AM	Gestor de aplicación (*application manager*)
AS	Servidor de aplicación (*application server*)
BGCF	Función de control de desganche en pasarela (*breakout gateway control functio*n)
CDF	Función de datos de tarificación (*charging data function*)
CDR	Registro detallado de llamadas (*call detail record*)
CM	Módem de cable (*cable modem*)
CMS	Servidor de gestión de llamada (*call management server*)
CMTS	Sistema de terminación de módem de cable (*cable modem termination system*)
CPE	Equipo en las instalaciones del cliente (*customer premises equipment*)
CSCF	Función de control de sesión de llamada (*call session control function*)
DHCP	Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)
DNS	Sistema de nombre de dominios (*domain name system*)
DOCSIS	Especificación de la interfaz de servicio de datos por cable (*data-over-cable service interface specification*)
EMS	Sistema de gestión de elemento (*element management system*)
E-MTA	Adaptador de terminal de medios incorporados (*embedded multimedia terminal adapter*)
ENUM	Correspondencia de número E.164 (E.164 *number mapping*)
ESP	Cabida útil de seguridad de encapsulado (*encapsulating security payload*)
FQDN	Nombre de dominio totalmente cualificado (*fully qualified domain name*)
FW	Barrera contrafuego (*firewall*)
GRUU	URI de agente de usuario encaminable globalmente (*globally routable user agent URI*)
HSS	Servidor de abonado en la red origen (*home subscriber server*)
HTTP	Protocolo de transferencia de hipertexto (*hyper text transfer protocol*)
ICE	Establecimiento de conectividad interactiva (*interactive connectivity establishment*)

I-CSCF	Interrogador de la función de control de sesión de llamada (*interrogating call session control function*)
IMS	Subsistema multimedios IP (*IP multimedia subsystem*)
IP	Protocolo Internet (*Internet protocol*)
IPSec	Seguridad del protocolo Internet (*Internet protocol security*)
MG	Pasarela de medios (*media gateway*)
MGC	Controlador de pasarela de medios (*media gateway controller*)
NA(P)T	Traducción dirección de red y de puerto (*network address and port translation*); NA(P)T y NAT se utilizan indistintamente
NAT	Traducción de dirección de red (*network address translation*)
NCS	Señalización de llamada basada en la red (*network-based call signalling*)
NMS	Sistema de gestión de red (*network management system*)
PACM	Provisión, activación, configuración y gestión (elemento PAC) (*provisioning, activation, configuration, and management (PAC element)*)
PAM	Gestor de aplicación de IPCablecom (*IPCablecom application manager*)
P-CSCF	Intermediario de la función de control de sesión de llamada (*proxy call session control function*)
PDS	Servidor de entrega de perfil (*profile delivery server*)
PSI	Identidad de servicio público (*public service identity*)
QoS	Calidad de servicio (*quality of service*)
RKS	Servidor de mantenimiento de registros (*record keeping server*)
RTCP	Protocolo de control de RTP (*RTP control protocol*)
RTP	Protocolo de transporte en tiempo real (*real-time transport protocol*)
RTPC	Red telefónica pública conmutada
S-CSCF	Servidor de la función de control de sesión de llamada (*serving vall dession vontrol function*)
SDP	Protocolo de descripción de sesión (*session description protocol)*
SG	Pasarela de señalización (*signalling gateway*)
SIP	Protocolo de inicio de sesión (*session initiation protocol*)
SLF	Función de ubicación de suscripción (*subscription locator function*)
SNMP	Protocolo simple de gestión de red (*simple network management protocol*)
SNTP	Protocolo simple de tiempo de red (*simple network time protocol*)
SS7	Sistema de señalización N.º 7 (*signalling system No. 7*)
STUN	Tránsito simple de UDP a través de un NAT (*simple traversal of UDP through NAT*)
TCP	Protocolo de control de transmisión (*transmission control protocol*)
TGCP	Protocolo de control de pasarela troncal (*trunking gateway control protocol*)
TLS	Seguridad de capa de transporte (*transport layer security*)

TR	Informe técnico (*technical report*)
TURN	Tránsito mediante NAT de retransmisión (*traversal using relay NAT*)
UA	Agente de usuario (*user agent*)
UDP	Protocolo de datagramas de usuario (*user datagram protocol*)
UE	Equipo de usuario (*user equipment*)
URI	Identificador de recursos uniforme (*uniform resource identifier*)
XCAP	Protocolo de acceso de configuración XML (*XML configuration access protocol*)
XDS	Servidor de datos XCAP (*XCAP data server*)

5 IPCablecom2

La arquitectura de IPCablecom2 describe un conjunto de grupos funcionales y entidades lógicas así como un conjunto de interfaces (denominadas puntos de referencia) que soportan los flujos de información intercambiados entre entidades.

En esta cláusula se proporciona:

- Una visión general de la arquitectura; incluyendo la descripción de las principales agrupaciones funcionales (por ejemplo, red local, red de acceso, borde, núcleo) y entidades lógicas (por ejemplo, UE, P-CSCF, S-CSCF, HSS) dentro de dichas agrupaciones.
- Un conjunto de objetivos de diseño para la arquitectura y especificaciones de IPCablecom2.
- Un conjunto de recomendaciones relativas a IPCablecom2.

5.1 Relación con el IMS del 3GPP

IPCablecom2 se basa en la versión 6 del susbsistema multimedia IP (IMS, *IP multimedia subsystem*) tal como ha sido definido por el 3GPP. El 3GPP es un acuerdo de colaboración en el que participan varios organismos de normalización. El objetivo del 3GPP es elaborar especificaciones técnicas e informes técnicos para GSM y para redes de sistemas móviles de tercera generación (3G).

El alcance del 3GPP incluye el desarrollo de una arquitectura de comunicaciones SIP basada en IP para redes móviles. La arquitectura resultante, denominada subsistema multimedia IP (IMS), define cómo pueden utilizarse los diversos protocolos (por ejemplo, SIP y DIAMETER) en una arquitectura a nivel de sistema para proporcionar servicios de comunicaciones basados en SIP.

Como parte del objetivo general de IPCablecom de aprovechar al máximo posible las normas ya desarrolladas por la industria, se persigue la alineación con la arquitectura y especificaciones del IMS que desarrolle el 3GPP. Específicamente, IPCablecom2 reutiliza muchas de las entidades funcionales básicas y puntos de referencia definidos en el IMS. La motivación básica que subyace tras este objetivo de diseño es la alineación con un conjunto de normas ampliamente apoyadas por los productos de los fabricantes, así como minimizar el esfuerzo de desarrollo de los productos necesarios para desplegar redes basadas en IPCablecom.

Aunque muchas de las entidades funcionales y puntos de referencia definidos en el IMS son de amplia aplicación en otros sectores de la industria, la versión 6 del IMS es una arquitectura que gira entorno a lo inalámbrico; está diseñada para satisfacer las necesidades de negocio y operacionales de la industria inalámbrica. Por lo tanto, no satisface todas las necesidades de la industria del cable. IPCablecom2 mejora el IMS para dar cabida a requisitos técnicos singulares de la industria del cable y para tener en cuenta los requisitos de negocio y operacionales de los operadores de cable.

3GPP está desarrollando una nueva versión de las especificaciones del IMS. Las futuras actualización de IPCablecom se alinearán con las nuevas versiones según convenga.

Para información adicional sobre la arquitectura IMS del 3GPP véase [TS 23.002].

5.2 Visión general

La arquitectura de IPCablecom2 está basada en la arquitectura del IMS, con algunas extensiones adicionales, como se señala en la cláusula 5.1. Dichas extensiones incluyen la utilización de componentes funcionales adicionales o alternativos comparados con la arquitectura del IMS, así como mejoras de capacidades proporcionadas por los componentes funcionales del IMS.

Algunas de las principales mejoras que introduce IPCablecom al IMS son las siguientes:

- Soporte de calidad de servicio (QoS) para aplicaciones basadas en IMS sobre redes de acceso DOCSIS, aprovechando así la arquitectura multimedia de IPCablecom [UIT-T J.179 Ap.I].
- Soporte del tránsito de señalización y medios a través de dispositivos de traducción de direcciones de red (NAT, *network address translation*) y de barrera contrafuegos (FW, *firewall*), en base a mecanismos desarrollados por el IETF.
- Soporte de la capacidad para identificar unívocamente y comunicar con un individuo cuando existen múltiples agentes de usuario (UA) registrados con la misma identidad pública.
- Soporte de seguridad de señalización de acceso y mecanismos de autenticación de UE adicionales.
- Soporte para la provisión, activación, configuración y gestión de los UE.

En la figura 1 se presenta una visión general de los elementos y agrupaciones funcionales de la arquitectura de IPCablecom2.

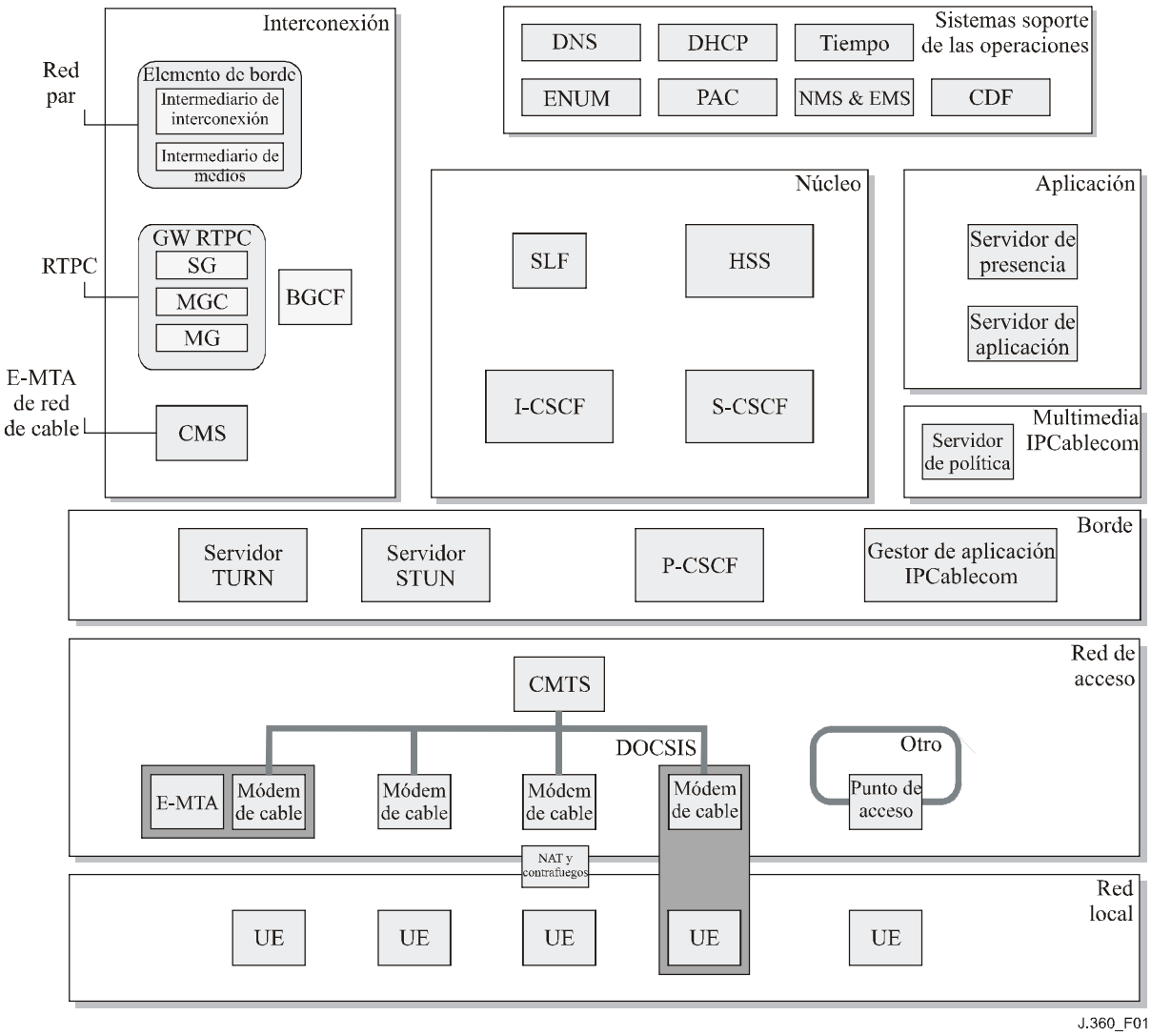


Figura 1 – Arquitectura de referencia de IPCablecom

Esta arquitectura proporciona una plataforma rica y modular sobre la que pueden construirse una gran diversidad de servicios de comunicaciones multimedia para un conjunto de equipos de usuario (UE). Obsérvese que la arquitectura de referencia describe varios casos de despliegue de UE (por ejemplo, UE tras el CM, una pasarela NAT y de barrera contrafuegos entre el UE y el CM). Estos casos de despliegue pretenden ilustrar el hecho de que los UE pueden desplegarse en entornos y configuraciones muy diversas. La arquitectura de referencia no proporciona un conjunto exhaustivo de escenarios de despliegue.

IPCablecom2 presupone un modelo de usuario compuesto por usuarios, identidades públicas, equipos de usuario y dispositivos. En el apéndice IV se describen las relaciones potenciales entre usuarios, identidades públicas, equipos de usuario y dispositivos. Por ejemplo, un usuario puede tener múltiples dispositivos equipos de usuario, cada uno de los cuales puede registrarse con una o más identidades públicas. Una identidad pública puede ser un número E.164 o puede ser un identificador alfanumérico que tiene sentido en el contexto de un servicio de telefonía SIP. Cada identidad pública está, en general, asociada con un usuario.

La arquitectura se divide en varias áreas lógicas o agrupaciones funcionales:

- Red local: la red local es la red que utiliza el equipo de usuario (UE) para conectarse a la red de acceso. Puede ser Ethernet, WiFi, Bluetooth o cualquier otra tecnología utilizada para establecer una red o conexión de equipos de usuario. Puede existir una pasarela NAT y

barrera contrafuegos entre la red local y la red de acceso. En algunos casos, el equipo de usuario puede incluir un componente de la red de acceso. En tales casos, la red local es una interfaz interna dentro del UE. Este es el caso de un UE que dispone de un módem de cable DOCSIS integrado.

Un UE incluye una aplicación basada en software o bien un dispositivo hardware donde se invocan, ejecutan o representan las características de servicio para el abonado. Todos los UE utilizan la misma infraestructura básica SIP para las comunicaciones basadas en IP en tiempo real y de servicios multimedia. Un UE de IPCablecom puede construirse modularmente e incluir varios niveles de funcionalidades en base a las capacidades que debe soportar. Por ejemplo, puede que un UE sólo soporte mensajería instantánea basada en texto y que, por tanto, no soporte códecs de audio o video Puede que exista un dispositivo NAT y barrera contrafuego (FW) entre un UE de una red local y la red de acceso. En tales casos, son necesarios mecanismos que permitan el tránsito de los NAT/FW de señalización y medios.

- Red de acceso: un UE puede residir o estar conectado a la red de acceso DOCSIS, o puede que obtenga los servicios de otras redes de acceso (incluyendo otras redes de acceso de cable que no estén bajo el control del operador de cable al que pertenezca la suscripción IPCablecom); esto es especialmente importante para un UE móvil, como por ejemplo una computadora portátil, un teléfono Wifi, etc. Cuando un equipo de usuario se encuentra en la red de acceso de cable, puede acceder a la QoS de la red de acceso interactuando con la infraestructura de señalización SIP de las redes de cable que, a su vez, interactúa con la infraestructura multimedia de IPCablecom a través del gestor de aplicación de IPCablecom y el servidor de política para reservar recursos de la red de acceso de cable.

  Los adaptadores de terminales multimedia integrados (E-MTA, *embedded-multimedia terminal adapter*) de IPCablecom están incluidos en el diagrama de referencia para que éste resulte más completo.

- Borde: esta agrupación funcional abarca puntos de referencia para los UE y la red de acceso. Un UE accede a la infraestructura SIP a través del intermediario de la función de control de sesión de llamada (P-CSCF *proxy-call session control function*). El P-CSCF actúa como intermediario (*proxy*) para los mensajes SIP entre el UE y el resto de la arquitectura, manteniendo asociaciones de seguridad con el UE. El P-CSCF puede solicitar recursos con QoS de la red de acceso al inicio de la sesión en nombre del UE a través del gestor de aplicación de IPCablecom. El gestor de aplicación de IPCablecom utiliza su interfaz con el servidor de política multimedia de IPCablecom, el cual facilita una política de calidad de servicio (QoS) para los componentes de la red de acceso de cable. Los servidores STUN y TURN definidos por el IETF se utilizan para permitir el acceso multimedia a través de dispositivos NAT y FW (el P-CSCF utiliza un servidor STUN diferenciado para la señalización de acceso a través de dispositivos NAT y FW). Los E-MTA de IPCablecom están servidos por sus respectivos CMTS tal como se describe en el Informe técnico de la arquitectura de IPCablecom 1.5 [UIT-T J.160].

- Núcleo: el núcleo contiene los componentes básicos requeridos para proporcionar servicios SIP y datos de abonados. Las agrupaciones funcionales del núcleo constan de los componentes funcionales siguientes: interrogador-CSCF (I-CSCF, *interrogating-CSCF*), servidor-CSCF (S-CSCF, *serving-CSCF*), función de localización de suscripción (SLF, *subscription locator function*), y servidor de abonado en la red origen (HSS, *home subscriber server*).

- EL I-CSCF es el punto de entrada inicial al núcleo para el protocolo SIP. El I-CSCF coopera con el HSS para determinar el S-CSCF que debe asignarse a una identidad pública y encamina las peticiones que genera un UE al S-CSCF asignado a la identidad pública del UE que realiza la petición. El I-CSCF también encamina peticiones SIP de terminación recibidas de la propia red o de redes externas. En este caso, el I-CSCF consulta al HSS para

determinar el S-CSCF que se ha asignado a la identidad pública de terminación y encamina la petición SIP a dicho S-CSCF para que sea procesada. El I-CSCF también permite el ocultamiento de la topología cuando la comunicación se establece con redes externas.

- El S-CSCF es responsable del procesamiento de la sesión SIP. Las llamadas o las sesiones de comunicación multimedia iniciadas con y desde identidades públicas se envían al S-CSCF asignado para autorización y procesamiento. El S-CSCF tiene facilidades de control de servicio que evalúan las peticiones SIP según criterios de filtrado predefinidos para cada abonado, o bien determina si la petición SIP debe ser encaminada a un servidor de aplicación para ser procesada. Ello permite una arquitectura extensible para la rápida introducción de nuevas características y servicios de valor añadido. El S-CSCF puede encaminar mensajes SIP hacia servidores de aplicación, servidores de presencia, otras CSCF o hacia funciones de control de pasarela de interconexión (BGCF, *breakout gateway control functions*), según proceda. El S-CSCF también incluye la función de registrador SIP que establece la correspondencia entre identidades públicas y sus direcciones de contacto SIP registradas, asigna URI de agente de usuario encaminable globalmente (GRUU, *globally routable user agent URI*), y almacena cualquier otro parámetro asociados con el registro, como por ejemplo, las capacidades de agente de usuario SIP. El S-CSCF obtiene los datos de suscripción del HSS.
- El HSS proporciona al S-CSCF y a servidores de aplicación el acceso a los perfiles de usuario y a otros datos de abonado. El HSS también mantiene la asignación de una identidad pública a un S-CSCF. Una suscripción puede asociarse a varias identidades públicas. Un HSS hace corresponder una suscripción a un S-CSCF, con lo que todas las entidades públicas serán asignadas al mismo HSS.
- Los S-CSCF y los servidores de aplicación pueden almacenar e l HSS ciertas clases de datos asociadas con suscripciones.
- La SLF se utiliza para localizar una instancia de HSS para una identidad dada cuando existen múltiples HSS.
- Aplicaciones: la agrupación funcional servidor de aplicación define servidores de aplicación que pueden ser invocados como parte del tratamiento de una petición originada o terminada en un S-CSCF para un usuario dado, o bien, pueden ser servidores autónomos que pueden invocarse y ser operados de forma independiente. El servidor de presencia es un servidor de aplicación especializado que contiene datos de presencia para identidades públicas. Los datos de presencia se obtienen de diversas fuentes en la red y permite conocer la voluntad y disponibilidad del usuario para comunicarse. El servidor de presencia también maneja el tratamiento de la privacidad y la autorización de suscripción de datos de presencia.
- Interconexión: la agrupación funcional interconexión permite establecer conexiones con otras redes. La interconexión con la RTPC es gestionada por la función de control de la pasarela de interconexión (BGCF, *breakout gateway control function*), que determina el controlador de pasarela de medios (MGC, *media gateway controller*) que debe utilizarse para la interconexión con la RTPC. El MGC controla las pasarelas de medios (MG) que proporcionan la capa de transporte y la interconexión de portadores con la RTPC. Las pasarelas de señalización (SG, *signalling gateways*) proporcionan la conectividad de la señalización por canal común N.º 7, SS7. Los MGC, SG y MG de IPCablecom se utilizan para la interconexión con la RTPC. La interconexión con redes pares que soporten el servicio de VoIP puede realizarse mediante un elemento de borde. El elemento de borde contiene la funcionalidad de intermediario de interconexión y, opcionalmente, la funcionalidad de intermediario de medios que pueden estar en plataformas separadas. El intermediario de interconexión puede llevar a cabo una serie de tareas, incluyendo el hacer cumplir el perfil del protocolo y la conversión de señalización, según sean necesarias para el interfuncionamiento con otras redes. La retransmisión de medios puede realizar dicha

tarea, es decir, retransmitir medios, con fines de ocultamiento de la topología. El CMS de IPCablecom está situado en la agrupación funcional de interconexión para indicar que los E-MTA que atiende pueden comunicarse con los UE.

- Sistemas de soporte operacional: proporcionan varias funciones, tales como la contabilidad y la provisión de UE. La CDF recopila mensajes de contabilidad procedentes de varios elementos, la DHCP ayuda en la distribución de direcciones IP a los UE, los ENUM y DNS ayudan a la resolución de URI y FQDN, los PAC y XDS soportan la provisión y configuración de las UE, y finalmente los EMS y NMS ayudan en las funciones de supervisión y de gestión.

Obsérvese que los componentes funcionales descritos anteriormente son funciones lógicas, que pueden combinarse en plataformas comunes.

5.3 Versiones y organización de IPCablecom

5.3.1 Versiones de IPCablecom

La arquitectura de IPCablecom sigue evolucionando conforme se añaden nuevas capacidades, de forma que actualmente se compone de varias versiones sucesivas.

- Versión 1.0 – Esta versión permite la aplicación de telefonía utilizando adaptadores de terminal multimedia integrados (E-MTA); está especificada en la versión inicial de las Recs. UIT-T J.160 a J.178.
- Versión 1.5 – Esta versión proporciona nuevas capacidades y añade SIP para la gestión de sesión en una red IPCablecom y entre redes IPCablecom; está especificada en las revisiones de las Recs. UIT-T J.160 a J.178.
- Multimedia – Esta versión diferencia calidades de servicio (QoS) y define una arquitectura genérica de QoS; está especificada en [UIT-T J.179].
- Versión 2 – Esta versión soporta puntos extremos basados en SIP y una plataforma de servicio basada en SIP que puede utilizarse para soportar diversos servicios.

En la figura 2 se ilustran las versiones de IPCablecom. Las aplicaciones que utilizan la plataforma de servicio SIP serán definidas en otras versiones autónomas y no se incluyen en la figura 2.

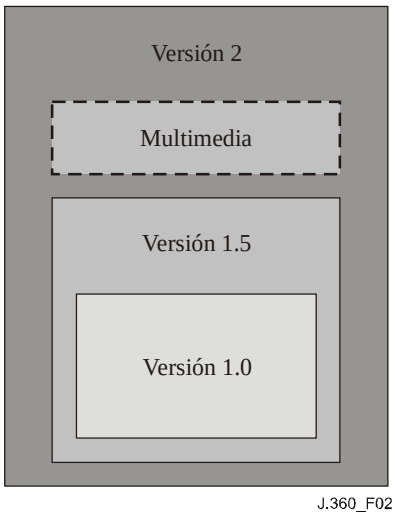


Figura 2 – Versiones de IPCablecom

5.3.2 Organización de IPCablecom

La organización de esta versión de IPCablecom2 se basa en la necesidad de la alineación con y ampliación de la especificación del IMS. En la figura 3 se ilustra al ámbito de la versión IPCablecom2.

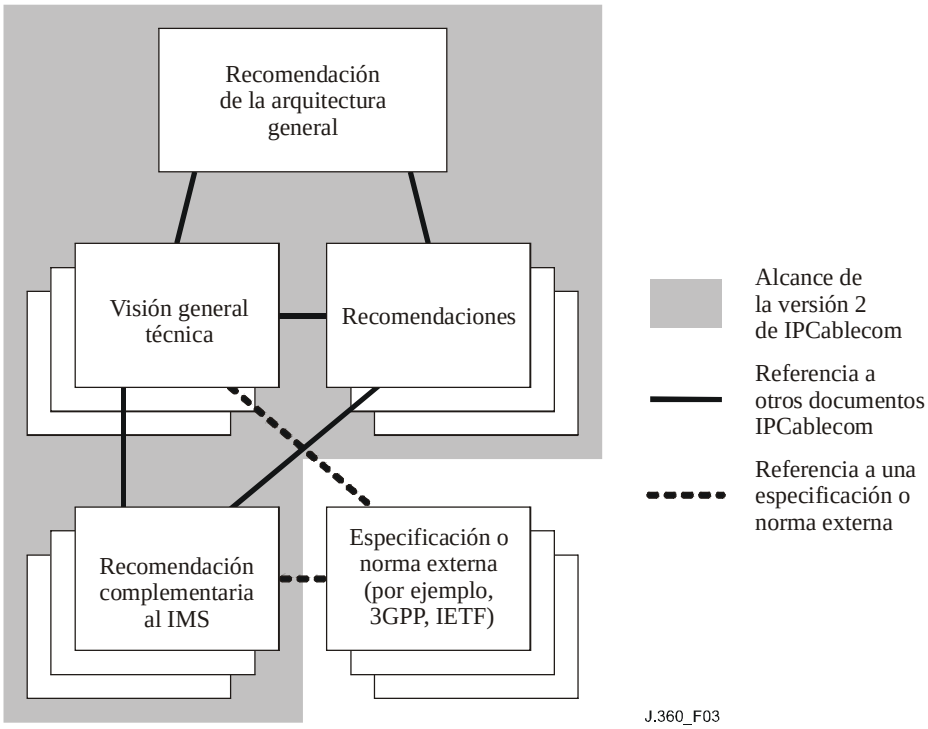


Figura 3 – Organización de IPCablecom2

En esta Recomendación se hace una descripción de alto nivel de la arquitectura de IPCablecom2. Las áreas funcionales individuales (por ejemplo, SIP, tránsito de NAT y FW, seguridad) se incluyen en apéndices específicos o en otras Recomendaciones. El objetivo de este documento es incluir los aspectos arquitectónicos y la utilización previsible del IMS en las redes de cable. Un documento puede ser una especificación si documenta requisitos normativos y define puntos de referencia específicos de IPCablecom, o si incluye un número reducido de modificaciones a una especificación del IMS (es decir, el número de cambios realizados a una especificación del IMS no es suficiente para justificar la elaboración de una especificación complementaria al IMS).

En algunos casos estos documentos no se basan en componentes arquitectónicos o puntos de referencia del IMS. Los documentos que están basados en el IMS simplemente hacen referencia a documentos IMS de la misma forma en que se referencian otros documentos de forma normativa. Las mejoras al IMS están incluidas en las especificación complementaria al IMS. Dichas especificaciones complementarias son especificación IMS que se han vuelto a publicar y que contienen cambios en base a requisitos específicos de las redes de cable. En función de la forma en que se organizan los documentos del IMS, una especificación complementaria (delta) al IMS puede incluir cambios que abarquen un conjunto de especificaciones o informes técnicos de IPCablecom. Por ejemplo, la especificación complementaria al IMS del 3GPP correspondiente a TS 24.229 contiene cambios en las áreas funcionales de SIP, tránsito de NAT y FW, seguridad y QoS.

El objetivo es introducir las mejoras de IPCablecom al IMS en las especificaciones del 3GPP. Conforme ello ocurra, las especificaciones complementarias al IMS se retirarán y serán sustituidas por referencias directas a las especificaciones del IMS del 3GPP.

El cuadro 1 incluye una lista de Recomendaciones.

Cuadro 1 – Recomendaciones relativas a IPCablecom2

Número de referencia de las Recomendaciones de IPCablecom2	**Nombre del documento**
J.360	Arquitectura general IPCablecom2 (esta Recomendación)
Apéndice I	Visión general de la señalización SIP de IPCablecom2
Apéndice II	Visión general de la calidad de servicio de IPCablecom2
Apéndice III	Visión general de la seguridad de IPCablecom2
Apéndice IV	Visión general del servidor de abonado en la red origen (HSS) de IPCablecom2
Apéndice V	Visión general del tránsito del NAT y de la barrera contrafuego de IPCablecom2
Apéndice VI	Visión general de la estrategia de utilización de IPv6 e IPv4 en IPCablecom2
Número de referencia de la Recomendación IPCablecom	**Nombre de la Recomendación**
J.362	Detección del punto de control de IPCablecom2
J.365	Interfaz del gestor de aplicación de IPCablecom2
J.364	Provisión, activación, configuración y gestión en IPCablecom2
J.361	Códec y medios de IPCablecom2
J.363	Recopilación de datos para contabilidad de IPCablecom2
Número de referencia de la especificación complementaria al IMS	**Nombre del documento**
J.366.0	Visión general de las recomendaciones complementarias al subsistema multimedia IP (IMS) de IPCablecom2
J.366.1	Especificación de la organización de datos de abonado de IPCablecom2 (3GPP TS 23.008)
J.366.2	Especificación de la etapa 2 del modelo de llamada multimedia IP de IPCablecom2 (3GPP TS 23.218)
J.366.3	Especificación de la etapa 2 del subsistema multimedia IP de IPCablecom2 (3GPP TS 23.228)
J.366.4	Especificación de la etapa 3 de SIP y SDP de IPCablecom2 (3GPP TS 24.229)
J.366.5	Especificación de las interfaces Cx y Dx de IPCablecom2 (3GPP TS 29.288)
J.366.6	Especificación de las interfaces Cx y Dx y del protocolo Diameter de IPCablecom2 (3GPP TS 29.229)
J.366.7	Especificación de la seguridad en el acceso para servicios basados en IP de IPCablecom2 (3GPP TS 33.203)
J.366.8	Especificación de la seguridad en el dominio de red de IPCablecom2 (3GPP TS 33.210)
J.366.9	Especificación de la arquitectura genérica de autenticación de IPCablecom2 (3GPP TS 33.220)

Tal como se describe en la cláusula 1.2, esta versión de IPCablecom2 define una arquitectura básica sobre la que pueden construirse las aplicaciones. En la medida en que dichas aplicaciones se apoyen en la arquitectura básica, serán independiente de la misma y se especificarán en versiones diferentes.

5.4 Consideraciones de diseño de IPCablecom2

Para permitir comunicaciones IP en tiempo real a través de la infraestructura de una red de cable, las especificaciones de IPCablecom2 definen requisitos técnicos y especifican puntos de referencia en las áreas siguientes:

- Señalización y control del servicio;
- Datos de abonado;
- Tránsito del elemento de traducción de dirección de red (NAT) y barrera contrafuegos;
- Calidad de servicio;
- Transporte y codificación de trenes de medios;
- Aprovisionamiento, activación, configuración y gestión;
- Contabilidad y utilización de la red;
- Seguridad;
- Interceptación legal.

5.4.1 Objetivos arquitectónicos genéricos

Los objetivos de diseño de la arquitectura de IPCablecom2 incluyen:

- Proporcionar una arquitectura independiente del servicio que permita añadir nuevos servicios sin que ellos afecte a la plataforma de control de servicios subyacente.
- Proporcionar una arquitectura modular en la que los componentes arquitectónicos puedan ser combinados de diversas formas para soportar una amplia gama de prestaciones. Por ejemplo, un equipo de usuario podría construirse mediante una combinación de bloques constructivos, tales como agentes de usuario SIP, puntos extremos de medios, oteadores de presencia y abonados de eventos.
- Soportar relaciones de muchos a muchos entre usuarios, dispositivos de puntos extremos y sesiones.
- Soportar una amplia variedad de UEs, incluyendo UE basados en software o en hardware, UE inteligentes, UE cableados o inalámbricos.
- Soportar el funcionamiento de IPv4 e IPv6.
- Soportar el interfuncionamiento con versiones anteriores de IPCablecom.
- Soportar movilidad del UE de forma que éste pueda acceder a servicios desde cualquier red de acceso, no solamente desde la red de acceso del operador de cable. En general, movilidad en el contexto de IPCablecom significa que el UE con conectividad IP pueda acceder a servicios de IPCablecom. Aunque es distinto del concepto de itinerancia desarrollado por el 3GPP (es decir, el P-CSCF puede estar en la red visitada), las mejoras introducidas para IPCablecom no deberían romper el modelo de itinerancia del 3GPP.
- Aprovechar las normas existentes y los protocolos abiertos siempre que ello sea posible. Esencialmente, adoptar la arquitectura IMS y definir las ampliaciones adicionales que sean necesarias.

5.4.2 Señalización y control del servicio

Los objetivos de la señalización y el control de servicios de IPCablecom2 incluyen:

- Permitir múltiples modelos de control de servicio. Estos modelos incluyen el control en el UE, el control en la red, y el control compartido. Cada aplicación específica de IPCablecom define el modelo de control del servicio.
- Permitir que los usuarios puedan establecer sesiones de comunicación con otros usuarios en la misma red, con usuarios en redes pares o con la RTPC.
- Permitir la presencia de UE no registrados para servicios de emergencia y la configuración del UE.

5.4.3 Datos de abonado

Los objetivos de diseño de los datos de abonado de IPCablecom2 incluyen:

- Definir una entidad lógica que sea el repositorio central de la información de usuario final o de suscripción necesaria para invocar o ejecutar servicios por las CSCF y los servidores de aplicación.
- Permitir el almacenamiento centralizado y distribución de datos permanentes y semi-permanentes.

5.4.4 Tránsito del traductor de dirección de puerto de red (NA(P)T, *network address and port translation*) y de la barrera contrafuego

Los objetivos de diseño del tránsito del NAT (NAT y NAPT se utilizan indistintamente) y de la barrera contrafuegos de IPCablecom2 incluyen:

- No imponer requisitos a los dispositivos NAT ni exigir que la red sea consciente de la presencia de un NAT.
- Permitir que existan varios equipos de usuario detrás de cada NAT.
- Permitir peticiones entrantes y salientes hacia y desde los UE a través de NATs.
- Mantener vinculaciones con varios P-CSCF para una entrega fiable de mensajes entrantes en caso de fallo de un P-CSCF.
- Soportar el tránsito de los NAT situados entre los UE y la red (NAT en red origen y NAT en red visitada).
- Ser independiente de la aplicación, es decir, la solución debería utilizar mecanismos que sean útiles para aplicaciones no basadas en SIP. No obstante, las soluciones implementadas pueden requerir soportar aplicaciones para utilizar los mecanismos definidos.
- Evitar trayectos de medios innecesariamente largos debido al retardo introducido en dichos medios.
- Poder restablecer las comunicaciones en situaciones de fallo (por ejemplo, cuando el dispositivo NAT debe re-arrancar y se pierden las vinculaciones).

5.4.5 Calidad de servicio

Los objetivos de diseño de calidad de servicio de IPCablecom2 incluyen:

- Aprovechar la especificación multimedia de IPCablecom a fin de proporcionar calidad de servicio (QoS) cuando un abonado accede al servicio a través de una red DOCSIS.
- Soportar el marcado y clasificación de paquetes en la red de acceso de forma que en el núcleo de red puedan utilizarse mecanismos de QoS tales como DiffServ (diferenciación de servicios).
- Proporcionar un mecanismo que no exija a las aplicaciones conocer la topología de la red de acceso.

5.4.6 Transporte y codificación de trenes de medios

Los objetivos de diseño del transporte de trenes de medios y codificación de IPCablecom2 incluyen:

- Minimizar los efectos del retardo, la pérdida de paquetes y la variación de fase en trenes de medios sensibles a dichos factores (por ejemplo, voz y video) a fin de asegurar un determinado nivel de calidad en los entornos objetivo (que incluyen la telefonía de audio/video, los trenes de video basados en IP y los sistemas inalámbricos).
- Definir un conjunto de códecs de video y audio y los protocolos de transmisión de medios asociados soportados.
- Incluir tecnologías de códecs de voz de banda estrecha y de banda ancha.
- Incluir tecnologías de códec de video emergentes para soportar aplicaciones tales como video telefonía, trenes de video IP, etc.
- Especificar los requisitos mínimos de compensación de eco y detección de activación por la voz.
- Soportar la transmisión transparente y libre de errores de la marcación multifrecuencia bitono (DTMF, *dual-tone multi frequency*).
- Soportar la transmisión facsímil, transmisión por módem, transmisión de DTMF y teletipo (TTY).
- Soportar el cálculo y la información de métricas sobre calidad de la voz.

5.4.7 Provisión, activación, configuración y gestión (PACM, *provisioning, activation, configuration, management*)

Los objetivos de diseño PACM de IPCablecom2 incluyen:

- Soportar modelos estáticos ligeros y modelos dinámicos de PACM, tanto para entornos controlados (red local de equipos de usuario bajo el control del proveedor de servicio) como no controlados (red local de equipos de usuario que no están bajo el control del proveedor de servicio).
- Soportar mecanismos de detección P-CSCF no basados en DHCP.
- Soportar un marco PACM de varios niveles para los UE, servicios y usuarios, permitiendo definiciones diferenciadas de PACM para cada nivel.
- Soportar métodos de mejora del software para los UE.
- Soportar múltiples modelos de funcionamiento (es decir, con marca y sin marca).

5.4.8 Contabilización y utilización de la red

Los objetivos de diseño de contabilidad y utilización de la red IPCablecom2 incluyen:

- Permitir contabilizar la utilización de la red y las actividades en tiempo real.

  En este caso, tiempo real hace referencia al momento en que los eventos se envían a un repositorio central y no al momento en que la factura final se pone a disposición del cliente, ni a cuando los eventos se envían para indicar una utilización incremental de recursos de la red (es decir, tarificación en línea).
- Permitir que varios elementos de red generen eventos que puedan estar correlados con una determinada sesión o abonado.
- Soportar la correlación entre eventos de contabilidad en los planos de señalización y de capacidad portadora.
- Facilitar la rápida introducción de nuevas prestaciones y servicios minimizando el impacto sobre otros elementos de red y la necesidad de señalizar información relacionada con el servicio y las prestaciones.

5.4.9 Seguridad

Los objetivos de diseño de seguridad de IPCablecom2 incluyen:

- Soportar mecanismos de confidencialidad, autenticación, integridad y control de acceso.
- Proteger la red frente a ataques de denegación de servicio, disrupción de red y ataques de apropiación indebida de servicios.
- Proteger los UE frente a ataques de denegación de servicio, vulnerabilidades de la seguridad y acceso no autorizado (desde la red).
- Soportar la privacidad del usuario final mediante la encriptación y mecanismos de control de acceso a datos de abonado, tales como información de presencia.
- Mecanismos de autenticación de UE, aprovisionamiento seguro, señalización segura, medios seguros y descarga de software segura.

5.4.10 Interceptación legal

Los objetivos de diseño de interceptación legal de IPCablecom2 incluyen:

- Soportar una arquitectura de interceptación independiente del servicio que no esté estrechamente ligada con las capacidades de servicio básicas de IPCablecom.
- Maximizar la transparencia de la vigilancia en la red.
- Garantizar que la arquitectura de vigilancia no limita el diseño de las aplicaciones.
- Permitir la interceptación de llamadas realizadas mediante NCS y SIP.

6 Componentes funcionales de IPCablecom

En esta cláusula se proporciona información adicional sobre cada una de las funciones presentes en la arquitectura de IPCablecom.

6.1 Red local

6.1.1 Equipo de usuario (UE, *user equipment*)

IPCablecom soporta clientes basados en señalización de llamada basada en red (NSC, *network-based call signalling*) para servicios de telefonía. El sistema multimedia de IPCablecom proporciona un marco de calidad de servicio (QoS) y contabilidad agnósticos respecto a los servicios. IPCablecom2 soporta clientes basados en SIP con diversas capacidades, como por ejemplo, teléfonos hardware y software, teléfonos inteligentes, teléfonos alámbricos e inalámbricos, equipos de usuario de mensajería instantánea, terminales de comunicaciones de video, etc. En coherencia con el IMS, los clientes de IPCablecom se denominan equipos de usuario (UE). Todos los equipos de usuario descritos anteriormente utilizan la misma infraestructura básica para disponer de servicios multimedia. Los equipos de usuario pueden ser dispositivos fijos o móviles, como computadoras portátiles o teléfonos con capacidad WiFi. Pueden residir en la red de acceso de cable, o pueden acceder a servicios de otras redes de acceso. Cuando los equipos de usuario se encuentran en la red de acceso de cable, pueden conseguir una QoS determinada en dicha red de acceso interactuando con la infraestructura de señalización, que a su vez interactúa con el servidor de política multimedia de IPCablecom.

6.1.2 NAT y barrera contrafuegos

Entre la red local y la red de acceso puede existir un NA(P)T (Traductor de dirección de red y de puerto) y una barrera contrafuegos. Puesto que un NAT puede modificar las direcciones y puertos IP, y una barrera contrafuegos restringe el acceso, los planos de señalización y de capacidad portadora han de comportarse de manera diferente cuando dichos elementos se insertan entre el UE y el P-CSCF.

6.2 Red de acceso

El UE se conecta al borde de red a través de la red de acceso de cable o a través de otras redes de acceso disponibles (por ejemplo, puntos de acceso públicos WiFi, red de datos celular 3G). Los elementos de la red de acceso proporcionan la conectividad IP y los recursos de QoS necesarios para que el UE utilice los servicios de IPCablecom.

6.2.1 Módem de cable (CM)

El módem de cable (CM, *cable modem*) es el equipo en domicilio de cliente (CPE) utilizado conjuntamente con el CMTS para proporcionar el servicio de acceso a internet de banda ancha. Un E-MTA (adaptador de terminal multimedia integrado) es un cliente basado en NCS de IPCablecom que incluye un módem de cable integrado. Aunque el E-MTA no establece comunicación directa con la red, es importante señalar que a través del mismo CM pueden establecerse servicios de telefonía basada en NCS y basada en SIP.

6.2.2 Sistema de terminación del módem de cable (CMTS)

El CMTS reside en la cabecera del operador de cable, y se utiliza conjuntamente con el CM para proporcionar el servicio de acceso a internet de banda ancha. A partir de la Rec. UIT-T J.112, DOCSIS ha definido la forma de proporcionar QoS en la red de acceso. IPCablecom multimedia definen la forma en que los servicios basados en IP pueden solicitar una QoS dada a la red DOCSIS. En IPCablecom se define cómo puede proporcionarse QoS a servicios SIP a través de IPCablecom multimedia y DOCSIS.

6.2.3 Punto de acceso

IPCablecom puede utilizarse para ofrecer servicio a UEs con conectividad IP a través de otros tipos de redes de acceso.

6.3 Borde

6.3.1 Intermediario de la función de control de sesión de llamada (P-CSCF)

Un UE accede a la infraestructura SIP a través de un P-CSCF (*proxy-call session control function*). El P-CSCF aísla la red SIP de las peculiaridades del protocolo específico de la red de acceso y permite el crecimiento de la infraestructura, asumiendo en su interacción con el UE determinadas tareas que hacen un uso intensivo de recursos. También representa los límites confiables para SIP entre partes no confiables de la red (red de acceso, red local) y partes confiables de la red (núcleo, aplicación, interconexión, sistemas de soporte operacional). Un P-CSCF realiza las funciones siguientes:

- Encaminar mensajes SIP desde el UE al I-CSCF o S-CSCF y viceversa.
- Mantener asociaciones de seguridad entre sí mismo y el UE, y confirmar la identidad de las identidades públicas autenticadas.
- Interactuar con el gestor de aplicación de IPCablecom para la gestión de la QoS.
- Proporcionar la funcionalidad que permita al UE atravesar los NAT y mantener vinculaciones de NAT para la señalización SIP.
- Generar identificadores (ID) de correlación de contabilidad y eventos de contabilidad.

6.3.2 Servidores STUN y TURN

Un servidor STUN es una entidad que recibe peticiones STUN y envía respuestas STUN. Las peticiones STUN son peticiones típicamente vinculantes que se utilizan para determinar las vinculaciones asignadas por los NAT. El UE envía una petición de vinculación al servidor sobre UDP. El servidor examina la dirección IP y el puerto origen de la petición y los copia en la respuesta que devuelve al UE.

La red IPCablecom utiliza dos servidores STUN, uno como componente funcional del P-CSCF (que no se muestra en la figura 1) y otro como servidor STUN autónomo:

- El servidor STUN componente funcional del P-CSCF es utilizado por los equipos de usuario SIP a fin de mantener las vinculaciones NAT para señalización. Estos mensajes STUN también pueden actuar como indicadores de supervivencia, permitiendo al UE determinar la disponibilidad del P-CSCF y detectar rearranques de los NAT.
- El servidor STUN externo que se muestra en la figura 1 se utiliza para determinar una de las posibles direcciones de medios candidatas que están utilizando el protocolo STUN.

Además de los servidores STUN, la arquitectura también incluye un servidor TURN. Un servidor TURN es una entidad que recibe peticiones TURN y envía respuestas TURN. Este servidor puede actuar como elemento de retransmisión de datos, recibiendo datos en la dirección que facilita a los UE y transmitiéndolos a los UE. Esta funcionalidad de retransmisión de datos permite que los medios transiten los NAT cuando otras técnicas de tránsito de NAT son insuficientes.

6.3.3 Gestor de aplicación de IPCablecom

El gestor de aplicación de IPCablecom es responsable de una serie de tareas. Resulta especialmente importante la determinación de los recursos necesarios para ofrecer QoS a una sesión en base a los descriptores de sesión recibidos y gestionar los recursos de QoS asignados a una sesión.

Determinar los recursos de QoS para una sesión implica interpretar el descriptor de sesión y calcular la anchura de banda necesaria, determinar el tipo de programación de tráfico y rellenar los clasificadores de tráfico. También implica determinar el número de flujos necesarios para la sesión (sólo voz o voz y vídeo) y gestionar la asociación entre flujos y sesión.

6.4 Núcleo

6.4.1 Servidor de CSCF (S-CSCF)

Todos los mensajes SIP al margen del diálogo hacia y desde un abonado pasan a través del S-CSCF que atiende a dicho abonado. A alto nivel, el S-CSCF soporta las capacidades siguientes:

- Función de registrador SIP, que proporciona una base de datos que vincula dinámicamente identidades públicas registradas (AOR) a un conjunto de direcciones de contacto, asigna GRUUs, y almacena cualesquiera otros parámetros asociados con el registro, por ejemplo, capacidades del agente de usuario y la dirección o direcciones del P-CSCF que pueden utilizarse para alcanzar los contactos.
- Autenticación y autorización del usuario SIP.
- Selección de servicio y filtrado.
- Encaminamiento de mensajes al P-CSCF de los UE servidos por el S-CSCF.
- Encaminamiento de mensajes a un I-CSCF para identidades de usuario públicas no servidas por el S-CSCF.
- Encaminamiento de mensajes a una BGCF para llamadas a la RTPC.
- Procesado en origen: procesado de peticiones entrantes de inicio de diálogo procedentes de agentes de usuario (UA) SIP incluidos en UE o en servidores de aplicación servidos por el S-CSCF.
- Procesado en terminación: procesado de peticiones salientes SIP que terminan en una identidad pública servida por el S-CSCF. Ello incluye soportar la bifurcación de mensajes SIP cuando con dicha identidad pública se registran varias direcciones de contacto.
- Consultas de encaminamiento externo a bases de datos tales como ENUM para determinar el encaminamiento de la llamada.

- Liberación de sesiones iniciada por la red.
- Generación de eventos de contabilidad.

En el núcleo pueden existir varios S-CSCF. En un instante dado, una suscripción (y todas las identidades públicas asociadas al mismo) solo puede ser gestionada a través de un único S-CSCF.

Los abonados están asociados con S-CSCFs. Los datos de suscripción se almacenan en uno o más servidores de abonado en la red origen (HSS, *home subscriber servers*). El S-CSCF interactúa con la SLF para identificar los HSS relevantes para obtener datos de los usuarios a los que sirve. El S-CSCF también puede interactuar con el HSS para almacenar ciertos tipos de datos de los usuarios que sirve.

Los puntos extremos y el S-CSCF soportan a los GRUU. Ello permite asignar un GRUU a puntos extremos durante el proceso de registro, permitiendo así a los puntos extremos iniciar una petición con un contacto específico en lugar de un AOR. Ello es importante para determinadas prestaciones tales como la transferencia de llamada y la conferencia.

6.4.2 Interrogador de CSCF (I-CSCF)

El I-CSCF permite:

- La interacción con el HSS para determinar la vinculación entre una suscripción (y las identidades públicas asociadas) y un S-CSCF.
- Las consultas al HSS para obtener el S-CSCF y encaminar las peticiones SIP desde otro operador de red al S-CSCF correcto.
- Encaminar mensajes a los servidores de aplicación (AS) utilizando identidades de servicio públicas (PSI, *public service identities*).
- Encaminar mensajes a un elemento de borde para una relación entre pares de VoIP.

6.4.3 Servidor de abonado en la red origen (HSS, *home subscriber server*)

El HSS es responsable de almacenar la siguiente información relativa a las suscripciones:

- La asociación entre abonado y S-CSCF.
- Información del perfil de la suscripción (criterios de filtrado).
- Información de seguridad de la suscripción.
- Datos transparentes u opacos para ser utilizados por servidores de aplicación.

El HSS proporciona a los componentes de la red el almacenamiento, la recuperación y el procesamiento de la información. Soporta las capacidades siguientes:

- Establecimiento de sesión – El HSS soporta los procedimientos de establecimiento de sesión. Para la terminación de tráfico proporciona información sobre cuál es el S-CSCF asignado para manejar una identidad pública.
- Seguridad – El HSS soporta varios esquemas de autenticación almacenando datos relacionados con la seguridad y proporcionando dichos datos de seguridad según sea necesario para soportar procedimientos de seguridad de los UE.
- Provisión de servicio – El HSS proporciona acceso a los datos del perfil del servicio para ser utilizados por el S-CSCF. El HSS también puede almacenar datos específicos de la aplicación para el servidor de aplicación.

6.4.4 Función de localización de la suscripción (SLF, *subscription locator function*)

La SLF proporciona el nombre del HSS que contiene los datos específicos de abonado requeridos. La SLF no es necesaria en el entorno de un HSS individual.

6.5 Multimedia de IPCablecom

IPCablecom multimedia define una plataforma basada en IP para la distribución de servicios multimedia con calidad de servicio mejorada utilizando redes de acceso DOCSIS 1.1 (este documento utiliza DOCSIS y asume DOCSIS 1.1 o superior). Esta plataforma permite que las capacidades del núcleo de IPCablecom (por ejemplo, autorización de QoS y control de admisión, mensajes de eventos para facturación y otras funciones de apoyo interno y de seguridad) soporten una amplia gama de servicios IP adicionales a la telefonía. Es decir, mientras que el CMS de IPCablecom está hecho a medida de los servicios telefónicos residenciales, los componentes multimedia de IPCablecom ofrecen una plataforma de propósito general para que los operadores de cable ofrezcan una amplia variedad de servicios multimedia IP que requieren un trato con QoS.

La arquitectura multimedia de IPCablecom define la interacción entre un CMTS, un servidor de política y un gestor de aplicación. El CMTS se incluye como parte de la red de acceso y se describe en la cláusula 6.2.2. El gestor de aplicación es específico de cada operación. IPCablecom define un gestor de aplicación que se describe en la cláusula 6.3.3. El servidor de política, que es un elemento multimedia singular de IPCablecom que puede comunicarse con diversos gestores de aplicación, se describe más adelante.

6.5.1 Servidor de política

El servidor de política actúa principalmente como intermediario entre el gestor o gestores de aplicación y el o los CMTS. Aplica políticas de red a las peticiones del gestor de aplicación y a los mensajes de intermediario entre el gestor de aplicación y el CMTS.

6.6 Aplicación

6.6.1 Servidor de aplicación (AS, *application server*)

Un servidor de aplicación (AS, *application server*) proporciona servicios específicos de la aplicación. Un AS puede influir sobre una sesión SIP en función de los servicios que soporta, pudendo también dar cabida y ejecutar servicios. Un AS puede iniciar o terminar servicios en nombre del usuario.

6.6.2 Servidor de presencia

El servidor de presencia es un servidor de aplicación especializado. Actúa como punto central para la conexión de fuentes de información de presencia y partes interesadas.

El servidor de presencia puede obtener información de presencia en múltiples formas, por ejemplo:

- Utilizando el método PUBLISH de SIP: la petición PUBLISH se dirige a una identidad pública y el S-CSCF la transmite al servidor de presencia de conformidad con reglas de encaminamiento normales.
- Utilizando el método SUBSCRIBE de SIP: el servidor de presencia también puede actuar como observador, utilizando el método SUBSCRIBE de SIP para suscribirse a información de presencia donde quiera que esté disponible, por ejemplo, de un registrador.

Las suscripciones de presencia de observadores se dirigen a identidades públicas y son entregadas por el S-CSCF al servidor de presencia. El servidor de presencia gestiona el diálogo para cada suscripción, y envía un mensaje NOTIFY de SIP al observador u observadores cada vez que hay un cambio en el estado de presencia a la que el observador está suscrito y autorizado.

6.7 Interconexión

6.7.1 Elemento de borde

La interconexión con redes pares pueden realizarse a través de un elemento de borde. El elemento de borde contiene una función de intermediario de interconexión y puede contener una función de intermediario de medios.

Las funcionalidades de intermediario de interconexión incluyen:

- interfuncionamiento de protocolos;
- aplicación obligada del perfil SIP (traducción, adaptación o normalización);
- servicios relacionados con la seguridad (por ejemplo, mantenimiento de una asociación de seguridad con la red par);
- gestión de direcciones IP (redes pares con el mismo espacio de direcciones IP privadas);
- interfuncionamiento entre redes IPv6 e IPv4;
- los intermediarios de medios intercambian medios entre redes pares.

IPCablecom no define requisitos funcionales específicos que deban ser soportados por los elementos de borde. En lugar de ello, cada operador puede determinar la necesidad y los requisitos exigibles a un elemento de borde.

6.7.2 Función de control de la pasarela de interconexión (BGCF, *breakout gateway control function*)

La BGCF permite la selección de la red para el encaminamiento a la RTPC, determinando cuál es el MGC de su red que ha de utilizarse para la conexión con la RTPC.

6.7.3 Pasarela con la red telefónica pública conmutada (GW RTPC, *gateway RTPC*)

La pasarela con la RTPC consta de la pasarela de señalización (SG), el controlador de pasarela de medios (MGC) y la pasarela de medios (MG). Los SG, MGC y MG se definen en versiones previas de IPCablecom y son reutilizados en esta versión de IPCablecom, con la adición de un punto de referencia de IPCablecom con el MGC. Los SG, MGC y MG son componentes lógicos que pueden implementarse en plataformas diferenciadas o que pueden estar incluidos en una única plataforma.

La SG realiza la conversión de señalización en una capa de transporte entre el transporte basado en SS7 y el transporte IP utilizado en la red IPCablecom. La SG no interpreta la capa de aplicación, sino que interpreta las capas necesarias para los mensajes de señalización de encaminamiento.

El MGC realiza la conversión de protocolo entre los mensajes PUSI del SS7 y los protocolos de control de llamadas de IPCablecom, y proporciona el control de la conexión de los canales de medios en la MG.

La MG proporciona la conversión del canal portador entre la red de conmutación de circuitos y los trenes de medios RTP IP de la red IPCablecom. La MG puede introducir códecs y compensadores de eco, etc.., según sea necesario para las conversiones de canales portadores.

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

Un servidor de gestión de llamadas de IPCablecom (CMS) soporta los servicios de telefonía para clientes NCS (es decir, los E-MTA). El CMS proporciona la mayor parte de las funcionalidades de la telefonía e interactúa con los servidores de aplicación (por ejemplo, servidores de mensajería unificada y servidores de conferencia) para aplicaciones adicionales a los E-MTA. Puede no disponer de características para el funcionamiento transparente a través de los E-MTA y los equipos de usuario (UE) propiedad del mismo usuario.

El CMS de IPCablecom se comunica con la CSCF como un par de la misma.

6.8 Sistemas de soporte de las operaciones

Es previsible que los servidores siguientes formen parte del sistema de soporte de las operaciones de la red IPCablecom.

6.8.1 Servidor del protocolo de configuración dinámica de anfitrión (DHCP, *dynamic host configuration protocol*)

El servidor DHCP se utiliza cuando la red local del UE está bajo el control del proveedor de servicios. Éste proporciona información sobre la participación en la red IP (por ejemplo, la dirección IP y la información del servidor DNS). Es posible que los UE situados en entornos que no estén bajo el control del proveedor de servicio no puedan utilizar los servicios del servidor DHCP del proveedor de servicio. En tales casos, se asume que el UE recibe de la red local la información sobre la participación en la red IP.

6.8.2 Servidor del sistema de nombres de dominio (DNS, *domain name system*)

El servidor DNS se utiliza para resolver entidades DNS (por ejemplo, FQDNs, registros SRV) en direcciones de red y viceversa. Es previsible que los UE y otros componentes de red similares utilicen un servicio DNS del proveedor de servicio para localizar entidades o para el encaminamiento de mensajes.

6.8.3 Servidor ENUM

El servidor ENUM se utiliza para almacenar y traducir números E.164 en URIs SIP o en registros de servidores de nombres (NS, *name server*) que apuntan al servidor de nombres del operador que tiene la delegación del número E.164 en particular. Más específicamente, un servidor ENUM utiliza el DNS para identificar al propietario (proveedor de servicio o usuario final) de un número E.164.

6.8.4 Elemento de provisión, activación y configuración (PAC, *provisioning, activation, and configuration)*

El elemento PAC es un componente definido por IPCablecom responsable de la provisión, activación y configuración de los UE. Es responsable de mantener información de la configuración del UE. Los datos de configuración contienen la información necesaria para que un UE pueda ofrecer servicios. Asimismo también es el elemento que transporta cambios de la configuración del tiempo de ejecución desde la red al usuario o viceversa.

El elemento PAC contiene los componentes lógicos servidor de entrega de perfil (PDS, *profile delivery server*) y servidor de datos XCAP (XDS, *XCAP data server*) e implementa los puntos de referencia asociados.

- Un PDS es el conjunto lógico formado por el notificador y el servidor responsable de manejar las peticiones de suscripción de configuración.
- Un XDS es un servidor XCAP que almacena, modifica y recupera datos entre UEs y elementos de red, o entre elementos de red.

6.8.5 Sistemas de gestión de elemento y de gestión de red

Un sistema de gestión de elemento (EMS, *element management system*) o un sistema de gestión de red (NMS, *network management system*) está relacionado con una o más entidades asociadas con la supervisión y gestión de elementos de red específicos o de toda una red, respectivamente.

Aunque los EMS pueden tener funcionalidades diferentes y ser diferentes para los distintos elementos de red, normalmente tienen interfaces con los NMS responsables del seguimiento y mantenimiento del buen estado de la red.

Los EMS y los NMS requieren disponer de puntos de referencia de gestión con varios elementos (por ejemplo, UE, PAC, servidores de aplicaciones, S-CSCF). IPCablecom sólo define puntos de referencia de supervisión y de gestión para equipos de usuario (UE).

6.8.6 Servidor de tiempo

Los UE utilizan un servidor de tiempo para obtener la hora.

6.8.7 Función de datos de tarificación (CDF, *charging data function)*

La función de datos de tarificación (CDF, *charging data function*) recibe eventos de tarificación de varios elementos de red de IPCablecom a través del punto de referencia Rf definido en el IMS. Puede utilizar la información contenida en los eventos de tarificación utilizados para elaborar registros detallados de llamada (CDR, *call detail records*).

Algunos elementos de IPCablecom entregan mensajes de eventos definidos en IPCablecom (EM, *event messages*) a un servidor de mantenimiento de registros (RKS, *record keeping server*). El RKS puede utilizarse para soportar un CMS, CMTS, MGC y un servidor de política. No obstante, el RKS no se incluye en la arquitectura de referencia.

7 Interfaces de protocolo y puntos de referencia

IPCablecom2 define un conjunto de interfaces de protocolo, o puntos de referencia, en una serie de áreas. Muchos de dichos puntos de referencia están directamente extraídos del IMS, habiéndose incorporado a los mismos las modificaciones y mejoras necesarias. Algunos de los puntos de referencia se han definido expresamente para IPCablecom2. Estos puntos de referencia se identifican mediante los respectivos convenios de denominación:

- IMS: dos o tres letras (por ejemplo, Gm, ISC)
- Puntos de referencia definidos por IPCablecom2: pkt-<área funcional>-<número del punto de referencia>.

Para una descripción más completa y la definición del protocolo véanse los informes técnicos (TR) y las especificaciones relevantes.

Es posible que algunos de dichos puntos de referencia no existan en implementaciones concretas de algún vendedor. Por ejemplo, si varios componentes funcionales IPCablecom2 están integrados, es posible que algunos de los puntos de referencia sean internos al dispositivo integrado.

7.1 Señalización y control del servicio

En la figura 4 se ilustran los puntos de referencia de señalización y de control de servicio de IPCablecom2. La mayor parte de los puntos de referencia se han definido en el IMS, habiéndose incorporado las variaciones necesarias para IPCablecom, tal como se ha identificado en diversas especificaciones de IPCablecom. También se incluyen puntos de referencia específicos de IPCablecom.

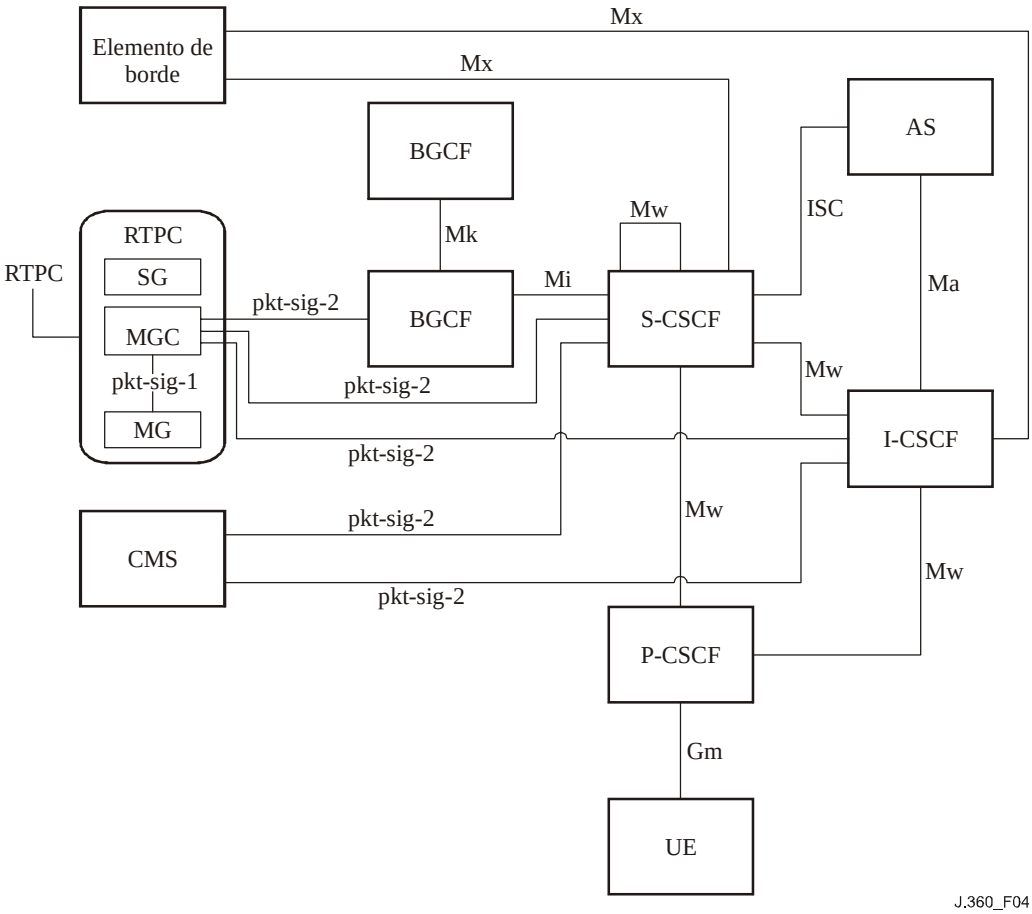


Figura 4 – Puntos de referencia de la señalización

En el cuadro 2 se describen los puntos de referencia identificados en la figura 4. Todos los puntos de referencia están basados en SIP, salvo que se indique lo contrario.

Cuadro 2 – Descripción de los puntos de referencia de la señalización

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
Mx	I-CSCF – Elemento de borde S-CSCF – Elemento de borde	Permite que un S-CSCF o un I-CSCF se comunique con un elemento de borde cuando interfunciona con otra red. Por ejemplo, una sesión entre la red origen y una red par puede ser encaminada a través de una función ALG del IMS situada dentro del elemento de borde para permitir el interfuncionamiento entre redes SIP con IPv6 y con IPv4.
Mi	S-CSCF – BGCF	Permite que el S-CSCF envíe la señalización de sesión a la BGCF para el interfuncionamiento con redes RTPC.
Mk	BGCF – BGCF	Permite que una BGCF envíe la señalización de sesión a otra BGCF.
Mw	P-CSCF – I-CSCF P-CSCF – S-CSCF I-CSCF – S-CSCF S-CSCF – S-CSCF	Permite que la comunicación y envío de mensajes de señalización entre las CSCF para el registro y control de sesión. También permite que el CMS intercambie mensajes SIP con el S-CSCF y I-CSCF para llamadas entre los E-MTA y los UE.
Ma	I-CSCF – AS	Permite que el I-CSCF envíe peticiones SIP destinadas a una identidad de servicio pública alojada en un servidor de aplicación (AS) directamente a dicho servidor de aplicación.
ISC	S-CSCF – AS	Permite que un S-CSCF se comunique con un servidor de aplicación (AS) para soportar varias aplicaciones.
Gm	UE – P-CSCF	Permite que un UE se comunique con el P-CSCF para registro y control de sesión.
pkt-sig-1	MGC – MG	El protocolo de control de pasarela troncal (TGCP, trunking gateway control protocol) presenta una interfaz tal como la definida en la especificación TGCP de IPCablecom [UIT-T J.171.1].
pkt-sig-2	CMS – S-CSCF CMS – I-CSCF MGC – BGCF MGC – S-CSCF MGC – I-CSCF	Protocolo CMSS, tal como se define en la especificación de señalización de CMS a CMS de IPCablecom [UIT-T J.178]. Permite al E-MTA de IPCablecom establecer sesiones de voz con elementos de IPCablecom. También permite que los BGCF, I-CSCF, y S-CSCF intercambien señalización de sesión con un MGC de IPCablecom para el interfuncionamiento con la RTPC.

Para más información, véase la visión general de la señalización SIP de IPCablecom2 (apéndice I).

7.2 Datos de abonado

Los datos de abonado de IPCablecom se almacenan en el HSS situado en la red origen. El HSS sirve al S-CSCF, al I-CSCF, y a varios servidores de aplicaciones, incluyendo el servidor de presencia. Mediante una consulta a la SLF se localiza el HSS adecuado para un abonado dado.

En la figura 5 se ilustra los puntos de referencia relacionados con los servicios de datos del abonado.

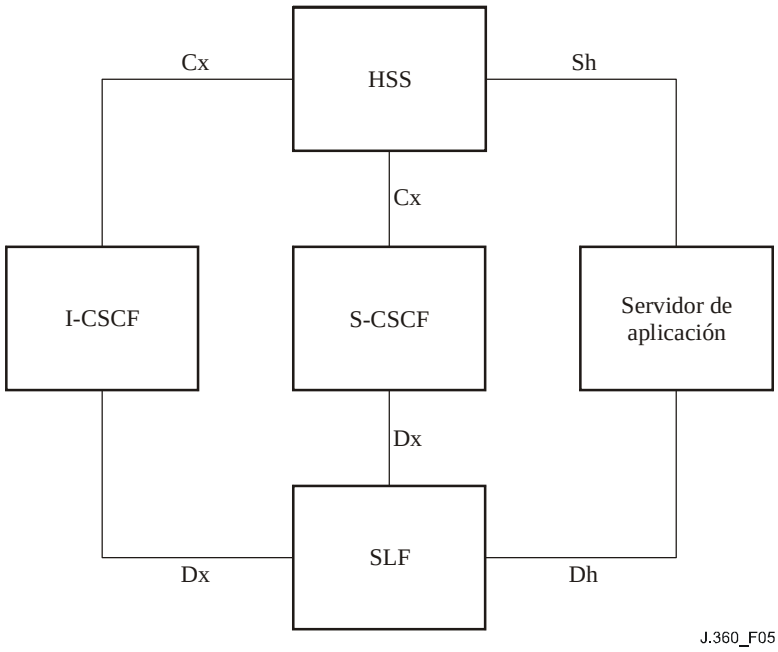


Figura 5 – Puntos de referencia de los datos de abonado

En el cuadro 3 se describen los puntos de referencia de la figura 5.

Cuadro 3 – Descripción de los puntos de referencia de los datos de abonado

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
Cx	I-CSCF – HSS S-CSCF – HSS	Permite que un I-CSCF y un S-CSCF busquen en el HSS información relativa al encaminamiento, autorización y autenticación, perfil del abonado y asignación de S-CSCF.
Sh	AS – HSS	Permite que un servidor de aplicación (AS) se comunique con el HSS para soportar diversas aplicaciones.
Dx	I-CSCF – SLF S-CSCF – SLF	Permite que un I-CSCF y un S-CSCF busquen la dirección del HSS que almacena los datos de suscripción de un usuario dado. Este punto de referencia no es necesario en un entorno con un único HSS.
Dh	AS – SLF	Permite que un AS busque la dirección del HSS que tiene los datos de la suscripción de un usuario dado. Este punto de referencia no es necesario en un entorno con un único HSS.

Para más información véase la visión general del HSS IPCablecom (apéndice IV).

7.3 Calidad de servicio

El enfoque de calidad de servicio (QoS) de IPCablecom2 se basa en el IPCablecom multimedia. En la arquitectura original de IPCablecom multimedia, todas las funciones del dominio de control del servicio estaban agrupadas en una única entidad denominada gestor de aplicación (AM, *application manager*), del que podían existir múltiples instancias. La arquitectura de IPCablecom2 convierte dicho dominio en nuevos elementos discretos con puntos de referencia definidos. Al objetos de proveer calidad de servicio, un gestor de aplicación (AM) sirve como interfaz entre la arquitectura IPCablecom SIP y la arquitectura IPCablecom multimedia. Su función es recibir mensajes de QoS

desde el P-CSCF y formular los mensajes adecuados al servidor de política de IPCablecom multimedia. Si bien dicha función de gestor de aplicación puede estar integrada en un servidor de política de IPCablecom multimedia, debe considerarse una función diferenciada puesto que tiene requisitos singulares y diferentes de los del servidor de política, tal como la resolución de una única sesión basada en una petición con QoS en un conjunto de peticiones individuales con QoS para cada flujo IP. La versión IPCablecom del gestor de aplicación es el gestor de aplicación de IPCablecom (PAM, *IPCablecom application manager*).

En la figura 6 se ilustra la relación entre el gestor de aplicación, el P-CSCF y el servidor de política de IPCablecom multimedia. Obsérvese también que el gestor de aplicación que aquí se muestra como una función diferente, puede estar incluido junto con el servidor de política multimedia de IPCablecom o, alternativamente, con un P-CSCF.

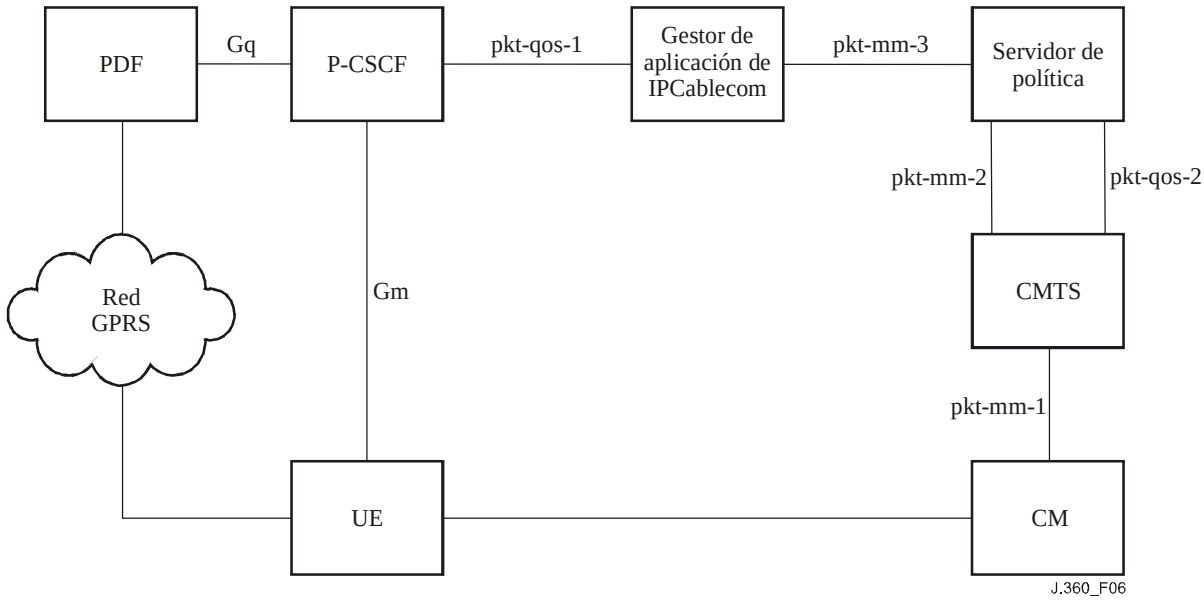


Figura 6 – Puntos de referencia de QoS

Tal como se ilustra en la figura 6, la función gestor de aplicación (AM) proporciona la correspondencia entre los requisitos de QoS de la sesión o diálogo, de conformidad con la señalización SIP, y el estado de QoS de cada uno de los flujos de servicio IP asociados de la red de acceso de cable.

En el cuadro 4 se describen los puntos de referencia de la figura 6.

Cuadro 4 – Descripción de los puntos de referencia de QoS

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
Gm	UE – P-CSCF	Véase el cuadro 2.
pkt-qos-1	P-CSCF – Gestor de aplicación	Esta es la interfaz del servicio web de IPCablecom multimedia, que permite que el P-CSCF haga peticiones de servicio con QoS al gestor de aplicación, que, a su vez, hace corresponder dichas peticiones con peticiones de política a través del punto de referencia pkt-mm-3. Las peticiones de servicio con una QoS las obtiene el P-CSCF a partir de los mensajes SIP que transportan las descripciones de sesión adecuadas. Este punto de referencia se define en la especificación de la interfaz de gestión de aplicación [UIT-T J.365].
pkt-qos-2	Servidor de política – CMTS	El servidor de política utiliza el protocolo de descubrimiento de puntos de control [UIT-T J.362] para determinar el CMTS servidor en la red para un UE dado.
pkt-mm-1	CM – CMTS	El CMTS ordena al CM que establezca, deshaga o modifique un flujo de servicio DOCSIS mediante señalización DSx. Este punto de referencia se define en IPCablecom multimedia [UIT-T J.179 Ap.I].
pkt-mm-2	Servidor de política – CMTS	El servidor de política envía las decisiones sobre la política al CMTS que, a su vez, proporciona respuestas a las mismas. Este punto de referencia se define en IPCablecom multimedia [UIT-T J.179 Ap.I].
pkt-mm-3	Gestor de aplicación – Servidor de política	Permite que el gestor de aplicación solicite al servidor de política que instale decisiones de política en el CMTS. Este punto de referencia se define en el IPCablecom multimedia [UIT-T J.179 Ap.I].

Para más información véase la visión general de QoS de IPCablecom2 (apéndice II).

7.4 Tránsito del traductor de direcciones de red (NAT, *network address translation*) y de la barrera contrafuegos

Los traductores de direcciones de red (NAT, *network address translator*) manipulan la información de dirección y del puerto incluida en la cabecera IP y de transporte. Ello genera un desafío a los equipos de usuario (UE) que se comunican entre sí mediante SIP:

- El UE anuncia las direcciones requeridas para las comunicaciones de medios en la señalización SIP (es decir, SDP). Sin embargo, la dirección local del UE situado tras un NAT puede no resultar alcanzable por otros UE y componentes de red.
- Los dispositivos NAT/barrera contrafuegos incluyen reglas que pueden variar sobre cómo puede atravesarse la barrera contrafuegos, y sobre cómo se crean las vinculaciones de NAT (es decir, correspondencia/filtrado independiente de la dirección, correspondencia/filtrado dependiente de la dirección, correspondencia/filtrado dependiente de la dirección y del puerto).
- Una vez establecida la comunicación, el NAT/barrera contrafuego mantiene el estado (es decir, los agujeros de la barrera contrafuego y las vinculaciones NAT) en base a temporizaciones. Si la temporización expira, los agujeros se cierran y se suprimen las vinculaciones del NAT. Deben ponerse en marcha mecanismos para mantener las vinculaciones NAT y los agujeros abiertos para señalización y comunicaciones de medios.

Los objetivos del tránsito del NAT/barrera contrafuego son proporcionar un mecanismo mediante el cual un UE pueda:

- Obtener y anunciar (por ejemplo, vía SDP) una dirección alcanzable. Cuando existan varias direcciones alcanzables, debería acordarse la "mejor"de ellas.
- Proporcionar un medio para abrir y mantener agujeros y vinculaciones de NAT para medios y señalización.

IPCablecom2 utiliza la metodología ICE para obtener y anunciar la "mejor" dirección alcanzable y cumplir los objetivos de diseño. Esta metodología utiliza STUN y TURN para conseguir direcciones candidatas. El UE anuncia dichas direcciones candidatas utilizando atributos del SDP descritos en la metodología ICE. El UE utiliza STUN para realizar pruebas de alcanzabilidad, permitiendo elegir la mejor dirección, es decir, aquella que utiliza la menor cantidad de recursos de red y tiene el menor retardo, al tiempo que mantiene el estado en el UE (en lugar de en la red). También permite el interfuncionamiento con los E-MTA ya que la dirección anunciada en los medios o líneas de conexión del SDP siempre será una dirección alcanzable.

El documento sobre la visión general del tránsito del NAT y de la barrera contrafuego de IPCablecom2 (apéndice V) proporciona información adicional sobre la metodología ICE, incluyendo una descripción sobre cómo los UE localizan los servidores STUN y TURN. Asimismo describe cómo se abren y mantienen las vinculaciones NAT.

Obsérvese que uno de los objetivos de diseño es proporcionar un mecanismo de tránsito del NAT y de la barrera contrafuegos que funcione con independencia de dónde se sitúen los NAT y de si éstos están o no anidados. No obstante, ello puede no ser posible en todos los casos.

La figura 7 muestra los puntos de referencia relacionados con el tránsito del NAT/barrera contrafuegos.

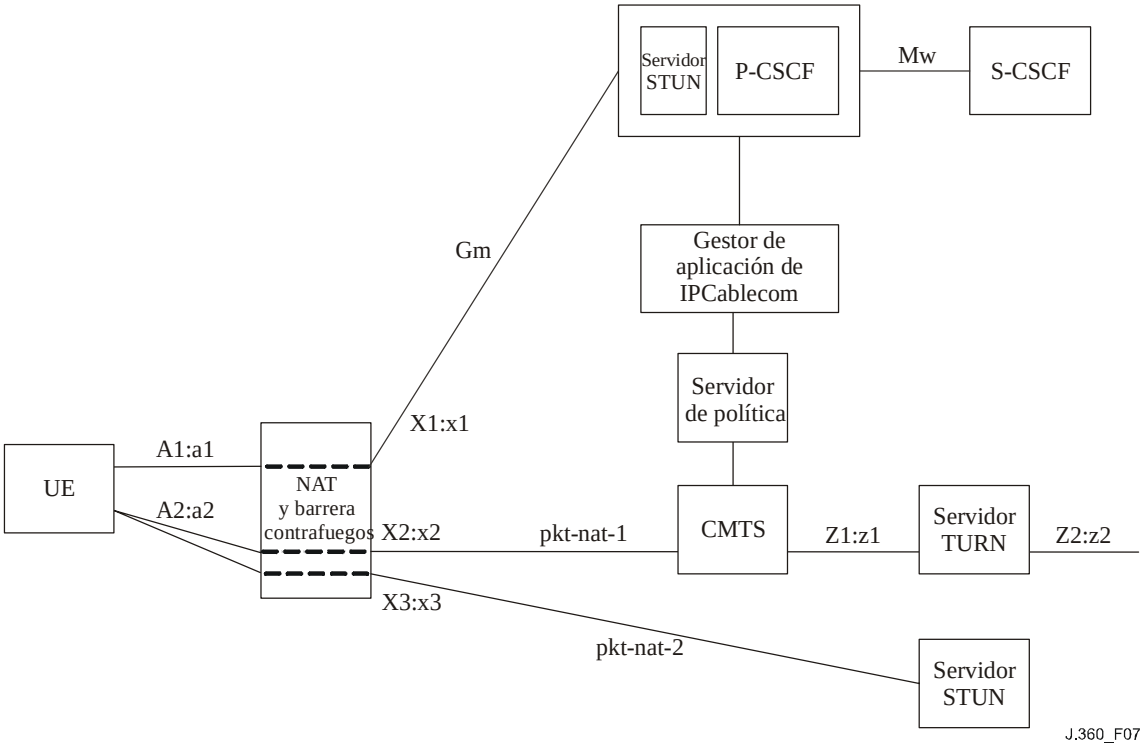


Figura 7 – Puntos de referencia de tránsito del NAT y de la barrera contrafuegos

En el cuadro 5 se describen los puntos de referencia de la figura 7.

Cuadro 5 – Descripción de los puntos de referencia de tránsito del NAT y de la barrera contrafuegos

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
Gm	UE – P-CSCF	Véase el cuadro 2.
Mw	P-CSCF – S-CSCF	Véase el cuadro 2.
pkt-nat-1	UE – Servidor TURN	Permite que el UE acceda a un servidor TURN para soportar el tránsito del NAT que no establezca una correspondencia independiente de la dirección.
pkt-nat-2	UE – Servidor STUN externo	Permite que el UE determine una de entre varias direcciones de medios candidatas utilizando STUN como apoyo a la metodología ICE.

Para más información véase el documento sobre la visión general del tránsito del NAT y de la barrera contrafuegos de IPCablecom (apéndice V).

7.5 Codificación de medios y transporte

IPCablecom2 utiliza RTP para transportar la mayoría de los servicios de comunicación (principalmente voz y video).

En la figura 8 se muestran los trenes de medios primarios de la arquitectura de IPCablecom2.

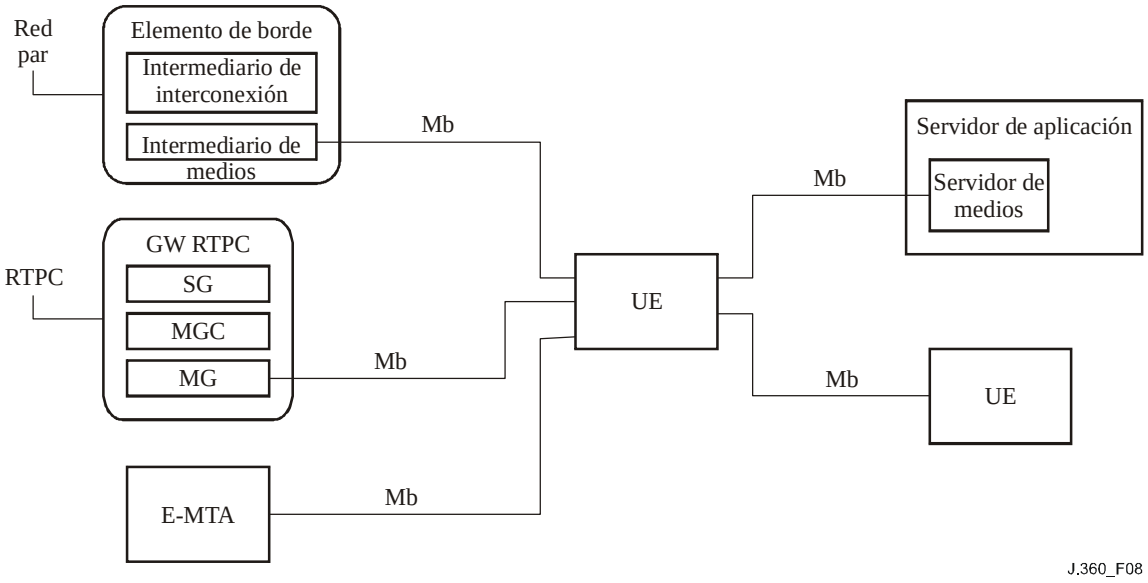


Figura 8 – Puntos de referencia de los trenes de medios

En el cuadro 6 se describen los puntos de referencia de la figura 8.

Cuadro 6 – Descripción de los puntos de referencia de los trenes de medios

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
Mb	UE – UE UE – MG UE – Elemento de borde UE – AS UE – E-MTA	Permite que componentes con capacidad de manejar medios envíen y reciban paquetes de datos de medios. Específicamente, un UE puede intercambiar medios con otro UE, una pasarela de medios (MG), un servidor de aplicación, un elemento de borde y un E-MTA.

A través del punto de referencia Mb puede pasar tráfico de audio codificado de banda estrecha o de banda ancha, tráfico de video codificado con códecs de video o una combinación de ambos tipos de tráfico. Los medios también pueden ser datos para la retransmisión de señales facsímil, de señales de un módem o de señales DTMF.

La supervisión de la calidad de audio en los puntos de referencia Mb se basa en RTCP. No se han especificado métricas para los trenes de video.

Para más información véase la especificación de códecs de audio/video de IPCablecom [UIT-T J.361].

7.6 Provisión, activación, configuración y gestión (PACM)

IPCablecom2 define un marco general de para la provisión, activación, configuración y gestión (PACM, *provisioning, activation, configuration, management*) que sirve de ayuda a los principales procesos de negocio. El marco incluye elementos normalizados (por ejemplo, DHCP), protocolos (por ejemplo, XCAP) y elementos de red específicos de IPCablecom (por ejemplo, PAC).

Además, el marco PACM se divide en las subáreas siguientes:

- Provisión.
- Participación en la red IP (conectividad con la red local).
- Identificación del proveedor de servicio.
- Flujos de provisión.
- Soporte de modelos asociados a una marca (es decir, ligados específicamente a un operador) o no asociados a una marca (es decir, que funcionan para cualquier operador).
- Marco general para la activación, configuración y gestión del UE.
- Activación de UE, abonado y servicio.
- Marco de configuración y gestión del UE.
- Modelo de datos.
- Protocolos de transporte.

En la figura 9 se ilustran los puntos de referencia asociados al PACM.

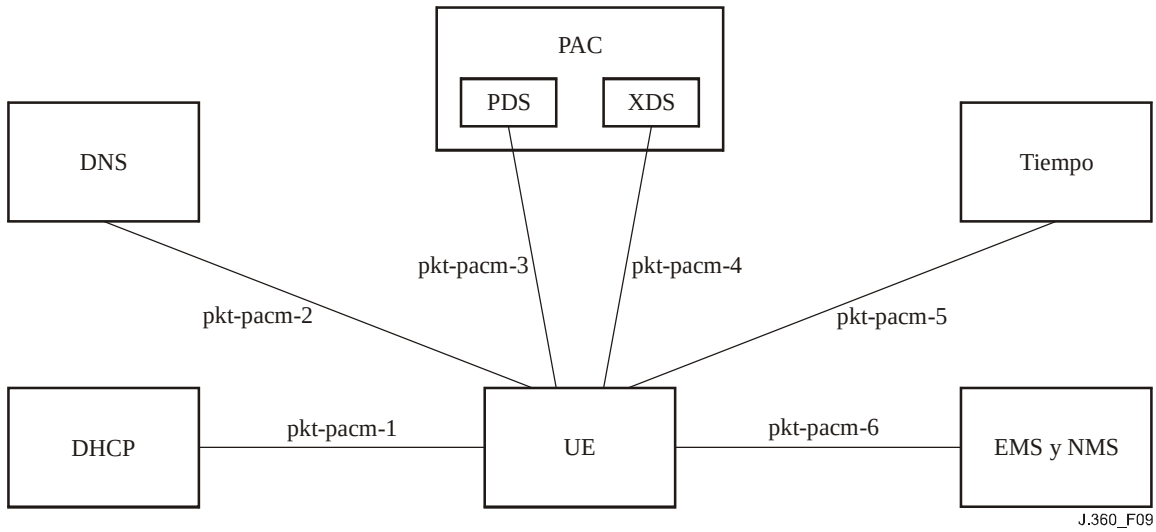


Figura 9 – Puntos de referencia de PACM

En el cuadro 7 se describen los puntos de referencia de la figura 9.

Cuadro 7 – Descripción de los puntos de referencia de PACM

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
pkt-pacm-1	UE – DHCP	Proporciona información de participación de la red (por ejemplo, dirección IP, direcciones del servidor DNS). Este punto de referencia puede ser suministrado por la red local o por una red de acceso no operada por el proveedor de servicio de IPCablecom.
pkt-pacm-2	UE – DNS	Permite que el UE resuelva nombres DNS para la localización de elementos de red o el encaminamiento de mensajes.
pkt-pacm-3	UE – PDS	Mediante la utilización de SIP, este punto de referencia permite que los UE se suscriban al estado asociado a los datos de configuración y de funcionalidades. Es un punto de referencia genérico que describe la interacción entre el UE y el XDS. Sin embargo, actualmente el PDS interactúa con el resto de los componentes SIP como un servidor de aplicación. Por lo tanto, los mensajes SIP de PACM atravesarán las interfaces Gm, Ma, Mw e ISC. NOTA 1 – El PDS aquí descrito se utiliza específicamente para PACM. No obstante, como componente lógico puede definirse para ser utilizado también en otras aplicaciones.
pkt-pacm-4	UE – XDS	Este punto de referencia se utiliza para distribuir y gestionar datos de configuración y funcionalidades. NOTA 2 – El XDS aquí descrito se utiliza específicamente para PACM. No obstante, como componente lógico puede definirse para ser utilizado también en otras aplicaciones.
pkt-pacm-5	UE-Tiempo	Permite que los UE obtenga el tiempo.
pkt-pacm-6	UE – EMS & NMS	Permite que los EMS y los NMS supervisen y gestionen los UE.

Para más información véase la especificación de provisión, activación, configuración y gestión de IPCablecom [UIT-T J.364].

7.7 Contabilización y utilización de la red

El IMS define puntos de referencia que permiten soportar distintos tipos de redes de acceso de conectividad del IMS (CAN, *connectivity access networks*). La contabilidad de IPCablecom2 asume que la red de acceso HFC de cable junto con el subsistema multimedia de IPCablecom definen un nuevo tipo de IP-CAN que se incorpora a la arquitectura general del IMS.

En la figura 10 se muestran los principales componentes de IPCablecom implicados en la tarificación fuera de línea y los puntos de referencia entre cada uno de los componentes.

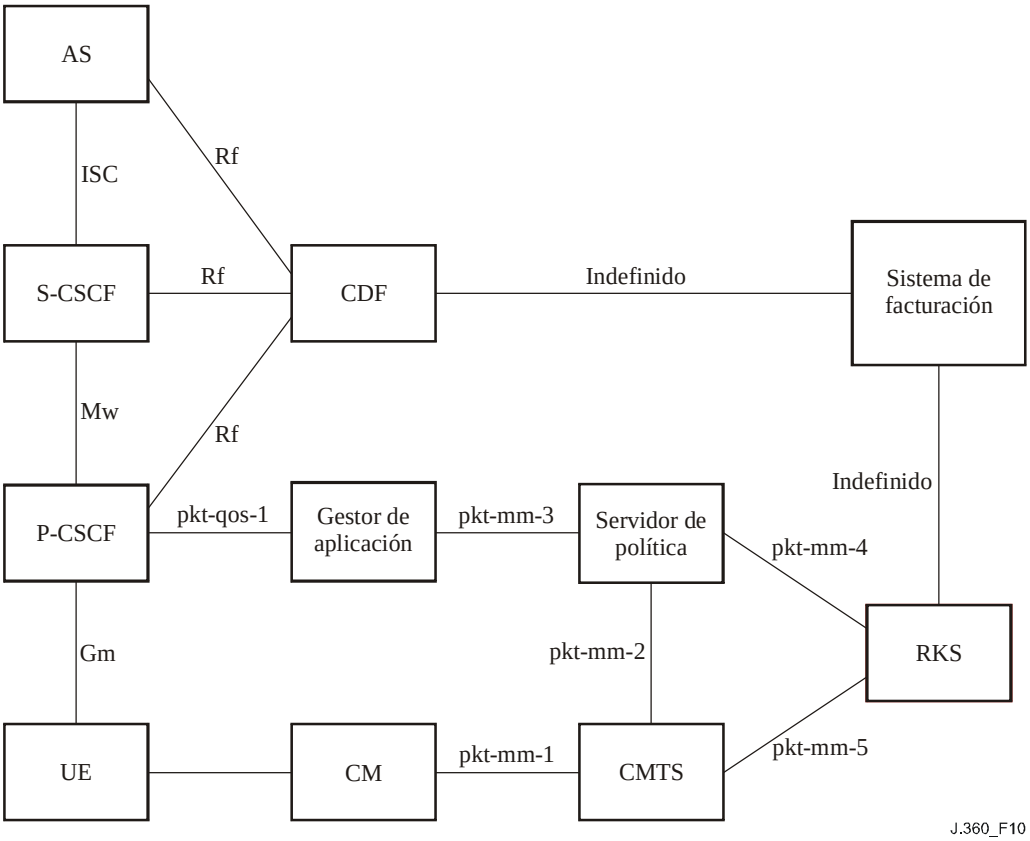


Figura 10 – Puntos de referencia de contabilidad

En el cuadro 8 se describen los puntos de referencia de la figura 10.

Cuadro 8 – Descripción de los puntos de referencia de contabilidad

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
Gm	UE – P-CSCF	Véase el cuadro 2.
Mw	P-CSCF – S-CSCF	Véase el cuadro 2.
ISC	S-CSCF – AS	Véase el cuadro 2.
Rf	CSCF – CDF	Punto de referencia basado en DIAMETER y situado entre los nodos IMS (P-CSCF, S-CSCF y AS) y la función de datos de tarificación (CDF, *charging data function*).
pkt-qos-1	P-CSCF – Gestor de aplicación	Véase el cuadro 4.
pkt-mm-1	CM – CMTS	Véase el cuadro 4.
pkt-mm-2	Servidor de política – CMTS	Véase el cuadro 4.
pkt-mm-3	Gestor de aplicación – Servidor de política	Véase el el cuadro 4.
pkt-mm-4	PS – RKS	Punto de referencia basado en RADIUS y situado entre el PS y el servidor de mantenimiento de registros (RKS, *record keeping server*). Este punto de referencia se define en IPCablecom multimedia [UIT-T J.179 Ap.I].
pkt-mm-5	CMTS – RKS	Punto de referencia basado en RADIUS y situado entre el CMTS y el RKS. Este punto de referencia se define en IPCablecom multimedia [UIT-T J.179 Ap.I]

Para más información véase la especificación de contabilidad IPCablecom [UIT-T J.363].

7.8 Seguridad

La arquitectura de seguridad de IPCablecom2 identifica los puntos de referencia asociados a los requisitos de seguridad en toda la arquitectura. Para organizar los puntos de referencia de seguridad, se han definido tres dominios de confianza.

- Dominio intra red – Los puntos de referencia situados en este dominio conectan elementos de red dentro del dominio de un proveedor de servicios.
- Dominio entre redes – Los puntos de referencia situados en este dominio conectan dos dominios. Los dominios pueden ser de proveedores de servicio distintos o pertenecer al mismo proveedor.
- Dominio de acceso – Los puntos de referencia situados en este dominio permiten a los UE conectarse a un proveedor de servicio.

Estos dominios de confianza se utilizan para descomponer la arquitectura de IPCablecom.

Para más información, véase el marco general de seguridad de IPCablecom2 (apéndice III).

7.8.1 Seguridad en el dominio de acceso

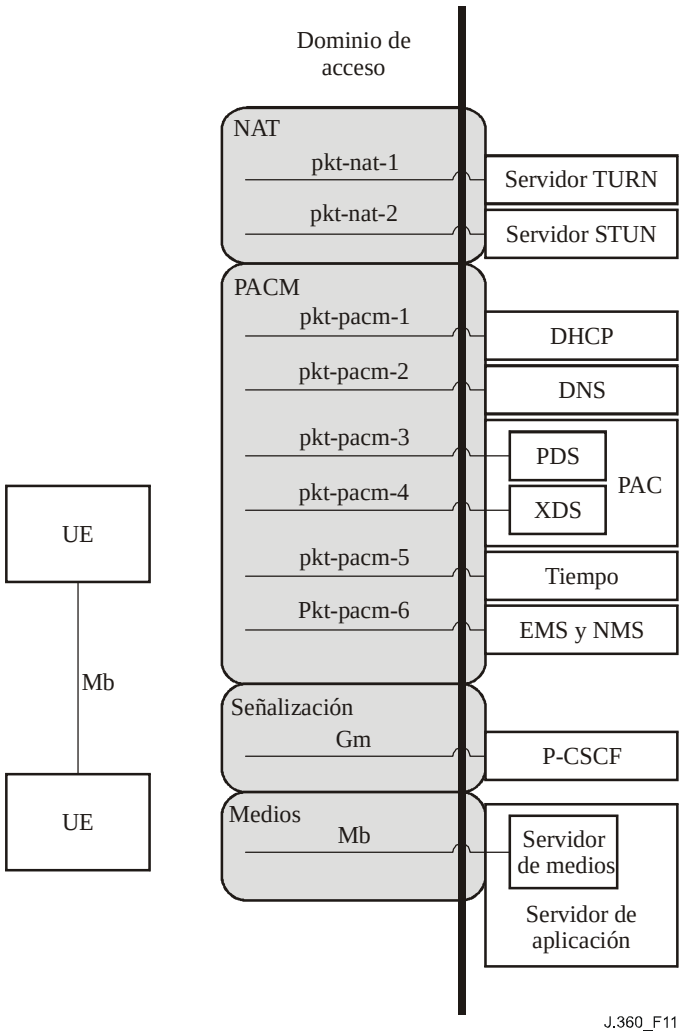


Figura 11 – Puntos de referencia del dominio del acceso

Las interacciones de los UE con la red tienen lugar en el dominio de acceso. Los métodos de acceso pueden ser de diversos tipos e incluyen DOCSIS y accesos inalámbricos. Debido a ello, el dominio de acceso puede ser objeto de multitud de amenazas, tal como se describe en el apéndice III. El cuadro 9 proporciona una visión general de alto nivel sobre cómo se hacen seguros los puntos de referencia del dominio de acceso.

Cuadro 9 – Descripción de los puntos de referencia del dominio del acceso

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
pkt-nat-1	UE – Servidor TURN	TURN: Las peticiones TURN son autenticadas y autorizadas en el propio protocolo TURN.
pkt-nat-2	UE – Servidor STUN externo	STUN: La integridad del mensaje se consigue mediante mecanismos STUN.
pkt-pacm-1	UE – Servidor DHCP	DHCP: IPCablecom no define la seguridad del protocolo DHCP.
pkt-pacm-2	UE – Servidor DNS	DNS: IPCablecom no define la seguridad del protocolo DNS.
pkt-pacm-3	UE – Servidor PDS	SIP: integridad y privacidad de los mensajes mediante la seguridad del protocolo internet, IPSec (*Internet protocol security*) o mediante la seguridad de la capa de transporte (TLS, *transport layer security*).
pkt-pacm-4	UE – Servidor XDS	XCAP: integridad y privacidad de los mensajes mediante HTTP sobre TLS
pkt-pacm-5	UE – Servidor de tiempo	SNTP: IPCablecom no define la seguridad para el protocolo SNTP.
pkt-pacm-6	UE – Servidor EMS y NMS	La seguridad de la interfaz de gestión está fuera del ámbito de esta especificación.
Gm	UE – P-CSCF	SIP: integridad y privacidad de los mensajes mediante IPsec o TLS. STUN: integridad del mensaje mediante mecanismos STUN.
Mb	UE – UE UE – MG UE – Elemento de borde UE – AS UE – E-MTA	RTP: La seguridad de los medios está fuera del ámbito de esta especificación. NOTA – La figura 11 sólo muestra unos pocos flujos de medios representativos.

7.8.2 Seguridad interna a un dominio de red

Los puntos de referencia y componentes internos de un dominio están contenidos en la red de un proveedor de servicio y, en consecuencia, conforman una política de seguridad de naturaleza holística. La seguridad de estos puntos de referencia se consigue por lo general mediante el punto de referencia Zb. El punto de referencia Zb utiliza el encapsulado de seguridad de la cabida útil (ESP, *encapsulating security payload*) de IPsec. Los puntos de referencia Zb que soportan TCP también pueden utilizar TLS.

Los siguientes puntos de referencia internos al dominio definen requisitos de seguridad adicionales que pueden aplicarse en lugar del punto de referencia Zb o adicionalmente al mismo:

- pkt-qos-2 – Mecanismo de desafío criptográfico definido mediante el protocolo de descubrimiento del punto de control.
- pkt-laes-4 – Mecanismo criptográfico definido mediante SNMPv3.
- pkt-laes-6 – Mecanismo de desafío criptográfico definido mediante el protocolo de descubrimiento del punto de control.

7.8.3 Seguridad entre dominios de red

Los puntos de referencia entre dominios constan de:

- Elemento de borde – Red par – Su seguridad se logra utilizando el punto de referencia Za, que utiliza el ESP de IPsec. El tráfico entre dominios en el IMS ha de pasar a través de una pasarela de seguridad (SEG, *security gateway*). La SEG soporta el punto de referencia Za y obliga a mantener una política de seguridad para los flujos de tráfico entre dominios. Se asume que el elemento de borde incluye la funcionalidad SEG, pero que dicha pasarela de seguridad puede constituir un elemento diferenciado.
- Pasarela RTPC – RTPC – La seguridad de la RTPC no está definida.
- CMS – Puntos extremos – La seguridad del punto de referencia CMS se define en la especificación de seguridad de IPCablecom [UIT-T J.170].

7.9 Interceptación legal

La arquitectura de la interceptación legal de IPCablecom2 se ilustra en la figura 12. Los elementos de control de llamada de IPCablecom, tales como las CSCF, forman un conjunto potencial de puntos de acceso de interceptación de datos relacionados con la llamada. Los elementos del plano portador de IPCablecom, tales como el CMTS y la MG, forman el conjunto de potenciales puntos de acceso de interceptación del contenido de las llamadas. La función de entrega (DF, *delivery function*) recibe de los puntos de acceso de interceptación de IPCablecom eventos relacionados con las llamadas interceptadas y el contenido de las mismas, los correlaciona con el servicio de abonado objetivo y entrega el resultado a la función de recopilación (CF, *collection function*) de los agentes facultados sobre un punto de referencia normalizado definido por [ES-DCI]. Obsérvese que la DF no forma parte de la arquitectura de IPCablecom, aunque éste especifique los puntos de referencia con la DF necesarios para la interceptación legal en las redes IPCablecom. Los elementos del control de llamada, tales como S-CSCF y P-CSCF, asignados a un abonado objetivo informan al DF de eventos relacionados con la llamada. Estos elementos de control también proporcionan los elementos pares necesarios para la interceptación en caso de redireccionamiento de llamadas y de control de la llamada por terceros. Los elementos de borde, tales como el BGCF, el I-CSCF y el MGC, informan a la DF sobre información del operador de interconexión. La DF aprovisiona los puntos de acceso para la interceptación del contenido de la llamada detectando, en primer lugar, los puntos de acceso mediante el protocolo de descubrimiento de puntos de control y, a continuación, realizando la interceptación en los puntos de acceso al contenido mediante SNMPv3. El proceso de acceso al contenido de la llamada comienza cuando la DF recibe un evento de inicio de la llamada de los elementos de control de llamada.

El CMS de IPCablecom se actualiza y mejora para permitir el interfuncionamiento con elementos de IPCablecom a fin de poder realizar la interceptación de llamadas a través de los componentes NCS y SIP. Los elementos MGC y MG de IPCablecom pueden, opcionalmente, ser mejorados para admitir los puntos de referencia de la figura 12.

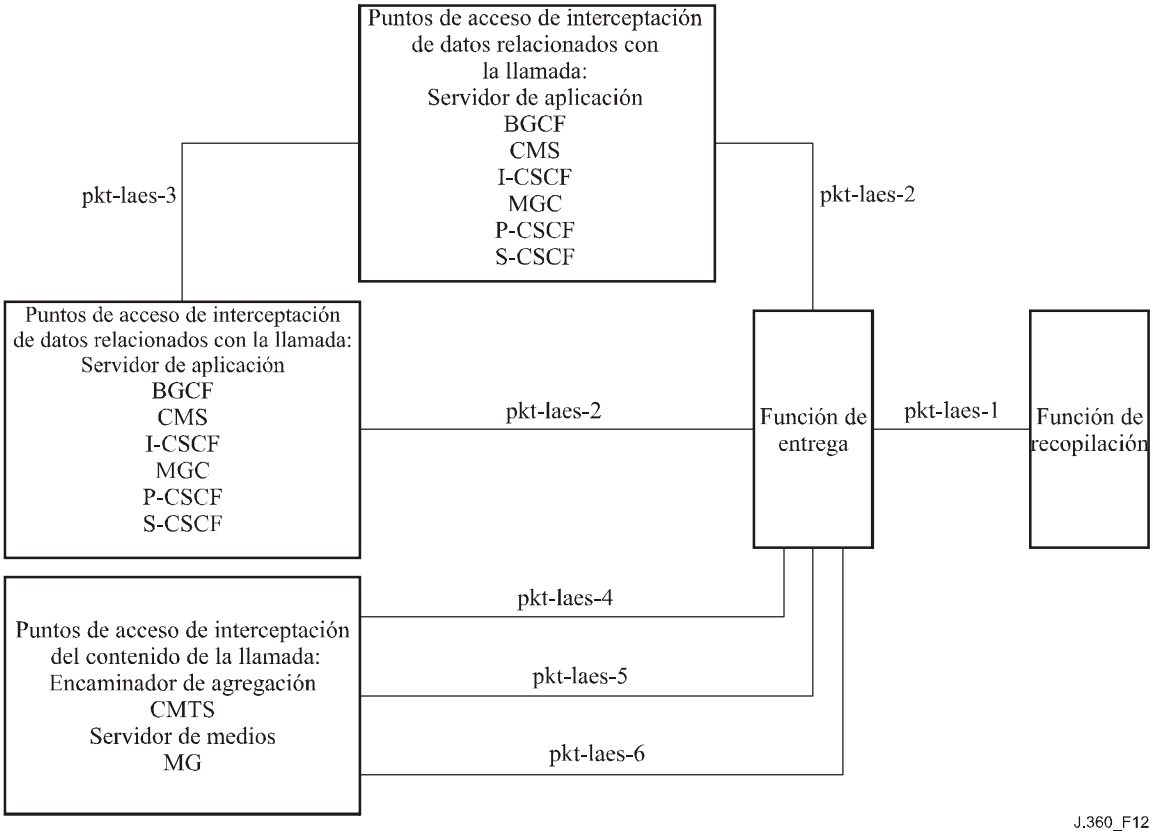


Figura 12 – Puntos de referencia de la interceptación legal

En el cuadro 10 se describen los puntos de referencia de la figura 12.

Cuadro 10 – Descripción de los puntos de referencia de la interceptación legal

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
pkt-laes-1	DF – CF	Los datos relacionados con la llamada y el contenido de la llamada, una vez correlados, se informan a la función de recopilación del agente facultado. Se define en [ES-DCI].
pkt-laes-2	Elemento de control de sesión– DF	Los eventos relativos a la llamada interceptada se informan a la DF. Este punto de referencia se basa en DIAMETER.
pkt-laes-3	Elemento de control de sesión – Elemento de control de sesión	Permite a los elementos de control de sesión aprovisionar dinámicamente interceptaciones en elementos pares para llamadas en las que los elementos de control asignados al sujeto objetivo ya no están involucrados en la llamada. El redireccionamiento de llamada es un ejemplo de ello. Este punto de referencia está basado en SIP.
pkt-laes-4	Entre DF y puntos de acceso a contenido	La DF aprovisiona de forma dinámica puntos de interceptación de contenido. Este punto de referencia se basa en SNMPv3.
pkt-laes-5	Entre punto de acceso a contenido y DF	Se informa del contenido de la llamada interceptada al DF. Este punto de referencia está basado en medios sobre UDP.
pkt-laes-6	Entre DF y puntos de acceso a contenido	La DF, como solicitante, utiliza el protocolo de descubrimiento de punto de control [UIT-T J.362] para determinar los puntos de acceso de interceptación del contenido de llamada adecuados, actuando como puntos de control en la red para la interceptación del contenido de la llamada.

Para más información véase la especificación de vigilancia electrónica de IPCablecom – funciones entre redes [ES-INF] y la especificación de vigilancia electrónica de IPCablecom – interfaz entre la función de entrega y la función de recopilación [ES-DCI].

7.10 Descubrimiento del punto de control

El punto de referencia de descubrimiento del punto de control que se muestra en la figura 13, define un protocolo basado en la red que puede utilizarse para identificar la dirección IP necesaria para realizar peticiones de QoS, así como para intervenir el contenido con fines de interceptación legal.

Para peticiones de QoS, ello aplica para identificar la dirección IP del CMTS para DQOS y para IPCablecom multimedia (PCMM). En caso de interceptación legal, se utiliza para descubrir la dirección IP que ha de utilizarse en la intervención del contenido realizada en el CMTS, así como en pasarelas de medios y en encaminadores y/o conmutadores de agregación que se encuentran delante de los puntos extremos de medios. Además de proporcionar la dirección IP, la respuesta identifica el protocolo a utilizar y puede indicar la subred en la que se encuentra la dirección de destino solicitada.

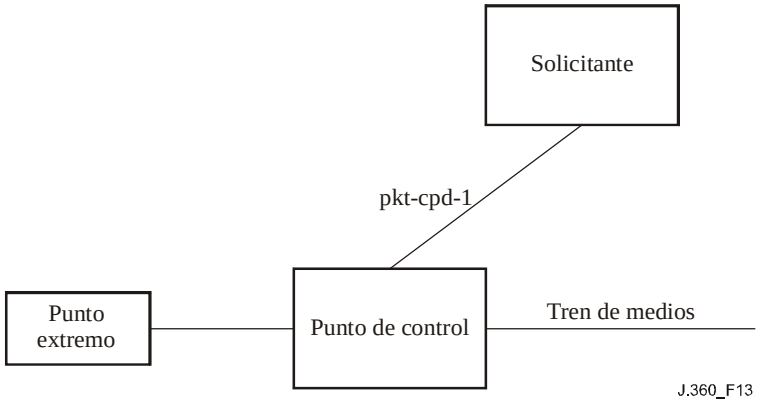


Figura 13 – Punto de referencia de descubrimiento del punto de control

En el cuadro 11 se describen los puntos de referencia de la figura 13.

Cuadro 11 – Descripción del punto de referencia de descubrimiento del punto de control

Punto de referencia	Elementos de red de IPCablecom	Descripción del punto de referencia
pkt-cpd-1	Solicitante – Punto de control	El solicitante utiliza el protocolo de descubrimiento de punto de control para determinar el punto de control adecuado en la red para un UE dado. Otros puntos de referencia de la arquitectura se basan en este punto de referencia.

Para más información véase la especificación de descubrimiento de puntos de control de IPCablecom2 [UIT-T J.362].

Apéndice I

Visión general de la señalización SIP

(Este apéndice no es parte integrante de esta Recomendación)

I.1 Introducción y objetivo

En este apéndice se presenta una visión general de la arquitectura de señalización SIP y se describen los requisitos de alto nivel necesarios para soportar comunicaciones basadas en SIP en la arquitectura de IPCablecom2.

El objetivo principal de este apéndice es definir cómo se comunican los elementos funcionales de IPCablecom2 que participan en la señalización de sesión mediante el protocolo SIP del IETF y sus extensiones, así como especificar las mejoras introducidas en el IMS del 3GPP.

Puesto que la señalización SIP de IPCablecom2 está estrechamente alineada con el IMS, los requisitos normativos de señalización SIP de IPCablecom2 se definen en especificaciones complementarias del IMS, que son especificaciones 3GPP mejoradas destinadas a incluir requisitos específicos del cable. Los requisitos de señalización SIP de IPCablecom2 se documentan en las tres especificaciones complementarias Recs. UIT-T J.366.2, J.366.3 y J.366.4.

I.1.1 Relación con las características y servicios de IPCablecom

Este apéndice y las especificaciones complementarias del IMS conexas constituyen la señalización SIP básica para una amplia gama de servicios de comunicaciones basados en IP, desde funcionalidades de la telefonía tradicional preexistente hasta servicios y aplicaciones nuevas y mejoradas. Esta señalización SIP es independiente del servicio y, por lo tanto, los requisitos específicos de cada servicio y funcionalidad de IPCablecom están fuera del ámbito de este documento y se definen de forma separada. La relación entre este apéndice, las especificaciones complementarias del IMS relativas a señalización SIP y los servicios y funcionalidades de IPCablecom se muestran en la figura I.1.

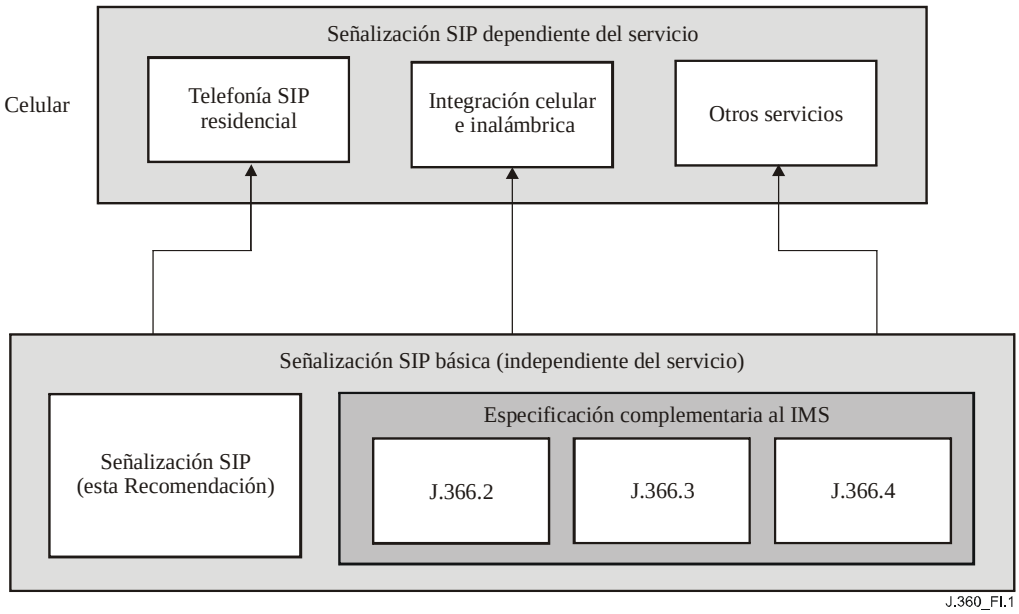


Figura I.1 – Relación entre señalización y servicios SIP básicos

I.1.2 Relación con otras especificaciones de IPCablecom2

Las especificaciones de la señalización SIP básica de IPCablecom2 definen en su conjunto los requisitos de señalización para las capacidades generales siguientes:

- Encaminamiento de mensajes SIP
- Registro
- Establecimiento de sesión de medios
- Marco de notificación de eventos
- Plataforma genérica de control de servicios
- Confirmación de la identidad.

Otras especificaciones de IPCablecom2 tales como las relativas a contabilidad, tránsito de NAT y seguridad, imponen requisitos adicionales a la señalización SIP y, por tanto, influyen en las especificaciones complementarias del IMS antes mencionadas, específicamente en [UIT-T J.366.4]. Asimismo, algunos mecanismos de señalización afectan a especificaciones complementarias del IMS no relativas a SIP, como es el caso de [UIT-T J.366.5]. Finalmente, la señalización SIP de IPCablecom2 impone requisitos a [UIT-T J.178] para que se soporte el interfuncionamiento entre UE de IPCablecom2 y el E-MTA de IPCablecom. En la figura I.2 se muestra la relación entre estas especificaciones.

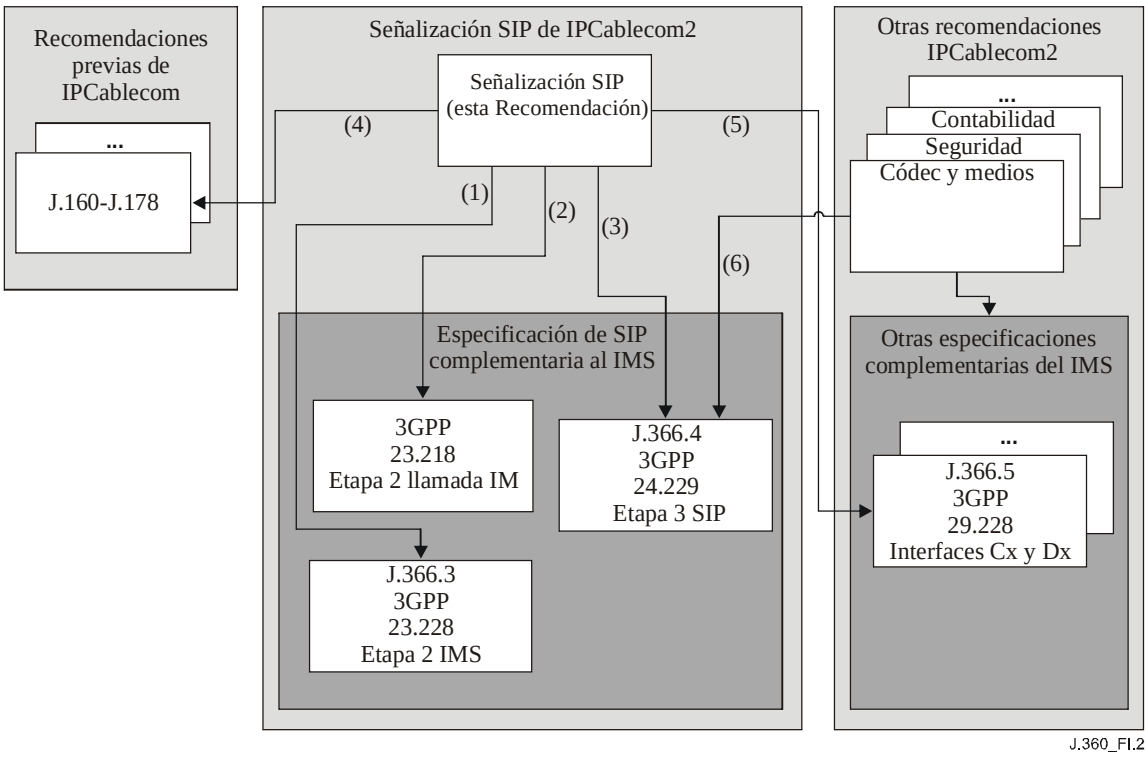


Figura I.2 – Relación entre las especificaciones de señalización SIP

I.2 Referencias

En este apéndice se utilizan las referencias informaciones adicionales siguientes:

[UIT-T J.366.4] Recomendación UIT-T J.366.4 (2006), *Subsistema multimedia IP(IMS) IPCablecom2: Protocolo de inicio de sesión (SIP) y protocolo de descripción de sesión (SDP) – Especificación nivel 3* (3GPP TS 24.229).

[UIT-T J.366.5] Recomendación UIT-T J.366.5 (2007), *Interfaces Cx y Dx del subsistema multimedios del protocolo Internet; especificación de los flujos de señalización y de los contenidos de los mensajes* (3 GPP TS 29.228).

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

[IETF RFC 3262] IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP).*

[IETF RFC 3311] IETF RFC 3311 (2002), *The Session Initiation Protocol (SIP) UPDATE Method*.

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

[IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp).*

[IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP).*

[IETF RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*

[IETF RFC 3486] IETF RFC 3486 (2003), *Compressing the Session Initiation Protocol (SIP).*

[IETF RFC 3556] IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth*.

[IETF RFC 3680] IETF RFC 3680 (2004), *A Session Initiation Protocol (SIP) Event Package for Registrations*.

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

I.3 Términos y definiciones

En este apéndice se utilizan los términos y definiciones adicionales siguientes:

I.3.1 identidad autorizada: Una instancia de una "identidad autorizada" en una red IPCablecom2 es la representación de un emparejamiento permitido entre una identidad pública y una identidad privada.

I.3.2 núcleo: El núcleo contiene los componentes básicos requeridos para proporcionar servicios SIP y datos de abonado. Las agrupaciones funcionales del núcleo constan de los componentes funcionales siguientes: interrogador CSCF (I-CSCF), servidor CSCF (S-CSCF), función de localización de abonado (SLF) y servidor de abonados de la red origen (HSS).

I.3.3 credenciales de identidad: Conjunto de información necesaria para realizar la autenticación de una identidad privada. La información real depende del mecanismo de autenticación.

I.3.4 proveedor de servicio IPCablecom2: Operador de red que opera uno o más dominios administrativos IPCablecom2 independientes.

I.3.5 dominio DNS del proveedor de servicio IPCablecom2: Nombre de dominio DNS que es propiedad y está gestionado por un dominio administrativo IPCablecom2. Se utiliza para formar los URI SIP que transportan identificadores públicos.

I.3.6 servidor intermediario (proxy): Entidad de intermediación SIP que actúa como servidora y como UE para realizar peticiones en nombre de otros UE. Un servidor intermediario juega principalmente el papel de encaminamiento, lo que significa que debe asegurar que se envía una petición a otra entidad "más cercana" al usuario objetivo. Los intermediarios también son de utilidad para la imposición de políticas (por ejemplo, garantizar que a un usuario se le permite hacer llamadas). Un intermediario interpreta y, si es necesario rescribe partes específicas de un mensaje de petición antes de reenviarlo.

I.3.7 identificador público: Identificador utilizado para hacer referencia a una identidad pública.

I.4 Abreviaturas y acrónimos

En este apéndice se utiliza la abreviatura adicional siguiente:

SIP UE Equipo de usuario que contiene un agente de usuario SIP (*user equipment that contains a SIP user agent*)

I.5 Señalización SIP de IPCablecom2

Las aplicaciones y servicios de IPCablecom2 se controlan utilizando el protocolo de inicio de sesión (SIP). IPCablecom2 se alinea con una instancia específica de arquitectura SIP definida en las especificaciones del subsistema multimedia IP (IMS) desarrolladas por el 3GPP. IPCablecom2 se basa en la versión 6 del IMS, al cual mejora en aquellos aspectos necesarios para soportar los requisitos de IPCablecom2.

I.5.1 Arquitectura de la señalización SIP de IPCablecom2 y puntos de referencia

En la figura I.3 se ilustran los puntos de referencia de control del servicio y de señalización IPCablecom2. La mayoría de los puntos de referencia se han normalizado para el IMS y han sido modificados lo necesario para IPCablecom2, tal como se identifica en varias especificaciones IPCablecom2. También se incluyen puntos de referencia específicos de IPCablecom2.

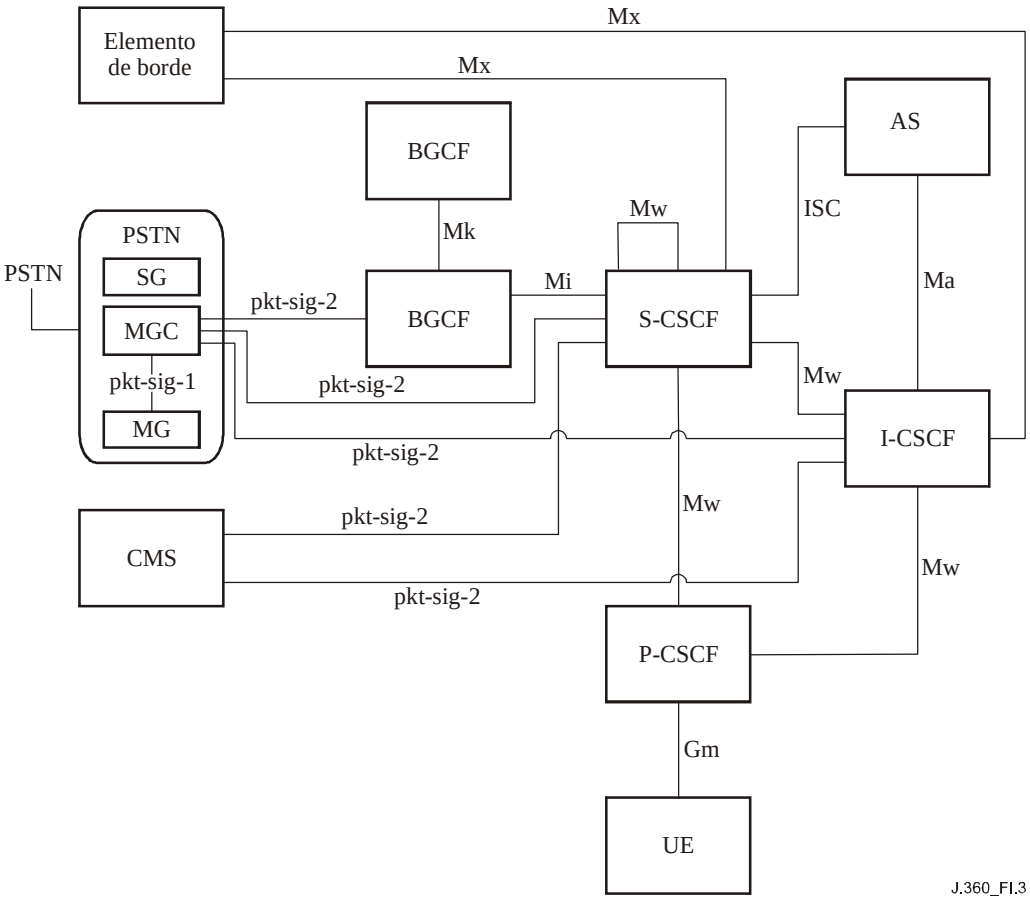


Figura I.3 – Puntos de referencia de la señalización de llamada

I.5.1.1 Componentes funcionales de la señalización SIP

I.5.1.1.1 Equipo de usuario (UE, *user equipment*)

IPCablecom2 soporta clientes SIP con una variedad de formas y capacidades, por ejemplo, teléfonos basados en software y basados en hardware, teléfonos inteligentes y teléfonos inalámbricos y alámbricos, aplicaciones de mensajería instantánea, terminales de video comunicaciones, etc. En coherencia con el IMS, a los clientes de IPCablecom2 se les denomina equipos de usuario (UE). Todos los tipos de UE utilizan la misma infraestructura básica para el acceso a servicios multimedia. Los UE pueden ser dispositivos fijos o móviles, tales como computadoras portátiles o teléfonos WiFi. Pueden residir en la red de acceso del cable u obtener los servicios de otras redes de acceso.

I.5.1.1.2 Intermediario de función de control de sesión de llamada (P-CSCF, *proxy call session control function*)

Un UE accede a la infraestructura SIP a través del P-CSCF. El P-CSCF aísla la red SIP de las particularidades de los protocolos específicos de la red de acceso y proporciona el escalado de la infraestructura manejando tareas intensivas en recursos cuando interactúa con el UE. También representa los límites de confianza de SIP, pues marca la separación entre partes no confiables de la red (red de acceso, red local) y partes confiables de la red (núcleo, aplicación, interconexión, soporte operacional). El P-CSCF proporciona las funciones siguientes:

- Encamina mensajes SIP desde el UE al I-CSCF o S-CSCF y viceversa.
- Mantiene asociaciones de seguridad con el UE, confirmando la identidad de las identidades públicas autenticadas.

- Hace el seguimiento del estado de registro de las identidades públicas y elimina la asociación de seguridad con el UE cuando la red desregistra una identidad pública.
- Verifica los datos de los mensajes entrantes (por ejemplo, verifica la cabecera "Route" de SIP).
- Bloquea servicios (por ejemplo, ignora determinadas peticiones entrantes de identidades públicas no registradas).
- Impone políticas (por ejemplo, si se habilita o no la seguridad de la señalización o la compresión).
- Genera eventos de contabilidad.

I.5.1.1.3 Servidor de CSCF (S-CSCF)

El S-CSCF es responsable de la provisión de servicios a abonados basados en UE. No obstante, el S-CSCF no proporciona servicios a los E-MTA de IPCablecom. En lugar de ello, los E-MTA son atendidos por sus CMS, tal como se describe en [UIT-T J.160].

A través del S-CSCF que atiende a un abonado, pasan todos los mensajes SIP distintos del diálogo hacia y desde dicho abonado. A alto nivel, el S-CSCF proporciona lo siguiente:

- Función de registrador SIP, que mantiene datos que dinámicamente vinculan identificadores públicos registrados (AOR) con un conjunto de direcciones de contacto, asigna URIs de agentes de usuario encaminables globalmente y almacena cualesquiera otros parámetros asociados con el registro; por ejemplo, capacidades de agente de usuario y la dirección o direcciones del P-CSCF que pueden ser utilizadas para realizar los contactos, distribuye el estado de registro del usuario a entidades que se abonan al lote Reg-Event.
- Autenticación y autorización de usuario SIP.
- Plataforma de control de servicio; aplica criterios de filtrado a peticiones de inicio de diálogo entrantes y, en base a activadores de punto de servicio, encamina peticiones a los servidores de aplicación adecuados a fin de proporcionar servicios y funcionalidades.
- Encaminamiento de mensajes SIP a un P-CSCF para UE servidos por el S-CSCF.
- Encaminamiento de mensajes SIP a un I-CSCF para identidades de usuario públicas no atendidas por el S-CSCF.
- Encaminamiento de mensajes a una BGCF para llamadas a la RTPC.
- Encaminamiento de mensajes a un I-CSCF para llamadas a una red par.
- Encaminamiento de mensajes a la THIG de I-CSCF para el ocultamiento de la topología a las llamadas a una red par.
- Procesamiento en originación: procesado de peticiones de inicio de diálogo entrantes procedentes de agentes de usuario SIP contenidos en UE o en servidores de aplicaciones atendidos por el S-CSCF.
- Procesamiento en terminación: procesado de mensajes SIP salientes que terminan en un identificador público servido por el S-CSCF. Ello incluye el desvío de mensajes SIP cuando se registran múltiples direcciones de contacto para dicho identificador público.
- Puede consultar bases de datos externas, como es el caso de ENUM, de portabilidad de número local (LNP, *local number portability*) y bases de datos de números 800 para determinar hacia dónde encaminar la llamada.
- Generación de eventos de contabilidad.
- Supervisión del estado de funcionamiento de las sesiones activas y liberación de la sesión si falla un componente del trayecto de señalización (por ejemplo, el S-CSCF puede liberar sesiones activas asociadas con, o en nombre de, un UE que ha fallado).
- Liberación de sesiones iniciada por la red (por ejemplo, debido a actividad administrativa).

Puede haber varios S-CSCF en el núcleo de IPCablecom. En un instante dado, una suscripción (y todos los identificadores públicos asociados a la misma) sólo puede ser gestionada por un único S-CSCF.

Los identificadores públicos se asignan a un S-CSCF en el momento del registro. Una vez que un identificador público se asigna a un S-CSCF, todas las demás instancias registradas de dicho identificador público deben ser asignadas al mismo S-CSCF. Asimismo, todos los identificadores públicos de la misma suscripción deben estar asociados con el mismo S-CSCF. Los datos de la suscripción se almacenan en uno o más servidores de abonado de la red origen (HSS). El S-CSCF interactúa con los HSS relevantes para obtener datos de los usuarios a los que sirve. El S-CSCF también puede interactuar con el HSS para almacenar ciertos tipos de datos de usuario de los usuarios que atiende.

Los URI de agente de usuario encaminable globalmente (GRUU) son soportados por los puntos extremos y por el S-CSCF. Ello permite que asignar a los puntos extremos un URI encaminable globalmente durante el proceso de registro, que a su vez permite que los puntos extremos inicien una petición a un contacto específico de un AOR. Esto es importante para determinadas funcionalidades tales como la transferencia de llamada y la conferencia.

I.5.1.1.4 Interrogador de CSCF (I-CSCF)

El I-CSCF es responsable del encaminamiento de peticiones entrantes hacia el S-CSCF de terminación correcto. También proporciona una función de pasarela de interfuncionamiento para la ocultación de topología (THIG, *topology hiding interworking gateway function*) que puede utilizarse para ocultar la topología interna de la red originaria a la red par o a un UE de la red originaria.

- Encamina mensajes REGISTER entrates recibidos desde el P-CSCF hacia el S-CSCF correcto;
- Encamina peticiones de inicio de diálogo entrantes recibidas de un S-CSCF de origen situada en la red originaria o de un S-CSCF de origen en una red par, hasta el S-CSCF de terminación correcto;
- Generación de eventos de contabilidad.

El I-CSCF es el punto de encaminamiento en la red para peticiones externas procedentes de otras redes y destinadas a usuarios en la red originaria. Se comunica con el HSS para determinar la vinculación entre una suscripción (y las identidades públicas asociadas) y un S-CSCF.

I.5.1.1.5 Servidor de aplicación (AS)

Un servidor de aplicación (AS, *application server*) proporciona servicios de IPCablecom de valor agregado y puede residir en la red originaria del usuario o en la ubicación de un tercero, que puede ser otra red o un AS autónomo. Un AS puede influir en una sesión SIP en nombre de los servicios que soporta y puede ser anfitrión de y ejecutar servicios. Un AS puede iniciar o terminar servicios en nombre de un usuario.

I.5.1.1.6 Elemento de borde

La interconexión con redes pares puede realizarse a través de un elemento de borde. El elemento de borde contiene una función de intermediación de interconexión y puede contener una función de intermediación de medios. También puede proporcionar una serie de funciones:

- Interfuncionamiento de protocolos.
- Imposición de un perfil SIP (traducción, adaptación o normalización).
- Servicios relacionados con la seguridad (por ejemplo, mantenimiento de una asociación de seguridad con el par).
- Gestión de direcciones IP (redes pares con el mismo espacio de direcciones IP privado).

- Interfuncionamiento entre redes IPv6 e IPv4.
- Retransmisión de medios entre redes pares (por ejemplo, para la seguridad de los medios o el interfuncionamiento de códecs).
- Ocultación de direcciones y de topología a nivel de señalización (por ejemplo, actúa como retransmisor de señalización y hace inteligible la información de dirección de las cabeceras).

I.5.1.1.7 Función de control de la pasarela de interconexión (BGCF, *breakout gateway control function*)

La BGCF permite seleccionar la red para el encaminamiento hacia la RTPC, estableciendo dentro de la propia red el MGC que debe utilizarse para la conexión con la RTPC. La BGCF puede hacer consultas a bases de datos de encaminamiento externas para determinar a dónde debe encaminamiento la llamada.

I.5.1.1.8 Pasarela con la red telefónica pública conmutada (GW RTPC)

La pasarela (GW) RTPC consta de la pasarela de señalización (SG, *signalling gateway*), el controlador de pasarela de medios (MGC, *media gateway controller*) y la pasarela de medios (MG, *media gateway*). Los elementos funcionales SG, MGC y MG se definen en versiones previas de IPCablecom y se reutilizan en esta versión de IPCablecom2, con la adición al MGC de un punto de referencia de IPCablecom2. Los SG, MGC y MG son componentes lógicos que pueden existir en plataformas separadas o ser combinados conjuntamente en una única plataforma.

La SG realiza la conversión de señalización en la capa de transporte entre el transporte basado en SS7 y el transporte basado en IP de la red IPCablecom. La SG no interpreta la capa de aplicación, pero sí las capas necesarias para el encaminamiento de mensajes de señalización.

El MGC realiza la conversión de protocolo entre los mensajes PUSI del SS7 y los protocolos de control de llamadas de IPCablecom, y proporciona el control de conexión de los canales de medios en la MG.

La MG proporciona la conversión de canales portadores entre la red de conmutación de circuitos y los flujos de medios RTP IP en la red IPCablecom. La MG puede introducir códecs y compensadores de eco, etc.. según sea necesario para proporcionar las conversiones de canal portador.

I.5.1.1.9 Servidor de gestión de llamadas (CMS, *call management server*)

Un servidor de gestión de llamadas de IPCablecom (CMS *call management server*) da soporte a los servicios de telefonía para clientes NCS (es decir, E-MTA). En IPCablecom2, el CMS proporciona la mayor parte de las funcionalidades de telefonía, interactuando directamente con servidores de aplicaciones (servidores de mensajería unificada, servidores de conferencia, etc.) a fin de proporcionar aplicaciones adicionales a los puntos extremos NCS. Sin embargo, no permite funcionalidades para un funcionamiento transparente a través de los E-MTA y los UE que sean propiedad del mismo usuario

I.5.1.2 Puntos de referencia de la señalización SIP

Los puntos de referencia incluidos en la figura I.3 se describen en el cuadro I.1. Todos los puntos de referencia están basados en SIP, salvo que se indique lo contrario.

Cuadro I.1 – Puntos de referencia de señalización de llamada

Punto de referencia	Elementos de red de IPCablecom2	Descripción del punto de referencia
Mx	I-CSCF – Elemento de borde S-CSCF – Elemento de borde	Permite que un S-CSCF o un I-CSCF se comuniquen con un elemento de borde en caso de interfuncionamiento con otra red. Por ejemplo, una sesión entre la red originaria y una red par puede encaminarse a través de una función ALG del IMS dentro del elemento de borde para permitir el interfuncionamiento entre redes SIP IPv6 e IPv4.
Mi	S-CSCF – BGCF	Permite que el S-CSCF transmita señalización de sesión a la BGCF para el interfuncionamiento con redes RTPC.
Mk	BGCF – BGCF	Permite que una BGCF transmita señalización de sesión a otra BGCF.
Mw	P-CSCF – I-CSCF P-CSCF – S-CSCF I-CSCF – S-CSCF S-CSCF – S-CSCF	Permite la comunicación y retransmisión de mensajes de señalización entre las CSCF con fines de registro y control de sesión.
Ma	I-CSCF – AS	Permite al I-CSCF transmitir directamente al servidor de aplicación peticiones SIP destinadas a una identidad de servicio pública alojada en un servidor de aplicación.
ISC	S-CSCF – AS	Permite que un S-CSCF se comunique con un servidor de aplicación para soportar diversas aplicaciones.
Gm	UE – P-CSCF	Permite que un UE se comunique con el P-CSCF con fines de registro y control de sesión.
pkt-sig-1	MGC – MG	Interfaz del protocolo de control de pasarela troncal (TGCP, *trunking gateway control protocol*) tal como se define en la especificación IPCablecom de TGCP en [UIT-T J.171.1].
pkt-sig-2	CMS – S-CSCF CMS – I-CSCF MGC – BGCF MGC – S-CSCF MGC – I-CSCF	Permite que el S-CSCF y el I-CSCF intercambien señalización de sesión con el CMS para permitir que los E-MTA establezcan sesiones de voz con los UE. También permite que BGCF, I-CSCF y S-CSCF intercambien señalización de sesión con el MGC para el interfuncionamiento con la RTPC.

I.5.2 Mejoras de IPCablecom2 al IMS

Aunque muchas de los componentes e interfaces definidas en el IMS tienen una amplia aplicabilidad en otras industrias, la versión 6 del IMS es todavía una arquitectura centrada en aspectos inalámbricos y diseñada para satisfacer las necesidades de negocio y operacionales de la industria inalámbrica. Por lo tanto, no satisface todas las necesidades de la industria del cable. IPCablecom2 mejora el IMS para soportar los requisitos tecnológicos específicos de la industria del cable y también para incluir los requisitos de negocio y operacionales de un operador de cable.

3GPP está desarrollando nuevas versiones de las especificaciones del IMS. Las actualizaciones futuras de IPCablecom2 se alinearán con estas nuevas versiones según sea necesario.

I.5.2.1 Acceso de banda ancha por cable

El acceso radioeléctrico está típicamente limitado por la escasez de recursos y un elevado retardo. Por lo tanto, el IMS obliga a incluir mecanismos especiales y ampliaciones de SIP para mitigar dichas limitaciones. Puesto que un acceso de banda ancha por cable no presenta las limitaciones de anchura de banda y de retardo típicas de los accesos radioeléctricos, dichas capacidades son opcionales en IPCablecom2.

La inclusión en los UE de las extensiones SIP siguientes, obligatorias en la versión 6 del IMS, son opcionales en IPCablecom2.

I.5.2.1.1 Modificadores de anchura de banda para RTCP

La [IETF RFC 3556] añade atributos SDP que permiten al UE especificar explícitamente la anchura de banda RTCP máxima que desea recibir del UE distante. Ello permite a un UE IMS reducir la utilización del recurso de acceso radioeléctrico especificando un valor de anchura de banda reducido de RTCP (que puede ser cero). En IPCablecom2, es opcional que los UE soporten los modificadores de anchura de banda RTCP. Si el UE soporta esta extensión, debe respetar los atributos de anchura de banda RTCP que reciba a fin de permitir el interfuncionamiento con los UE IMS que utilicen dichos parámetros. Asimismo, el UE debe poder enviar los modificadores de anchura de banda RTCP basados en valores configurados localmente (el valor configurado puede estar basado en el tipo de red de acceso).

I.5.2.1.2 P-Associated-URI (URI asociado privado)

La [IETF RFC 3455] define una cabecera P-Associated-URI (URI asociado privado) que se utiliza como parte del registro implícito que informa al UE de las múltiples identidades públicas en el conjunto de registros implícitos. Ello reduce el tráfico de mensajes de registro ya que pueden registrarse múltiples identidades públicas con una única transacción. En IPCablecom2, es opcional que un UE soporte la cabecera P-Associated-URI.

I.5.2.1.3 Compresión SIP

La [IETF RFC 3486] proporciona una capacidad de compresión de mensajes SIP que reduce la anchura de banda de señalización utilizada y el retardo en la red de acceso radioeléctrica. En IPCablecom2, es opcional que un UE soporte la compresión SIP. El P-CSCF controla si la compresión SIP se permite o no, en base a datos configurados localmente o en función del tipo de red de acceso de la que se informa en la cabecera P-Access-Network-Info (información privada de red de acceso).

I.5.2.1.4 Temporizadores SIP

El IMS modifica (amplía) los intervalos de temporización de los mensajes SIP a fin de reducir la carga de señales en la red de acceso y para tolerar el creciente retardo del acceso radioeléctrico. En IPCablecom2, el UE debe ser conforme con los intervalos de temporización SIP normalizados especificados en [IETF RFC 3261].

I.5.2.2 Modularidad

En IPCablecom2 se exige modularidad a nivel de UE a fin de permitir el interfuncionamiento con puntos extremos que no sean SIP 3GPP, y que los operadores puedan ajustar sus despliegues a ofertas de servicio específicas. Por lo tanto, algunas de las extensiones SIP que son obligatorias en la versión 6 del IMS se consideran opcionales en IPCablecom2.

I.5.2.2.1 Respuesta provisional fiable

La [IETF RFC 3262] define una petición SIP denominada PRACK (acuse de recibo de respuesta provisional) que se utiliza para habilitar un medio bidireccional temprano y asegurar una entrega fiable de respuestas provisionales. En IPCablecom2, es obligatorio que los UE soporten PRACK, y su utilización debe poder configurarse de alguno de los modos siguientes:

1) Requerido – El UE debe incluir la etiqueta de opción "100rel" en el campo de cabecera SIP *Require* (Requerir) de la petición INVITE, de forma que sólo pueda establecer sesiones con otros UE que soporten el PRACK.

2) Negociado – El UE debe incluir la etiqueta de opción "100rel" en el campo de cabecera SIP *Supported* (Soportado) de la petición INVITE de forma que pueda negociar si se utiliza o no el PRACK en función de si éste es o no soportado por el UE distante.

I.5.2.2.2 UPDATE (actualizar)

La [IETF RFC 3311] define una petición SIP denominada UPDATE (actualizar) que se utiliza para la actualización de las sesiones de medios antes de responder (principalmente para las precondiciones). En IPCablecom2 es obligatorio soportar UPDATE en el UE (es decir, el UE debe siempre anunciarlo en la cabecera *Allow* (Permitir), pero su uso es opcional. Por ejemplo, el UE puede optar por no enviar UPDATE si conoce que el UE distante no lo soporta en función de lo recibido en la cabecera *Allow* (Permitir) entrante.

I.5.2.2.3 Lote de evento registro (Reg-Event)

La [IETF RFC 3680] define un nuevo lote de evento denominado Reg-Event (evento de registro) que la red utiliza para informar al UE que ha sido desregistrado. La red puede utilizar este lote de evento para impedir que un UE acceda a los servicios de la red o para provocar que un UE se desregistre para una reasignación de S-CSCF. En IPCablecom2, es opcional que un UE soporte este lote de evento. Si lo soporta, el UE debe tener controles de configuración para deshabilitar su uso.

I.5.2.2.4 Cabecera P-Access-Network-Info

La [IETF RFC 3455] define una cabecera SIP denominada P-Access-Network-Info (información privada de red de acceso) que permite informar a la red de la tecnología de acceso (por ejemplo, radio, 802.11, DOCSIS). En IPCablecom2, es opcional que el UE soporte P-Access-Network-Info. Si lo soporta, el UE sólo informará P-Access-Network-Info si conoce el tipo de tecnología de acceso que utiliza. Por ejemplo, un MTA integrado puede conocer que su red de acceso es DOCSIS, mientras que un cliente software puede no conocer si su acceso es DOCSIS o WiFi.

I.5.2.2.5 Inhabilitación de la seguridad de la señalización

En IPCablecom2 es obligatorio soportar la seguridad de la señalización del UE y del P-CSCF. No obstante, el P-CSCF debe soportar parámetros de configuración que permitan inhabilitar la seguridad de la señalización entre el UE y el P-CSCF. El P-CSCF debe soportar tres modos de funcionamiento que se aplican a todas las asociaciones de señalización del UE con el P-CSCF:

1) Seguridad de señalización desconectada: la seguridad de la señalización está siempre desconectada en todos los UE servidos por el P-CSCF.
2) Seguridad de señalización conectada: la seguridad de la señalización está habilitada en todos los UE servidos por el P-CSCF.
3) Seguridad de señalización negociada: la seguridad de la señalización está conectada en todos los UE que la soportan (obsérvese que la seguridad de la señalización es obligatoria en los UE de IPCablecom2) y desconectada en todos los UE que no la soportan.

I.5.2.3 Servicios

La arquitectura de IPCablecom2 básica debe soportar algunas capacidades básicas adicionales para servicios tales como la telefonía SIP residencial y la integración entre la componente celular y de acceso inalámbrico, no soportada por la versión 6 del IMS.

I.5.2.3.1 Portabilidad de número y encaminamiento a través de operador del URI Tel

En IPCablecom2 la portabilidad de la numeración es opcional para el S-CSCF y obligatoria para el MGC. La BGCF permite la adición en toda la red de un operador preasignado. El UE soporta estos parámetros opcionalmente. Obsérvese que un UE que soporte Tel URI debe también soportar estos parámetros.

I.5.2.3.2 URI de agente de usuario encaminable globalmente (GRUU, *globally routable user agent URI*)

GRUU define un mecanismo que permite que un registrador proporcione una dirección de contacto encaminable globalmente hasta un agente de usuario que se esté registrando. Es una facilidad que

requieren determinadas funcionalidades, tales como a transferencia de llamada, que deben tener capacidad para encaminar una petición iniciada durante el diálogo hacia una instancia registrada específica de una dirección-de-registro (AOR, *address-of-record*) cuando existen múltiples instancias registradas. En IPCablecom2, es opcional que el UE soporte GRUU, pero es obligatorio para los componentes de red que se ven afectados por el GRUU (por ejemplo, S-CSCF). Un UE que soporte GRUU debe utilizar la AOR como dirección de contacto cuando interfuncione con UE distantes que no soporten GRUU.

I.5.2.3.3 Proyecto de documento Internet (Internet-Draft) – Lote de eventos de registro GRUU (*GRUU reg-event package*)

El registro implícito permite registrar varias identidades públicas en una única transacción REGISTER. La respuesta a REGISTER puede incluir un único URI GRUU. Por lo tanto, cuando se soportan tanto GRUU como el registro implícito, debe de haber una forma de comunicar múltiples GRUU al UE. Esto se consigue utilizando una extensión del lote de eventos Reg (registro) que permite comunicar múltiples URI GRUU al lote de eventos Reg en un NOTIFY.

I.6 Requisitos del IMS para IPCablecom2

En esta cláusula se describen los requisitos que actualmente no soporta la versión 6 del IMS pero que son necesarios en la arquitectura de señalización SIP de IPCablecom2.

I.6.1 Señalización segura SIP

IPCablecom2 permite que se inhabilite la seguridad de la señalización entre el UE y el P-CSCF. En esta cláusula se destaca en primer lugar el modelo de seguridad de señalización definido en el IMS del 3GPP, describiéndose a continuación el impacto sobre el IMS derivado de permitir el acceso a servicios IMS sin señalización SIP segura entre el UE y el P-CSCF.

I.6.1.1 Descripción

La arquitectura de seguridad del IMS [UIT-T J.366.7] se basa en varias relaciones de seguridad obligatorias, dos de las cuales están estrechamente ligadas con los procedimientos de registro del IMS:

1) Autenticación mutua entre el usuario y red.

2) Asociación de seguridad entre el UE y el P-CSCF, que protege la integridad y ofrece una protección opcional para la confidencialidad de la señalización SIP (es decir, seguridad en la señalización).

De conformidad con los procedimientos de registro del IMS, el UE envía en primer lugar una petición inicial REGISTER al P-CSCF, que encamina la petición al S-CSCF que sirve al usuario. Dado que aún no se ha establecido una asociación de seguridad entre el UE y el P-CSCF, la petición inicial REGISTER se envía sin protección. El S-CSCF determina que la petición REGISTER recibida se envió sin protección verificando el parámetro "integridad protegida" en el campo cabecera *Authorization* (autorización) de SIP. Debido a que la petición REGISTER se envió sin protección y que el usuario no está aún registrado, el S-CSCF inicia los procedimientos de autenticación mutuos generando una respuesta 401 (no autorizado) a la petición REGISTER sin protección, y el S-CSCF arranca un temporizador reg-await-auth (espera de autenticación para registro).

Después de recibir la respuesta 401 (Unauthorized), el UE establece un conjunto de asociaciones de seguridad con el P-CSCF. El UE envía entonces una segunda petición REGISTER que contiene la respuesta al desafío de autenticación, que se envía protegida sobre la asociación recién establecida y se encamina al mismo S-CSCF. Debido a que la petición REGISTER se había enviado protegida y a que está en curso un procedimiento de autenticación para este usuario (es decir, existe un temporizador "reg-await-auth" en marcha para este usuario), el S-CSCF autentica al usuario

verificando la respuesta al desafío de autenticación. Una vez que el S-CSCF completa satisfactoriamente los procedimientos de registro, se envía al UE una respuesta 200 (OK).

Con la excepción de una petición REGISTER inicial, el IMS requiere que todos los mensajes SIP hacia y desde el UE se envíen protegidos sobre la asociación de seguridad. La asociación de seguridad también permite la autenticación del origen de los datos, lo cual permite que el P-CSCF confirme la identidad del UE.

La seguridad de la señalización es una capacidad obligatoria del UE en la arquitectura SIP de IPCablecom2. No obstante, IPCablecom2 permite que la seguridad de señalización se desactive de las formas siguientes:

1) el UE puede ser configurado [UIT-T J.364] para tener desactivada la seguridad de la señalización; o

2) el P-CSCF puede ser configurado para tener desactivada la seguridad de la señalización para todos los UE que accedan a los servicios IMS a través de dicho P-CSCF.

Además, existen ciertas peticiones que pueden no requerir seguridad de la señalización. En el IMS de IPCablecom2, la única petición de este tipo es la suscripción al lote de eventos "ua-profile" (perfil de agente de usuario).

I.6.1.2 Componentes afectados

En esta cláusula se describen los componentes del IMS que se ven afectados por permitir el acceso a servicios IMS sin señalización segura entre UE y P-CSCF, así como la naturaleza del efecto sobre el componente.

NOTA – En el apéndice III se exponen consideraciones de seguridad adicionales relativas a la desactivación de la seguridad de señalización.

I.6.1.2.1 Equipo de usuario (UE)

Un UE de IPCablecom2 debe soportar la negociación y establecimiento de asociaciones de seguridad tal como se describe en el IMS. No obstante, aunque no se recomienda la desactivación de la seguridad, un UE de IPCablecom2 debe ser suficientemente flexible como para interfuncionar en un entorno en el que los procedimientos de seguridad se hayan desactivado.

En IPCablecom2, el UE no inicia una asociación de seguridad en los casos siguientes:

- Cuando el UE recibe una indicación desde el P-CSCF durante el registro que señala que la seguridad de señalización se ha desactivado.
- Cuando el UE se ha configurado para que la seguridad de señalización esté desactivada, tal como se describe en [UIT-T J.364], y no ha recibido una indicación del P-CSCF durante el registro inicial que señale que la seguridad de señalización sea necesaria.

Si el UE incluye la etiqueta de opción "sec-agree" (acuerdo de seguridad) en el campo "Require" (requerir) de la cabecera, tal como se define en [IETF RFC 3329], cuando se envía una petición REGISTER inicial y se recibe una respuesta 420 (Bad Extensión, extensión errónea) con el valor de la etiqueta de opción "sec-agree" en el campo "Unsupported" (no soportado) de la cabecera, el UE debería reenviar la petición REGISTER y no seguir los procedimientos de [IETF RFC 3329].

Si el UE se configura para que la seguridad de señalización esté desactivada y el UE no ha recibido una respuesta 494 (Security Agreement Required, acuerdo de seguridad requerido), el UE no debe seguir los procedimientos descritos en [IETF RFC 3329].

Si el UE se registra con éxito sin haber establecido una asociación de seguridad, a cualquier petición inicial o transacción autónoma (excluyendo REGISTER) se aplica lo siguiente:

- Si el UE soporta la cabecera "P-Preferred-Identity", debe insertarlo y fijar su valor con una identidad de usuario pública registrada del propio usuario.

- Si el UE no soporta la cabecera "P-Preferred-Identity", el UE se asegurará de que el campo cabecera "From" toma un valor de identidad de usuario pública del propio usuario. En este caso, puede ocurrir que no se mantenga la privacidad.

En base a la política local, se pueden permitir peticiones de suscripción al lote de eventos ua-profile (perfil de agente de usuario) con anterioridad al registro. Si el UE no está registrado, a las peticiones SUBSCRIBE realizadas al lote de eventos ua-profile se les aplica lo siguiente:

- El UE debe incluir la cabecera "From" y fijar su valor con la identidad de usuario pública obtenida tal como se describe en la cláusula I.6.13 "Encaminamiento de SUBSCRIBEs para información de configuración".
- Si el UE soporta la cabecera "P-Preferred-Identity", el UE debe insertarla y fijar su valor con la misma identidad de usuario pública incluida en el campo cabecera "From".

I.6.1.2.2 P-CSCF

En IPCablecom2, el P-CSCF debe soportar los requisitos de seguridad de la señalización tal como se definen en el apéndice III.

El P-CSCF puede configurarse para que la seguridad de señalización esté "desactivada" o sea "requerida" para todos los UE que acceden a servicios IMS a través de dicho P-CSCF. El P-CSCF también puede configurarse para que la seguridad de señalización sea "opcional"; en ese caso, el P-CSCF determina si la seguridad de señalización está desactivada para un UE determinado en base a una indicación recibida del UE durante el registro inicial.

Si el P-CSCF se configura para que la seguridad de señalización sea "opcional" o esté "desactivada", se aplica lo siguiente:

- El P-CSCF debe aceptar las peticiones REGISTER sin la etiqueta de opción "sec-agree" en la cabecera "Require" tal como se define en [RFC 3329]. En este caso, el P-CSCF debe ignorar los procedimientos relativos al acuerdo del mecanismo de seguridad especificado en [UIT-T J.364].
- El P-CSCF debería permitir peticiones no protegidas distintas a REGISTER.

Si el P-CSCF se configura para tener la seguridad de señalización "desactivada", se aplica lo siguiente:

- El P-CSCF debe aceptar peticiones REGISTER sin la etiqueta de opción "sec-agree" en la cabecera "Require" tal como se define en [IETF RFC 3329]. En este caso, el P-CSCF debe ignorar los procedimientos relativos al acuerdo del mecanismo de seguridad especificado en [UIT-T J.366.4].
- Si el P-CSCF recibe una petición REGISTER de un UE con la etiqueta de opción "sec-agree" en el campo cabecera "Require" tal como se define en [IETF RFC 3329], el P-CSCF debe rechazar la petición con una respuesta 420 (Bad Extension, extensión errónea) e incluir la etiqueta de opción "sec-agree" en la cabecera "Unsupported".
- El P-CSCF debería permitir peticiones no protegidas distintas a REGISTER.

Si el P-CSCF se configura de forma que la seguridad de señalización es "requerida", se aplica lo siguiente:

- Si el P-CSCF recibe una petición REGISTER de un UE sin la etiqueta de opción "sec-agree" en la cabecera "Require" tal como se define en [IETF RFC 3329], el P-CSCF rechazará la petición con una respuesta 494 (Security Agreement Required, acuerdo de seguridad requerido).

El P-CSCF debería confirmar la identidad del originador de la petición (es decir, insertar una cabecera "P-Asserted-Identity") y eliminar la cabecera "P-Preferred-Identity" en caso de estar

presente, sólo para peticiones que no sean REGISTER y hayan sido recibidas sobre una asociación de seguridad.

Si el P-CSCF recibe una petición que no sea REGISTER y sin una cabecera "Route" es decir, una petición de un usuario no registrado), el P-CSCF retransmitirá la petición al I-CSCF del usuario servido.

I.6.1.2.3 I-CSCF

En IPCablecom2, el I-CSCF debe soportar requisitos de seguridad de señalización tal como se define en el apéndice III.

I.6.1.2.4 S-CSCF

En IPCablecom2, el S-CSCF debe soportar requisitos de seguridad de señalización tal como se define en el apéndice III.

El S-CSCF puede configurarse para que la seguridad de señalización sea "requerida" para todos los UE que accedan a servicios IMS a través de dicho S-CSCF. El S-CSCF también puede configurarse para que la seguridad de señalización sea "opcional"; en ese caso el S-CSCF acepta peticiones REGISTER no protegidas autenticadas. El operador debe coordinar las configuraciones del S-CSCF y del P-CSCF.

Si el S-CSCF y el P-CSCF se configuran para permitir el acceso a servicios IMS sin señalización SIP segura para uno o más UE, se aplica lo siguiente:

- Si el S-CSCF recibe una petición REGISTER y la autenticación de dicho usuario está en curso (es decir, el temporizador "reg-await-auth" está en marcha), el S-CSCF ejecutará los procedimientos de registro especificados en [UIT-T J.366.4] como si el valor del parámetro "integrity-protected" (integridad protegida) de la cabecera "Authorization" fuera "sí".
- Si mientras se está realizando el procesamiento en origen de una identidad de usuario pública registrada, el S-CSCF recibiera una petición en la que faltara la cabecera "P-Asserted-Identity" que por otra parte requiere [UIT-T J.366.4], entonces:
  - El S-CSCF identificará al originador en base al valor contenido en la cabecera "P-Preferred-Identity", si existe, o en base a la cabecera "From" si no existiera la cabecera "P-Preferred-Identity".
  - Si la petición contiene una respuesta de autenticación válida, el S-CSCF insertará una cabecera "P-Asserted-Identity" y eliminará la cabecera "P-Preferred-Identity"en caso de existir.
  - Si la petición no contiene una respuesta de autenticación válida, el S-CSCF debería desafiar la petición generando una respuesta a 401 (Unauthorized).

Si el S-CSCF recibe una petición SUBSCRIBE dirigida al lote de eventos "ua-profile" y procedente de una identidad de usuario pública no registrada pero conocida, el S-CSCF debería procesar el origen como si el usuario estuviera registrado.

I.6.1.3 Especificación complementaria al IMS para IPCablecom2

En la especificación complementaria al IMS para IPCablecom2 [UIT-T J.366.4] se incluyen los requisitos necesarios para la señalización segura SIP.

I.6.2 Soporte de IPv4 y de IPv6

I.6.2.1 Descripción

[UIT-T J.366.4] especifica que a los UE y a las entidades del susbsistema IMS se les asignen direcciones IPv6. Como parte del soporte de la "banda ancha fija" por parte de la versión 7 del IMS del 3GPP, esto se ha ampliado a fin de permitir que a los UE y los subsistemas IMS se les pueda

asignar direcciones IPv4, direcciones IPv6 o ambas. IPCablecom2 requiere que se soporte IPv4 y que los UE y los componentes del IMS de IPCablecom2 soporten ambos tipos de direcciones.

Algunos procedimientos de [UIT-T J.366.4] se describen explícitamente como específicos para IPv6. Dichos procedimientos no son aplicables a clientes IPv4 (por ejemplo, "Cambio de dirección IPv6 por motivos de privacidad").

I.6.2.2 Componentes afectados

Los cambios necesarios para permitir IPv4 están incluidos en [UIT-T J.366.4]. Esta petición de modificación de las especificaciones del 3GPP incluye los siguientes cambios relevantes:

- Cambios de URI y de la asignación de direcciones, a fin de permitir la asignación de direcciones IPv4, IPv6, o de ambos tipos a los UE y a entidades del subsistema IMS (cláusula 4.2 de [UIT-T J.366.4]).
  - La utilización de IPv6 en IPCablecom2 requiere estudios adicionales. Inicialmente sólo se asume la utilización de IPv4. El cambio se hará de acuerdo con los cambios que realice el 3GPP.
- Modificaciones a los procedimientos del S-CSCF, mediante la generalización de un procedimiento que verifique un tipo de dirección IP en el SDP, cuando se da un caso de error por el que el extremo distante indica que no soporta el tipo de dirección (cláusula 5.4.3.2 de [UIT-T J.366.4]).
  - El interfuncionamiento entre una red IPCablecom2 basada en IPv4 y redes basadas en IPv6 requiere estudios adicionales, pero este cambio se incluye para incorporar todos los cambios conexos derivados de CR de la versión 7 del 3GPP.
  - Las modificaciones de los procedimientos del UE para el descubrimiento de P-CSCF a las referencias relevantes a procedimientos DHCP basados en IPv4 (cláusula 9.2.1 de [UIT-T J.366.4]).
  - Este cambio particular no es relevante para IPCablecom2 puesto que se utilizan procedimientos alternativos para el descubrimiento de P-CSCF, pero se incluye para incorporar todos los cambios conexos de CR de la versión 7 de 3GPP.

I.6.2.3 Especificación complementaria al IMS para IPCablecom2

En la especificación complementaria al IMS para IPCablecom2, cláusulas 4.2, 5.4.3.2 y 9.2.1 de [UIT-T J.366.4], se incluyen los requisitos necesarios para soportar IPv4 e IPv6:

I.6.3 Compresión SIP

I.6.3.1 Descripción

En la versión 6 del IMS del 3GPP [UIT-T J.366.4] es obligatorio que el UE y el P-CSCF soporten la compresión de señalización (SigComp) tal como se define en [IETF RFC 3320] y la compresión SIP tal como se define en [IETF RFC 3486]. La compresión SIP es obligatoria al objeto de minimizar retardos sobre un acceso 3GPP de anchura de banda reducida. Para el acceso de banda ancha por cable de IPCablecom2, no son de aplicación este conjunto de consideraciones. Obsérvese que, como parte del soporte de la "banda ancha fija" que ofrece la versión 7 del IMS del 3GPP, es opcional para los UE que utilizan tecnología de acceso de banda ancha soporten y utilicen la compresión SIP, no siendo obligatorio que el P-CSCF la utilice (por ejemplo, cuando lo soporte el cliente) si el UE utiliza tecnología de acceso de banda ancha.

IPCablecom2 incorpora estos cambios de la versión 7 del IMS del 3GPP sobre la compresión SIP: la compresión de señalización (SigComp), definida en [IETF RFC 3320], y la compresión SIP, definida en [IETF RFC 3486], son de implementación opcional en un UE de IPCablecom2 y de utilización opcional en un P-CSCF.

La implementación de los requisitos anteriores es función del conocimiento que se tenga de si el UE se encuentra en una red de banda ancha utilizando un nuevo valor de tipo de acceso, según se indique en la cabecera "P-Access-Network-Info", que representa la tecnología de red de acceso DOCSIS. Para un análisis más detallado, véase la cláusula I.6.12.1.2.

NOTA – La solución de la versión 7 del IMS del 3GPP está sujeta a estudios adicionales en el seno del 3GPP para determinar si existen otras formas más adecuadas de determinar retardos de acceso y sobre si debería utilizarse la compresión SIP. En este sentido, IPCablecom2 se podrá realinear con cualquier ulterior cambio en este sentido.

I.6.3.2 Componentes afectados

Los cambios requeridos se han identificado e incluido en la versión 7.

I.6.3.2.1 Equipo de usuario (UE)

En los UE utilizados en una red de acceso de banda ancha es opcional soportar SigComp y la compresión SIP.

Si el UE soporta SigComp y la compresión SIP, no debería utilizarlas si no se encuentra en una red de acceso de banda ancha (en base al tipo de acceso reflejado en "P-Access-Network-Info"), o si el UE desconoce el tipo de acceso.

I.6.3.2.2 P-CSCF

Para un P-CSCF desplegado en una red de acceso de banda ancha por cable, es obligatorio soportar SigComp y la compresión SIP, pero su utilización es opcional.

Si el UE soporta SigComp, el P-CSCF no debería proponer utilizar la compresión SIP si el UE se encuentra en una red de acceso de banda ancha por cable (en base al tipo de acceso reflejado en "P-Access-Network-Info"), o si el tipo de acceso es desconocido.

I.6.3.3 Especificación complementaria al IMS para IPCablecom2

La especificación complementaria al IMS para IPCablecom2, cláusula 8 de [UIT-T J.366.4], incluye los requisitos necesarios para la compresión SIP.

I.6.4 Fiabilidad de las respuestas provisionales SIP

I.6.4.1 Descripción

La fiabilidad de la respuesta provisional del protocolo SIP es un extensión definida en [IETF RFC 3262] para soportar múltiples aplicaciones. En primer lugar, es necesaria cuando se establecen sesiones utilizando la extensión de precondiciones SIP. En segundo lugar, permite que exista una oferta/respuesta SDP como parte de una petición INVITE y una respuesta provisional inicial, necesaria para soportar medios iniciales (por ejemplo, en determinados escenarios de interfuncionamiento con la RTPC). Finalmente, garantiza que la acción tomada por un UE al recibir una respuesta provisional tiene realmente lugar (por ejemplo, que un UE originario aplique un tono de llamada cuando reciba una respuesta 180 a INVITE).

En la versión 6 del IMS del 3GPP es obligatoria la fiabilidad de las respuestas provisionales del UE cuando éste inicia una sesión, como forma de soportar la extensión de precondiciones SIP. IPCablecom2 actualizará estos requisitos para permitir que un UE, en base a los datos de configuración, interfuncione con UEs que no sean 3GPP y que no soporten este extensión SIP.

I.6.4.2 Componentes afectados

Los efectos derivados de permitir el interfuncionamiento de un UE con puntos extremos que no soporten la extensión SIP de respuesta provisional fiable se limitan al propio UE.

I.6.4.2.1 Equipo de usuario (UE)

Un UE que soporte sesiones debe soportar la extensión de respuesta provisional fiable, tal como se define en [IETF RFC 3262].

Un UE puede configurarse para que sea necesario que soporte la extensión de respuesta provisional fiable. En este caso, cualquier intento de establecimiento de una sesión con otro UE que no soporte dicha extensión fracasará.

Alternativamente, un UE puede configurarse para negociar que se soporte la extensión de respuesta provisional fiable, de forma que la extensión sólo se utilice si la soportan el UE de inicio y de terminación.

I.6.4.3 Especificación complementaria al IMS afectada

La especificación complementaria al IMS para IPCablecom2 incluye los requisitos asociados a la fiabilidad de las respuestas provisionales SIP.

Véase la cláusula 5.1 y el cuadro A.4 de [UIT-T J.366.4].

I.6.5 Actualización de SIP

I.6.5.1 Descripción

El método de extensión SIP UPDATE definido en [IETF RFC 3311] permite a un cliente SIP actualizar los parámetros de una sesión. En particular, se utiliza para soportar precondiciones SIP [IETF RFC 3312].

La versión 6 del IMS del 3GPP obliga a soportar el método UPDATE como parte de la extensión de precondiciones. IPCablecom2 amplía estos requisitos para permitir la utilización facultativa de UPDATE al margen de las precondiciones. Específicamente, un UE IPCablecom2 debe soportar UPDATE, pero debería adoptar procedimientos para maximizar el interfuncionamiento con los UE que no soporten UPDATE (por ejemplo, sustitución de re-INVITE).

I.6.5.2 Componentes afectados

Los efectos debidos a permitir que un UE interfuncione con puntos extremos que no soporten la extensión UPDATE de SIP se limitan exclusivamente al UE.

I.6.5.2.1 Equipo de usuario (UE)

Un UE debe soportar UPDATE en sesiones establecidas utilizando precondiciones.

Un UE también puede requerir que se soporte UPDATE en sesiones establecidas sin precondiciones. En este caso, el establecimiento de una sesión con un UE que no soporte UPDATE fracasará.

Alternativamente, un UE puede negociar soportar UPDATE en sesiones establecidas sin precondiciones, de forma que la extensión sólo se utilice si es soportada por ambos UE, el iniciador y el de terminación.

I.6.5.3 Especificación complementaria al IMS para IPCablecom2 afectada

En la especificación complementaria al IMS para IPCablecom2 IMS se incluyen los requisitos necesarios para el UPDATE SIP. Véase la cláusula 5.1 y el cuadro A.4 de [UIT-T J.366.4].

I.6.6 Precondiciones SIP

I.6.6.1 Descripción

La arquitectura de señalización de IPCablecom2 puede soportar opcionalmente las precondiciones SIP, tal como se definen en [IETF RFC 3312] y actualizadas según [IETF RFC 4032]. Aunque originalmente SIP las hizo obligatorias, se han relajado los requisitos de las precondiciones SIP.

Éstas han dejado de ser obligatorias en la versión 6 del IMS de 3GPP. Los cambios se incorporarán en la siguiente versión de las especificaciones de la versión 6 del IMS.

I.6.6.2 Componentes afectados

En esta cláusula se describen los efectos sobre los componentes por el hecho de que el UE soporte opcionalmente la extensión de las precondiciones SIP.

I.6.6.2.1 Equipo de usuario (UE)

Los equipos de usuario de IPCablecom2 pueden soportar precondiciones SIP. Si las soporta, el UE debe cumplir [IETF RFC 3312] y [IETF RFC 4032].

El UE de IPCablecom2 debería negociar la utilización de precondiciones SIP. El UE debería indicar la forma en que soporta las precondiciones SIP mediante las cabeceras SIP apropiadas (Soportada o Requerir) y ser flexible para permitir el establecimiento de sesiones con UE que no soporten precondiciones. Por ejemplo, un UE que termine un diálogo SIP debería incluir la etiqueta de opción "precondición" en la cabecera "Require" (requerir) si la petición de inicio de diálogo recibida del UE de origen indica que soporta las precondiciones SIP con la etiqueta de opción "precondiciones" en la cabecera "Supported" (soportado).

I.6.6.3 Especificación complementaria al IMS para IPCablecom2

En la especificación complementaria al IMS para IPCablecom2 se incluyen los requisitos necesarios para precondiciones SIP: Véanse las cláusulas 5.1.3, 5.1.4 y 6.1 de [UIT-T J.366.4].

I.6.7 Modificadores de la anchura de banda de SDP para RTCP

I.6.7.1 Descripción

El SDP normalizado no dispone de un mecanismo para controlar explícitamente la anchura de banda RTCP. En lugar de ello, la anchura de banda RTCP se fija al 5% de la anchura de banda de la sesión. En [IETF RFC 3556] se introducen dos nuevos modificadores de anchura de banda SDP para RTCP que pueden utilizarse para fija explícitamente la anchura de banda RTCP a cualquier valor, con independencia de la anchura de banda de la sesión RTP. El IMS utiliza este mecanismo para limitar la anchura de banda RTCP a un valor inferior al 5% (posiblemente a cero) en despliegues en los que el acceso radioeléctrico es escaso y caro.

Dado que el acceso de banda ancha no tiene las restricciones de anchura de banda de la radio, no es necesario limitar la anchura de banda RTCP por debajo del valor por defecto del 5% en la red de acceso de IPCablecom. Sin embargo, se considera de utilidad que el UE de IPCablecom2 soporte dichos modificadores de anchura de banda cuando los reciba de un UE IMS a fin de evitar sobrepasar la atribución de anchura de banda RTCP en la red de acceso radioeléctrica IMS. Por lo tanto, es opcional que los UE de IPCablecom2 soporten los modificadores de anchura de banda RTCP.

I.6.7.2 Componentes afectados

En esta cláusula se describen los efectos sobre los componentes por el hecho de que el UE soporte opcionalmente los modificadores de anchura de banda RTCP.

I.6.7.2.1 Equipo de usuario (UE)

Para los UE de IPCablecom2 desplegados en una red de acceso de banda ancha de cable es opcional soportar [IETF RFC 3556].

I.6.7.3 Especificación complementaria al IMS para IPCablecom2

En la especificación complementaria al IMS para IPCablecom2 se incluyen, los requisitos necesarios para los modificadores de anchura de banda SDP para RTCP.

Véase la cláusula 6 de [UIT-T J.366.4].

I.6.8 Lote de eventos del estado de registro

El lote de eventos SIP para el estado de registro es una función opcional del UE de IPCablecom2.

I.6.8.1 Descripción

Cuando un UE realiza con éxito el registro inicial, se crea el estado de registro en un registrador SIP (es decir, en S-CSCF) para una lista de URI asociados con la identidad de usuario pública que había sido registrada. La lista de los URI incluye la identidad del usuario público que fue explícitamente registrada (salvo que esté prohibida), el conjunto de identidades de usuario públicas implícitamente registradas y, posiblemente, otras identidades de usuario públicas asociadas.

El estado de registro de un URI en la lista cambia dinámicamente por motivos tales como:

- Desregistro iniciado por la red: de acuerdo con la política de administrador local, la red puede desregistrar una identidad de usuario pública. Esto puede ocurrir, por ejemplo, debido al impago de facturas.
- Re-autenticación iniciada por la red: de acuerdo con la política de administrador local, la red puede reducir el plazo de tiempo de expiración de un registro actual a fin de forzar una re-autenticación del UE. Esto puede ocurrir, por ejemplo, cuando se detecta fraude.
- Registro de múltiples dispositivo: las direcciones de contacto ligadas a cualquiera de los URI de la red pueden cambiar debido al registro de otros dispositivos.

De conformidad con los procedimientos de registro del IMS, el UE debe suscribirse a la información del estado de registro después de un registro inicial exitoso, y mantener la suscripción hasta que todos los URI de la lista se hayan desregistrado. Esta suscripción permite notificar al UE eventos tales como los cambios en el estado de registro (es decir, de "activo" a "terminado"), reducción de los temporizadores de expiración de registro, y modificaciones en las vinculaciones de direcciones de contacto.

I.6.8.2 Componentes afectados

En esta cláusula se describen los efectos sobre los componentes por el hecho de que el UE soporte opcionalmente el lote de eventos de registro ("Event Reg").

I.6.8.2.1 Equipo de usuario (UE)

Para un UE de IPCablecom2 es opcional soportar el "Lote de eventos SIP para registros" [IETF RFC 3680]. Si el UE no soporta el lote de eventos de estado de registro descrito en [IETF RFC 3680], no podrá realizar los procedimientos descritos en [UIT-T J.366.4] relativos a la suscripción y notificación de información del estado de registro.

Las implicaciones básicas por el hecho de no soportar [IETF RFC 3680] son:

- El UE no recibe indicación explícita de los AOR adicionales que se registren implícitamente, salvo que soporte la cabecera opcional "P-Associated-URI" (véase la cláusula I.6.12).
- El UE puede quedar desregistrado sin su conocimiento. Si esto ocurre, el UE no podrá recibir peticiones y la mayoría de las peticiones no relativas al REGISTRO que envíe el UE serán descartadas o rechazadas por el P-CSCF en función de la existencia o no de una asociación de seguridad (véase la cláusula I.6.1).

Si el UE determina que ha sido desregistrado (por ejemplo, se envía una petición para la que vence el temporizador o es rechazada con un código de error adecuado), el UE debería intentar recuperarse utilizando procedimientos específicos de la implementación. A título de ejemplo, un UE podría realizar procedimientos de desregistro iniciados por la red tal como se describe en [UIT-T J.366.4].

Si el UE soporta el lote de eventos de estado de registro, debería soportar la cabecera "P-Associated-URI" a fin de determinar si la identidad de usuario pública utilizada en el registro está prohibida (véase la cláusula I.6.12.2.1).

I.6.8.2.2 P-CSCF

El P-CSCF no se ve afectado. En el IMS es posible que (por ejemplo, como un caso anormal) el P-CSCF reciba peticiones de un UE que, sin saberlo, ha sido desregistrado. Dichos casos pueden ir en aumento si la red IPCablecom2 realiza desregistros o reautenticaciones iniciadas por la red y existen UE que no soportan el lote de eventos de estado de registro.

I.6.9 Portabilidad numérica

I.6.9.1 Descripción

IPCablecom soporta la portabilidad de número local (LNP, *local number portability*) y el encaminamiento no discriminatorio para operadores. En esta cláusula se describe cómo se obtienen y utilizan en una red IPCablecom2 los datos para la portabilidad de número local y el encaminamiento a través de un operador.

Para soportar la portabilidad de número, la red IPCablecom2 debe determinar, cuando proceda, si el número llamado ha sido portado. Si el número llamado ha sido portado a un destino en la RTPC, la red IPCablecom2 debería aplicar una política de encaminamiento basada en el número de encaminamiento de portabilidad y transferir a la RTPC dicho número de encaminamiento, así como el indicador de la base de datos de portabilidad numérica. El mecanismo para obtener los datos de portabilidad numérica está fuera del alcance de este apéndice y puede variar en función de los componentes de IPCablecom2 utilizados para obtener los datos de portabilidad.

Los procedimientos IMS existentes establecen que el S-CSCF resuelva un URI Tel que contenga una dirección E.164 en un URI SIP mediante un mecanismo ENUM/DNS. IPCablecom2 asume que cuando dicho URI Tel se resuelve en un URI SIP, no es necesario que la red IPCablecom2 haga una consulta. En este caso, la petición puede encaminarse en base al URI SIP. Como tal, se asume que el servidor ENUM/DNS que contiene la correspondencia entre dirección E.164 y URI SIP se sincroniza con los procesos de portabilidad local. Los procedimientos/mecanismos para dicha sincronización están fuera del alcance de este apéndice.

Cuando el URI Tel que contiene el número E.164 no puede resolverse en un URI SIP, la red IPCablecom2 obtendrá los datos relativos a la portabilidad de número local para el número llamado donde sea pertinente (por ejemplo, si la petición se debe encaminar a un operador de tránsito, no se exige que la red IPCablecom2 realice la consulta. En su lugar, el operador "N – 1" es quien típicamente debe realizar la consulta.

Por defecto, si la consulta sea necesaria la realiza el MGC cuando la consulta de portabilidad para dicha petición no ha sido ya realizada (obsérvese que dado que se trata de portabilidad local, es razonable que la petición se encamine normalmente al MGC que pueda hacer el encaminamiento adecuado en base al resultado de la consulta).

El S-CSCF también puede soportar capacidades de portabilidad local. Si así es, el S-CSCF debería ser configurable para controlar si deben utilizarse dichas capacidades a fin de proporcionar flexibilidad sobre dónde debe realizarse la consulta de portabilidad. Los mecanismos mediante los que un S-CSCF obtiene los datos de portabilidad local quedan fuera del alcance de este apéndice (los mecanismos pueden incluir mecanismos basados en ENUM, incluidos mecanismos para obtener los datos de portabilidad local de la petición de resolución de E.164 a URI SIP. Dichos mecanismos se sujetan a lo establecido en los proyectos de textos del IETF. La políticas de encaminamiento correspondientes a los casos en los que el S-CSCF resuelve el UIR Tel en un URI SIP y también consigue los datos de portabilidad local asociados al URI quedan fuera del ámbito de este apéndice.

Para un encaminamiento no discriminatorio entre operadores, la red IPCablecom2 selecciona la ruta hacia la RTPC en base al código de acceso de operador marcado o al correspondiente al que el cliente está preasignado, y transfiere el identificador de operador y el indicador de marcación a la RTPC. Ello implica que el URI Tel debería soportar el parámetro código de identificación de operador, "cic" (*carrier identification code*), y el parámetro identificador de servicio alternativo, "dai" (*dial around indicator*), de forma que el MGC pueda seleccionar el grupo de enlaces adecuado y pasar el identificador de servicio alternativo y el código de identificación de operador a la RTPC.

Obsérvese que los requisitos actuales de IPCablecom2 no exigen que se soporte la preasignación de operador independientemente para cada abonado específicamente. En lugar de ello, puede establecerse un operador preasignado para todos los abonados de la red. La BGCF puede permitir que se añada al URI Tel el operador asignado de la red mediante el parámetro "cic", así como actualizar el parámetro "dai". Si se soporta, la BGCF añade estos parámetros de configuración/política de encaminamiento. Obsérvese que estos parámetros pueden haber sido añadidos por un componente de red anterior y en es caso, no deben ser sobre-escritos por la BGCF.

Corresponden al servidor de aplicaciones las responsabilidades siguientes relativas al acceso no discriminatorio:

- Fijación del valor/política a aplicar en relación con el identificador de servicio alternativo para el ID de operador que proporciona un UE en una petición.
- Obtención del código de identificación de operador para llamadas a cobro revertido.
- Completar los valores del código de identificación de operador y del identificador de servicio alternativo en el caso en que un abonado concreto esté preasignado a un operador.

  NOTA – Tal como se ha señalado anteriormente, este no es actualmente un requisito, pero si lo fuera, debería soportarse de esta forma.

IPCablecom2 soporta los requisitos de portabilidad de número y de encaminamiento a través de un operador utilizando los parámetros de portabilidad de número local del URI Tel y el encaminamiento a través de un operador, así como el parámetro identificador de servicio alternativo definido en [UIT-T J.178].

I.6.9.2 Componentes afectados

A fin de soportar la portabilidad de número y el encaminamiento a través de un operador, la información de portabilidad debe ser transportad en la señalización SIP. En concreto, el URI Tel debe soportar los parámetros "rn", "cic"y "npdi", así como el parámetro "dai" definido en [UIT-T J.178]. Esta información se utiliza para los intermediarios (proxies) de encaminamiento (por ejemplo, BGCF) a fin de seleccionar los puntos de salida hacia la RTPC, y por la pasarela RTPC para comunicar la información de encaminamiento correcta a la RTPC. Estos parámetros pueden transportarse en un URI Tel nativo o en el equivalente SIP de un URI Tel, en el que "user = phone" (usuario = teléfono).

I.6.9.2.1 Equipo de usuario (UE)

La única responsabilidad del UE para soportar el encaminamiento a través de un operador es identificar para la red el operador marcado por el usuario cuando hace una llamada. El UE lo hace reconociendo los números marcados por el usuario a través de un mapa de números e identificando el operador en el parámetro "cic" de Tel URI del mensaje INVITE original.

Alternativamente, el mapa de números puede especificar que el UE debe informar de todos los números marcados, incluyendo los números correspondientes al operador en un URI SIP con parámetros de usuario "user=dialstring". Con este enfoque, se requeriría que un servidor de aplicación extrajera el CIC y normalice el URI Tel.

Los mecanismos para configurar el mapa de números a fin de controlar el comportamiento del UE quedan fuera del ámbito de este apéndice.

El UE no juega ningún otro papel para soportar la portabilidad de número.

I.6.9.2.2 S-CSCF

Tal como se especifica en [UIT-T J.366.4], cuando el S-CSCF de origen recibe una petición de URI (Request-URI) del formulario URI Tel, debe intentar resolver la dirección E.164 en un URI SIP globalmente encaminable utilizando ENUM. Si la resolución fracasa, el S-CSCF asume que la llamada está destinada a la RTPC y envía un mensaje INVITE a la BGCF para su ulterior encaminamiento.

IPCablecom2 mejora dichos requisitos para soportar la portabilidad de número. El S-CSCF puede soportar las capacidades de portabilidad de número. Si así ocurre, el S-CSCF proporciona controles de configuración que permiten al operador habilitar o deshabilitar los procedimientos de portabilidad de número. El operador puede así elegir entre consultas de portabilidad de número realizadas por el S-CSCF o por una entidad situada más abajo en la estructura de red, como por ejemplo el MGC o la RTPC:

Si el S-CSCF se ha configurado para soportar la portabilidad de número, una vez que ha determinado que una llamada debe dirigirse a la RTPC, el S-CSCF de origen debe determinar si el número llamada está portado, en cuyo caso, también debe determinar el número de encaminamiento. No se especifica cómo obtiene el S-CSCF esta información (por ejemplo, puede ser mediante una consulta ENUM). Si el número está portado, el S-CSCF de origen debe añadir un parámetro "rn" a la petición URI Tel para identificar el número de encaminamiento y añadir un parámetro "npdi" para indicar que se ha hecho la exploración de la base de datos de portabilidad de número.

Si el S-CSCF se ha configurado para no soportar la portabilidad de número, enviará a la BGCF peticiones destinadas a la RTPC sin rellenar los parámetros URI Tel de portabilidad de número.

Las políticas y procedimientos para la gestión de escenarios en que los URI SIP y URI Tel con información de portabilidad de número se obtienen a partir de un intento de resolución de una dirección E.164 en una URI SIP (si ello es posible mediante algún mecanismo) quedan fuera del alcance de este apéndice.

I.6.9.2.3 BGCF

La BGCF recibe peticiones INVITE del S-CSCF y selecciona la mejor ruta hacia la RTPC en base a una política de encaminamiento configurada localmente. Tal como se especifica en [UIT-T J.366.4], la entrada necesaria para la decisión de encaminamiento es el número de teléfono llamado que se identifica en el URI Tel de la petición INVITE. IPCablecom2 mejora los requisitos de encaminamiento para incluir los parámetros "cic" y "rn" URI Tel, como consecuencia de lo cual, la BGCF puede soportar dichos parámetros en una decisión de encaminamiento. No se especifica cómo dichos parámetros afectan al encaminamiento.

La BGCF puede soportar la adición de los parámetros "cic" y "dai" a la URI Tel para permitir la preasignación a un operador en toda la red. La adición de dichos parámetros se basa en la política de encaminamiento. Los atribuidos de la petición que se encamina puede determinar si se añade un parámetro "cic". La BGCF permitirá que dichos parámetros hayan sido añadidos a la petición por otro componente de red, y por tanto, no sobrescribirá sobre los parámetros si éstos ya han sido aprovisionados.

I.6.9.2.4 MGC

El MGC recibe peticiones de la BGCF para el encaminamiento hacia la RTPC o desde la RTPC hacia la red IPCablecom2.

Las peticiones desde la BGCF pueden tener un URI Tel que incluya los parámetros de operador ("cic") y/o de portabilidad de número ("npdi", "rn").Las peticiones de la RTPC pueden también incluir parámetros de portabilidad de número.

El MGC determinará si se hace una consulta de portabilidad de número basada en una configuración local y el contenido de dicha petición, incluyendo los parámetros recibidos de portabilidad de número.

La política de encaminamiento MGC incluye encaminamiento basado en parámetros del operador y de la portabilidad de número. La información detallada de la política de encaminamiento del MGC queda fuera del alcance de este apéndice.

I.6.10 URI de agente de usuario encaminable globalmente (GRUU)

I.6.10.1 Descripción

En la arquitectura SIP de IPCablecom2, es opcional que el UE soporte el URI de agente de usuario SIP encaminable globalmente (GRUU). El GRUU es beneficioso para IPCablecom2 pues permite ciertas funcionalidades de la llamada, como la transferencia de la llamada, que permiten que una petición SIP se dirija con precisión a una instancia de agente de usuario SIP de un UE. También permite que se definan funcionalidades que se apliquen correctamente a peticiones que se dirigen a una instancia de agente de usuario SIP concreta de un UE, en lugar de hacerlo de forma general a una identidad de usuario pública. Por ejemplo, cuando una petición se dirige a un UE concreto a través de un GRUU, puede ser deseable evitar redirigir la petición a un sistema de correo de voz.

I.6.10.2 Componentes afectados

En esta cláusula se describen los efectos sobre los componentes por el hecho de soportar el GRUU.

I.6.10.2.1 Equipo de usuario (UE)

Un UE de IPCablecom2 que soporte GRUU debe cumplir los requisitos y directrices del agente de usuario en desarrollo.

- El UE debe solicitar un GRUU cuando se registra, y recuperar y retener el GRUU facilitado en la respuesta al registro.
- Si la identidad de usuario pública registrada es parte de un registro implícito, el UE debe también obtener y retener el GRUU para cada identidad de usuario pública registrada (para más información véase la cláusula I.6.10.3).

Cuando se envían peticiones o respuestas SIP que requieran una dirección de contacto, el UE debería utilizar un GRUU en lugar del URI de contacto que registró.

- En particular, el UE debe utilizar el correspondiente GRUU retenido como dirección de contacto cuando se envían petición SIP con una cabecera "From" que contenga una identidad de usuario pública registrada.
- El UE también debe utilizar el correspondiente GRUU retenido como dirección de contacto cuando responda a peticiones SIP en las que la "P-Called-Party" sea una identidad de usuario pública implícitamente registrada.

I.6.10.2.2 S-CSCF

El S-CSCF debe poder responder a peticiones de registro que solicitan que se devuelvan URIs de GRUU. En este caso, necesita construir y devolver un GRUU que esté vinculado con el identificador de instancia y de identidad de usuario pública proporcionada.

Además de atender peticiones dirigidas a identidades de usuario públicas de las que sea responsable, un S-CSFCF debe también atender peticiones dirigidas a cualquier GRUU que hubiera sido previamente asignado a una identidad de usuario pública de la que sea responsable. Ese es el

caso cuando la responsabilidad de una identidad de usuario pública se transfiere desde un S-CSCF a otro.

Para satisfacer esta necesidad, el formato del GRUU para IPCablecom2 se define por convenio de la forma siguiente:

- El GRUU asociado con una identidad de usuario pública en formato SIP o SIPS es el mismo URI que la identidad de usuario pública con la adición del parámetro URI "gruu" y de un parámetro "opaque".
- Para un URI que incluya un número telefónico, puede solicitarse un GRUU utilizando un URI SIP que incluya un número de teléfono con el formato correcto en la parte de usuario del URI SIP, junto con el nombre del domino del proveedor y un parámetro "user=phone". Ciertamente, puede que no se solicite un GRUU para una identidad de usuario pública en el URI Tel porque puede que no se registre un URI tras del formato "tel". El GRUU resultante puede ser utilizado para los formularios SIP y TEL de la identidad de usuario pública.
- El parámetro "opaque" del GRUU que devuelve el S-CSCF consta de un nombre de parámetro "opaque=" seguido de un valor idéntico al valor del parámetro "sip.instance" que proporciona el UE en la petición REGISTER.

Cuando una petición se dirige a un GRUU, el perfil de usuario debe poder diferenciar qué servicios son aplicables a la petición en función de si el objetivo de la petición es un GRUU o una identidad de usuario pública. Esto puede conseguirse mediante un disparo de punto de servicio (SPT, *service point trigger*) que verifique si la petición ("Request") URI de la petición en curso incluye un parámetro URI "gruu".

Tal como se describe en la especificación de GRUU, cuando se hace una petición SIP a un URI con la propiedad GRUU, la lógica de encaminamiento viene determinada por la propiedad GRUU. Por lo tanto, la lógica del S-CSCF para la traducción de la petición URI de una petición de terminación es distinta para un GRUU que para una identidad de usuario pública. Para un GRUU, el único objetivo posible es un contacto registrado con la identidad de usuario pública y el identificador de instancia asociada al GRUU.

I.6.10.3 Especificación complementaria al IMS para IPCablecom2

Las especificaciones complementarias del IMS para IPCablecom2 Recs. UIT-T J.366.2, J.366.3, [UIT-T J.366.4] y [UIT-T J.366.5] incluyen los requisitos necesarios para el URI del agente de usuario globalmente encaminable (GRUU).

I.6.11 Ampliación del lote de eventos de estado de registro para GRUU

I.6.11.1 Descripción

Se definen extensiones adicionales para soportar el transporte de las URI GRUU en el lote de eventos de registro SIP. La extensión del lote de eventos de registro para GRUU debe soportarse si, a su vez, los elementos IPCablecom2 (UE, S-CSCF y HSS) soportan el GRUU. En cualquier otro caso, es opcional que la arquitectura de señalización SIP soporte la extensión del lote de eventos de registro de GRUU.

La extensión de lote de eventos de registro (Reg-event) para soportar GRUU es opcional en la arquitectura de señalización SIP de IPCablecom2. Mejora la información proporcionada por el lote de eventos de registro para incluir un GRUU si se asigna uno a un contacto registrado.

Esta funcionalidad está incluida en IPCablecom2 porque permite que un UE obtenga todos los GRUU asociados con un conjunto de registro implícito. Cuando un UE se registra y solicita la asignación de un GRUU, la respuesta incluirá el correspondiente GRUU para la identidad de usuario pública que se había registrado. Sin embargo, si la identidad de usuario pública forma parte de un conjunto de registro implícito, los registro del mismo contacto se hacen para cada una de las identidades de usuario públicas. Cada una resulta en la asignación de un GRUU diferente, pero no

existe forma de obtener dichos GRUU en la respuesta al REGISTER. Si el UE tiene una suscripción al lote de eventos de registro, la inclusión de la extensión del lote de eventos de registro para GRUU significa que el UE recibirá en una notificación los GRUU asociados con un conjunto de registro implícito.

I.6.11.2 Componentes afectados

En esta cláusula se describen los efectos sobre los componentes por el hecho de que el UE soporte opcionalmente la extensión GRUU de eventos de registro.

I.6.11.2.1 Equipo de usuario (UE)

Si un UE se ha suscrito a un lote de eventos de registro, y posteriormente recibe la notificación que indique que ha tenido lugar un registro implícito para un contacto que ha sido registrado por dicho UE, éste debe retener el GRUU de la notificación para una utilización futura. La forma en la que se utiliza se trata en la cláusula I.6.10.

I.6.11.2.2 S-CSCF

Cuando se envía una notificación correspondiente a un lote de eventos de registro, el S-CSCF debe utilizar el lote de eventos de registro para incluir el GRUU de cada contacto registrado al que se haya asignado un GRUU.

I.6.11.3 Especificación complementaria al IMS para IPCablecom2

La especificación complementaria al IMS para IPCablecom2 [UIT-T J.366.4] incluye los requisitos necesarios para la extensión del lote de eventos de estado de registro para GRUU.

I.6.12 Cabeceras privadas del 3GPP

En [IETF RFC 3455] se describe un conjunto de cabeceras SIP privadas para ser utilizadas en las especificaciones del 3GPP. De ellos, hay dos cabeceras-p (privadas) cuyos requisitos IPCablecom2 son distintos de los correspondientes en el IMS.

NOTA – Las cabeceras privadas descritas en [IETF RFC 3455] que no se identifican en esta cláusula se soportan en IPCablecom2 sin cambio alguno.

I.6.12.1 Descripción

I.6.12.1.1 Cabecera P-Associated-URI

El UE recibe la cabecera "P-Associated-URI" en la respuesta 200 (OK) a una petición REGISTER (registro). De conformidad con [UIT-T J.366.4], incluye la identidad de usuario pública y su conjunto asociado de identidades de usuario públicas registradas implícitas.

NOTA – Ello difiere de la descripción hecha en [IETF RFC 3455].

De conformidad con los procedimientos de registro del IMS, se requiere que el UE soporte esta cabecera, que indica al UE lo siguiente:

- el conjunto de identidades de usuario públicas implícitamente registradas;
- la identidad de usuario pública por defecto, que será confirmada por el P-CSCF en los procedimientos "P-Asserted-Identity" si el UE no incluye una cabecera "P-Preferred-Identity", o no incluye una identidad de usuario pública registrada en la cabecera "P-Preferred-Identity";
- si se prohíbe o no la identidad de usuario pública para registro, pues las identidades prohibidas no están incluidas en la cabecera "P-Associated-URI".

En IPCablecom2, es opcional que el UE soporte la cabecera "P-Associated-URI".

I.6.12.1.2 Cabecera P-Access-Network-Info

De conformidad con el IMS, el UE debe incluir la cabecera "P-Access-Network-Info" en cualquier mensaje SIP (con algunas excepciones) que se envíe con protección de integridad. Identifica la tecnología de acceso utilizada para la conectividad IP (por ejemplo, IP-CAN), y lo transfiere el S-CSCF a los servidores de aplicaciones confiables formado parte del registro de un tercero.

Sus usos potenciales incluyen:

- servicios de emergencia, tal como se describe en la cláusula 5.2.10 de [UIT-T J.366.4];
- determinación de si es necesaria la compresión SIP entre el UE y el P-CSCF, tal como se describe en la cláusula I.6.3;
- optimización del valor de los temporizadores SIP, tal como se describe en la cláusula I.6.14; y
- optimización de los servicios en función del tipo de red de acceso.

En IPCablecom2, el UE incluye la cabecera "P-Access-Network-Info" sólo si se conoce la tecnología de acceso.

NOTA – Los nuevos valores de tipo de acceso para IPCablecom2 debe registrarse en la organización de normalización apropiada.

I.6.12.2 Componentes afectados

En esta cláusula se describen los efectos sobre los componentes por el hecho de soportar opcionalmente las cabeceras "P-Associated-URI" y "P-Access-Network-Info".

I.6.12.2.1 Equipo de usuario (UE)

Si el UE no soporta la cabecera "P-Associated-URI", no tiene forma de conocer si la identidad que ha utilizado en el registro está prohibida. Por lo tanto, debe tenerse cuidado para que los UE que no soporten la cabecera "P-Associated-URI" no se registren utilizando una identidad prohibida. Las identidades prohibidas no están vinculadas a la información de contacto y no pueden utilizarse para confirmar la identidad. Las implicaciones básicas por no soportar la cabecera "P-Associated-URI" son las siguientes:

- El UE no recibe indicación explícita de que se hayan registrado implícitamente AOR adicionales salvo que soporte el lote de eventos de estado de registro (véase la cláusula I.6.8).
- Si la identidad de usuario pública utilizada para el registro está prohibida, el UE no podrá suscribirse con éxito al lote de eventos de estado de registro, si no existe asociación de seguridad.
- Si se emite una petición con una "P-Preferred-Identity"que contenga una identidad de usuario pública prohibida, el P-CSCF la ignorará e insertará en su lugar una "P-Asserted-Identity" con una identidad de usuario pública por defecto conocida.

El UE soportará los procedimientos de la cabecera "P-Access-Network-Info" descritos en [UIT-T J.366.4], con las aclaraciones siguientes:

- El UE inserta la cabecera "P-Access-Network-Info" sólo si se conoce la tecnología de la red de acceso.

I.6.12.2.2 P-CSCF

Si el P-CSCF recibe una petición REGISTER que no contenga una cabecera "P-Access-Network-Info" y conoce la tecnología de acceso que se utiliza en el UE, el P-CSCF insertará la cabecera "P-Access-Network-Info".

NOTA – Dado que puede que ni el UE ni el P-CSCF inserten la cabecera "P-Access-Network-Info" (es decir, cuando ninguno de ellos conoce la tecnología de la red de acceso), las funcionalidades y servicios que utilizan la "P-Access-Network-Info" deben gestionar adecuadamente su ausencia.

I.6.12.2.3 S-CSCF

Si el UE no soporta la cabecera "P-Associated-URI" y la seguridad de señalización está deshabilitada o es opcional, el S-CSCF de origen puede recibir peticiones que no sean REGISTER y que incluyan una identidad de usuario pública prohibida en la cabecera "P-Preferred-Identity" y/o en la cabecera "From". En este caso, el S-CSCF rechazará la petición generando una respuesta 403 (Forbidden).

I.6.13 Encaminamiento de peticiones SUBSCRIBE para información de configuración

I.6.13.1 Descripción

Los UE de IPCablecom2 obtienen información de configuración utilizando el protocolo SIP mediante la suscripción al lote de eventos ua-profile. La suscripción inicial para la configuración se dirige a un URI de petición (Request-URI) especial específico para cada tipo de dispositivo. El UE construye el Request-URI a partir de un identificador de dispositivo especifico del UE, combinado con el nombre de domino del proveedor. La petición de suscripción inicial para la configuración debe ser encaminada a un elemento PAC de IPCablecom2 capaz de proporcionar un perfil de dispositivo adecuado para el UE.

Es importante diferenciar entre dos clases de UE para las que las peticiones SUBSCRIBE para configuración deben ser procesadas:

1) Los UE cuyos URI de dispositivo conoce el sistema.

2) Los UE cuyos URI de dispositivo desconoce el sistema.

Los procedimientos que se describen a continuación permiten que las peticiones SUBSCRIBE para información de configuración se encaminadas adecuadamente en cualquiera de los dos casos.

Un UE puede o no ser consciente de si la red conoce o no su URI de dispositivo. Si es desconocido, no podrá registrarse. El procedimiento que utiliza funcionará en cualquiera de ambos casos. Envía una petición de suscripción para su perfil antes de registrarse. Esta petición se dirige al URI específico del dispositivo. Incluye una cabecera "From" que contiene el URI específico del dispositivo, y debe incluir una cabecera "P-Preferred-Identity" que también contiene el URI específico del dispositivo. Ello responde a los procedimientos descritos en la cláusula I.6.1.2.1 que se aplican cuando no hay asociación de seguridad entre el UE y el P-CSCF y el UE no se ha registrado.

Debido a que el UE no se ha registrado, el P-CSCF no tiene base para autenticar la petición. En lugar de ello, deja la cabecera "P-Preferred-Identity" en su lugar, y aplaza la autenticación a un servidor subsiguiente. Para seleccionar un I-CSCF para un ulterior procesamiento y al que remitir la petición, utiliza la cabecera "P-Preferred-Identity" si existe y si no existe, la cabecera "From".

En ausencia de una cabecera "P-Asserted-Identity", el I-CSCF utiliza "P-Preferred-Identity" si existe, o la cabecera "From" si aquella no existe, a fin de establecer el destino al que encaminar la petición para el procesamiento de origen.

Si se conoce el URI del dispositivo, habrá una entrada explícita para el mismo en el HSS, como una identidad de usuario pública. El I-CSCF encamina la petición al S-CSCF que atiende a dicha identidad de usuario pública.

El URI del dispositivo en el caso de un dispositivo desconocido es, por definición, desconocido para el HSS, de forma que no existe en el HSS una entrada exactamente concordante. No obstante, cuando sea deseable que se soporten dispositivos desconocidos, existirá en el HSS una entrada de identidad de servicio pública (PSI) que sea válida en todos los casos y que concuerde con todos los

URI de dispositivos desconocidos deseados. Por ejemplo, los dos valores siguientes pueden ser suficientes:

sip:MAC%3a!.*!@provider.net

sip:urn%3auuid%3a!.*!@provider.net

La entrada del HSS debería identificar un elemento PAC que maneje suscripciones desconocidas de dispositivos desconocidos. El I-CSCF encamina las suscripciones realizadas por dispositivos desconocidos a este servidor para el procesamiento de origen ("orig").

El elemento PAC es responsable de cualquier autenticación o autorización que elija para dispositivos desconocidos. El servidor opta entonces entre respetar la petición o rechazarla. Dado que se invocó para realizar el procesamiento de origen, puede ser necesario encaminar la petición a otro destino para el procesamiento de terminación. No obstante, en el caso de IPCablecom2 el único caso aplicable es aquél en el que la dirección de origen y de terminación son la misma. Por lo tanto, el servidor puede simplemente respetar la petición sin un ulterior encaminamiento. Utiliza información de la petición de suscripción (por ejemplo, información del tipo de dispositivo) para seleccionar una configuración por defecto adecuada para el dispositivo (una que permita al dispositivo utilizar cualquier capacidad restringida que el proveedor pueda permitir opcionalmente). Típicamente este objetivo una comunicación inicial suficiente destinada a establecer una relación de negocio entre el proveedor y el usuario del dispositivo, después de la cual el dispositivo cambiará su estado, pasando a ser *conocido* para el sistema. Para más información, véase [UIT-T J.364].

I.6.13.2 Componentes afectados

En esta cláusula se describen los efectos sobre los componentes por el hecho de soportar la suscripción al lote de eventos de perfil de UA antes del registro.

I.6.13.2.1 Equipo de usuario (UE)

Un UE debería subscribirse para el perfil del dispositivo, utilizando el URI específico del dispositivo sin registrarse previamente empleando dicho URI. Lo hará de acuerdo con los procedimientos de la cláusula I.6.1.2.1 sobre seguridad de señalización y el UE.

I.6.13.2.2 P-CSCF

Véase la cláusula I.6.1.2.2 sobre seguridad de señalización y el P-CSCF.

I.6.13.2.3 I-CSCF

Véase la cláusula I.6.1.2.3 sobre seguridad de señalización y el I-CSCF.

I.6.13.2.4 S-CSCF

Véase la cláusula I.6.1.2.4 sobre seguridad de señalización y el S-CSCF.

I.6.13.2.5 HSS

El HSS debe poder tratar el caso en el que un URI – petición (URI-Request) concuerde con dos entradas en el HSS, una para una identidad de servicio pública (PSI) válida para cualquier caso y otra para una identidad de usuario pública. En este caso, la entrada para la identidad de usuario pública tendrá precedencia sobre la de la PSI válida para cualquier caso.

I.6.13.2.6 Elemento de PAC

El elemento de provisión, activación y configuración (PAC) para un URI de dispositivo conocido funcionará como un servidor de aplicación de terminación en nombre del correspondiente usuario. Puede detectar que el dispositivo es conocido gracias a la presencia de una cabecera "P-Asserted-Identity" que contiene el URI del dispositivo.

El elemento PAC para un URI de dispositivo desconocido funcionará como un servidor de PSI de origen. Puede detectar que el dispositivo es desconocido por la ausencia de una cabecera "P-Asserted-Identity".

I.6.13.3 Especificación complementaria al IMS para IPCablecom2

La especificación complementaria al IMS para IPCablecom2 [UIT-T J.366.4] incluye los requisitos necesarios para encaminar SUBSCRIBE de para información de configuración.

I.6.14 Temporizadores SIP

I.6.14.1 Descripción

Para acomodar el procesamiento de la interfaz aire de 3GPP y los retardos de transmisión, la versión 6 del IMS del 3GPP [UIT-T J.366.4] especifica un conjunto modificado de valores de temporizadores SIP (comparados con los definidos en [IETF RFC 3261]) que se aplican desde el P-CSCF al UE, y viceversa. Ello no es aplicable al acceso de banda ancha, en el que se utilizan valores normalizados de temporizadores SIP [IETF RFC 3261]. Dentro del soporte a la "banda ancha fija" que ofrece la versión 7 del IMS del 3GPP, los UE que utilicen tecnología de acceso de banda ancha y el P-CSCF que interaccione con dichos UE utilizan valores normalizados de temporizadores SIP [IETF RFC 3261].

IPCablecom2 incorpora estos cambios de la versión 7 del IMS del 3GPP para los temporizadores SIP.

Esta solución es función de la especificación de un nuevo tipo de acceso para la cabecera "P-Access-Network-Info", que represente la tecnología de la red de acceso de banda ancha de IPCablecom2. Para más información véase la cláusula I.6.12.1.2.

Puesto que el UE y el P-CSCF necesitan utilizar un conjunto consistente de valores de temporizadores SIP, si el UE no proporciona una cabecera "P-Access-Network-Info", tanto UE como P-CSCF, utilizarán los valores normalizados de temporizadores SIP [IETF RFC 3261]. Obsérvese que esto supone un requisito incremental con respecto a los cambios de la versión 7 del IMS del 3GPP.

Obsérvese que la solución de la versión 7 del IMS del 3GPP puede ser objeto de estudios ulteriores en el seno del 3GPP para determinar si existen otras formas más convenientes de establecer los retardos de acceso y si los valores de los temporizadores SIP deberían ser modificados. IPCablecom2 podría realinearse con cualquier cambio que ulteriormente pudiera hacerse en esta área.

I.6.14.2 Componentes afectados

Los cambios requeridos se identifican e incorporan en la versión 7.

Un requisito adicional es que dado que el UE y el P-CSCF han de utilizar un conjunto consistente de valores de temporizadores SIP, si el UE no proporciona una cabecera "P-Access-Network-Info", tanto UE como P-CSCF utilizarán los valores normalizados de temporizadores SIP [IETF RFC 3261].

I.6.14.2.1 Equipo de usuario (UE)

Sólo los UE con tecnología de acceso inalámbrica 3GPP utilizan los valores de temporizadores SIP 3GPP modificados. Los restantes UE utilizan valores de temporizadores SIP normalizados [IETF RFC 3261].

I.6.14.2.2 P-CSCF

El P-CSCF aplica valores de temporizadores SIP 3GPP modificados hacia los UE con tecnologías de acceso inalámbricas. Para los UE utilizados con otras tecnologías de acceso, el P-CSCF aplica

valores de temporizadores SIP normalizados [IETF RFC 3261]. El P-CSCF toma la determinación en función del tipo de acceso que se identifica en "P-Access-Network-Info". Cuando un UE no proporciona "P-Access-Network-Info", se aplican valores de temporizadores normalizados [IETF RFC 3261].

I.6.14.3 Especificación complementaria al IMS para IPCablecom2

En la especificación complementaria al IMS para IPCablecom2, cláusula 7.7 de [UIT-T J.366.4], se incluyen los requisitos necesarios para temporizadores SIP.

I.6.15 Cambios generales

I.6.15.1 Descripción

En esta cláusula ase describen un conjunto de cambios diversos del IMS destinados a satisfacer los requerimientos específicos de IPCablecom2, incluyendo clarificaciones terminológicas y el soporte de los direccionamientos basados en IPv4 y IPv6.

- [UIT-T J.366.4] utiliza terminología que implica en algunos casos una tecnología de acceso específica. Los términos "originación móvil", "originado en móvil", "terminación móvil", "terminado en móvil" e "iniciado en móvil" se utilizan a en TS 24.229. Como parte del soporte de la "banda ancha fija" que se hace en la versión 7 del IMS del 3GPP, [UIT-T J.366.4] se ha modificado para corregir la terminología utilizando términos como "originación UE", "originado en UE", "terminación UE", "terminado en UE" e "iniciado en UE". IPCablecom2 asume implícitamente este cambio de terminología.
- [UIT-T J.366.4] especifica procedimientos para la obtención de identidad pública, identidad privada y nombre de domino de red del hogar cuando el UE contiene una UICC (tarjeta de circuito integrado UMTS) pero no ISIM (módulo de identidad de servicios IM). (Véanse las cláusulas 4.2 y 5.1.1.1A y el anexo C a [UIT-T J.366.4].) Algunos UE utilizados en IPCablecom2 puede que no tengan ni UICC ni ISIM. En tales casos, el UE se configurará o se aprovisionará con la información requerida. Para más información sobre este caso, véase el apéndice III.

Debería reconocerse lo siguiente:

- Algunos procedimientos de [UIT-T J.366.4] se describen explícitamente como relativos al acceso 3GPP. Dichos procedimientos no son aplicables a clientes de banda ancha (por ejemplo: la cláusula 5.2.8.1 de [UIT-T J.366.4] "Liberación de la llamada iniciada por el P-CSCF " incluye escenarios relativos a la "cobertura radioeléctrica " y a los "recursos de la interfaz radioeléctrica ".
- [UIT-T J.366.4] también incluye anexos que están explícitamente dirigidos al acceso GPRS. Dichos anexos evidencian en sí mismos que no son aplicables al acceso de banda ancha IPCablecom2, y pudiendo el material correspondiente a IPCablecom2 estar incluido en otras especificaciones de IPCablecom2.

I.6.15.2 Componentes afectados

Se han identificados cambios requeridos para la generalización de la terminología de acceso (de "-móvil" a "UE"). Estos cambios generalizan [UIT-T J.366.4] pero no afectan a los procedimientos. En esta cláusula no se hace un desglose detallado del impacto sobre los componentes.

I.6.15.3 Especificación complementaria al IMS para IPCablecom2

Los cambios requeridos para la generalización de la terminología de acceso (de "-móvil" a "UE") están implícitamente asumidos y, por simplicidad, [UIT-T J.366.4] no está actualizada con estos cambios.

I.6.16 Interfuncionamiento con versiones previas de IPCablecom

Un UE debe ser capaz de establecer sesiones de voz con puntos extremos soportados en versiones previas de IPCablecom. Por ejemplo, los UE y los E-MTA en una misma red de operador deben poder llamarse mutuamente sin encaminar las llamadas a través de otro operador IP o a través de la RTPC: Asimismo, un UE debe poder establecer llamadas con puntos extremos MG basados en TGCP a fin de interfuncionar con la RTPC:

El control de servicio para los UE no está integrado en forma alguna con el control del servicio para los E-MTA. El control del servicio del UE está compartido entre el UE y su servidor S-CSCF y los servidores de aplicación asociados. El CMS proporciona y controla los servicios del E-MTA a través del NCS. Los UE y los E-MTA se ven uno a otro simplemente como entidades de red diferenciadas susceptibles de ser llamadas.

La capacidad de establecer llamadas entre los UE y otros puntos extremos soportados en versiones previas de IPCablecom es posible gracias a la interfaz SIP-based pkt-sig-2 que conecta el S-CSCF, I-CSCF y BGCF con el CMS y MGC (véase la figura I.3). Los requisitos para soportar esta interfaz sobre el CMS y el MGC se definen en [UIT-T J.178].

Apéndice II

Visión general técnica de la arquitectura de calidad de servicio

(Este apéndice no es parte integrante de esta Recomendación)

II.1 Introducción

En este apéndice se proporciona una visión general de la arquitectura de calidad de servicio (QoS) de IPCablecom2. Específicamente, se describe cómo que se utiliza el sistema multimedia IPCablecom2 para proporcionar aplicaciones de QoS que se construyen sobre IPCablecom2. Para ayudar al lector a entender cabalmente la arquitectura de QoS de IPCablecom2, en este apéndice se analizan los objetivos de alto nivel y los componentes lógicos e interfaces específicas definidas.

II.1.1 Visión general del sistema multimedia IPCablecom

El sistema multimedia IPCablecom define una plataforma basada en IP para ofrecer servicios multimedia sobre una red de acceso DOCSIS 1.1 (Rec. UIT-T J.112) o superior (para el resto de este documento las referencias a DOCSIS asumen DOCSIS 1.1 o superior). Esta plataforma amplía las capacidades principales de IPCablecom (por ejemplo, autorización de QoS y control de admisión, mensajes de eventos para facturación y otras funciones de apoyo y seguridad) para soportar una amplia gama de servicios IP adicionales a la telefonía. Es decir, mientras que la arquitectura IPCablecom está adaptada específicamente a los servicios telefónicos residenciales, la arquitectura multimedia IPCablecom ofrece una plataforma de propósito general para que los operadores de cable puedan distribuir una serie de servicios multimedia IPCablecom que requieran tratamiento específico de calidad de servicio. Por este motivo, no se definen ni se analizan servicios concretos.

Aunque la plataforma multimedia IPCablecom se basa en el trabajo de IPCablecom, para desplegar servicios multimedia no es un requisito previo utilizar toda la infraestructura de voz definida en IPCablecom. En lugar de ello, el objetivo es que un operador de cable pueda elegir entre desplegar inicialmente servicios de voz o servicios multimedia, con la garantía de que estas plataformas se integrarán e interoperarán sin fisuras siempre que sean desplegadas en paralelo.

II.2 Referencias

En este apéndice se utilizan las referencias informativas siguientes:

[UIT-T J.163] Recomendación UIT-T J.163 (2005), *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.179 Ap.I] Recomendación UIT-T J.179 (2005), *Soporte de IPCablecom para multimedia.* Apéndice I: *Información general*.

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

[UIT-T J.362] Recomendación UIT-T J.362 (2006), *Detección de punto de control IPCablecom2*.

[UIT-T J.365] Recomendación UIT-T J.365 (2006), *Interfaz de gestor de aplicación IPCablecom2*.

[UIT-T J.366.4] Recomendación UIT-T J.366.4 (2006), *Subsistema multimedia IP (IMS) IPCablecom2: Protocolo de inicio de sesión (SIP) y protocolo de descripción de sesión (SDP) – Especificación nivel 3* (3GPP TS 24.229).

[IETF RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.

[IETF RFC 3890] IETF RFC 3890 (2004), *A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)*.

II.3 Términos y definiciones

En este apéndice se utilizan los términos adicionales siguientes:

II.3.1 versión 6 del IMS: Conjunto de especificaciones aprobadas que constituyen la versión 6 del subsistema multimedia IP del 3GPP

II.4 Abreviaturas, siglas o acrónimos

En este apéndice se utilizan las siguientes abreviaturas, siglas o acrónimos.

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

DSCP Punto de código de servicios diferenciados (*differentiated services code point*)

P-CSCF Función CSCF proxy (*proxy CSCF*)

WS Servicios Web (*web services*)

II.5 Requisitos y alcance de la calidad de servicio

El objetivo de este apéndice es proporcionar una definición de la arquitectura necesaria para que un dispositivo UE obtenga acceso a recursos de red IPCablecom. En particular, describe un mecanismo completo para que una red IPCablecom solicite los recursos de QoS específicos requeridos para soportar los medios asociados a sesiones SIP sobre una red DOCSIS.

Esta arquitectura también reconoce que IPCablecom proporcionará QoS para una amplia variedad de aplicaciones y servicios (voz, video, etc.); en este sentido, proporciona un mecanismo genérico para solicitar recursos de la red de acceso y no requiere que las aplicaciones conozcan la topología de la red de acceso.

II.5.1 Requisitos

Se incluyen a continuación un conjunto de requisitos que se consideran esenciales para desarrollar una arquitectura de QoS de propósito general que satisfaga los servicios previstos para IPCablecom2:

- La arquitectura de QoS debe permitir la creación de flujos de servicio para UE que no sean conscientes de los criterios de QoS a través de una política impulsada desde la red.
- Definir de un gestor de aplicación IPCablecom2 (IPAM, *IPCablecom2 application manager*) que medie en la interacción relativa a la QoS entre el P-CSCF y la infraestructura multimedia.
- Soportar el marcado y clasificación de paquetes desde la red de acceso de forma que pueda utilizarse un mecanismo de QoS (por ejemplo servicios diferenciados, *DiffServ*) en la red troncal.
- El IPAM debe recibir información suficiente del P-CSCF sobre cada flujo que forme parte de la sesión, de forma que pueda:
  - Construir un clasificador adecuado al tiempo que permita mecanismos de tránsito del NAT.
  - Construir una especificación de flujo o un perfil de tráfico alternativo que refleje el límite superior más reducido de los requisitos relativos a los recursos de cualquier códec alternativo que esté permitido para el flujo, incluyendo anchura de banda, velocidad de paquetización y tipo de programación.

  - Determinar el tipo de medios para poder seleccionar un punto de código de servicios diferenciados adecuado (DSCP, *differentiated services code point*).
- El IPAM debe recibir información suficiente de la P-CSCF para cada sesión de forma que pueda:
  - Construir un identificador de correlación adecuado para los registros de contabilidad.
  - Identificar el abonado para poder acceder a los datos del perfil del mismo.
  - Reconocer si la sesión debe tener una prioridad más elevada (por ejemplo, una llamada de emergencia).
- La interfaz debe permitir que la reserva y el compromiso de recursos se realicen en etapas diferenciadas.

II.5.2 Alcance

El alcance actual de la arquitectura de QoS de IPCablecom está limitada exclusivamente a la parte de acceso basada en DOCSIS de la red de un operador de cable y a la forma en la que la red IPCablecom puede solicitar recursos de QoS al marco multimedia IPCablecom. Por lo tanto, la arquitectura descrita en este apéndice no considera el caso de un UE en itinerancia que pueda agregarse a una red IPCablecom desde redes de acceso no basadas en DOCSIS.

Además, esta arquitectura no prohíbe la utilización de las capacidades de QoS en redes habilitadas para IPCable2Home. No obstante, la provisión de QoS en una red IPCable2Home no está dentro del alcance de este apéndice.

II.6 Marco de la arquitectura para calidad de servicio

En el contexto global de aprovechar al máximo posible las normas existentes en la industria, un objetivo específico es la alineación con la arquitectura y especificaciones del IMS desarrolladas por el 3GPP. Específicamente, IPCablecom2 se alinea con la versión 6 del IMS y reutiliza muchos de los componentes y puntos de referencia básicos del IMS. Otro objetivo igualmente importante es utilizar el conjunto de capacidades de QoS que proporciona el sistema multimedia IPCablecom.

IPCablecom2 debe soportar un modelo de impulso (*push*) de la política relativa a la interfaz con el sistema multimedia IPCablecom. La versión 6 del IMS proporciona dos mecanismos conexos para la provisión de la calidad de servicio y la tarificación de los flujos de servicio IP que configuran las sesiones multimedia. La política local basada en el servicio (SBLP, *service-based local policy*) proporciona un mecanismo para la autorización, establecimiento y modificación de portadores IP utilizando un testigo de autorización similar al de la arquitectura de calidad de servicio dinámica [UIT-T J.163] de IPCablecom. Tal como ocurre en el caso de DQoS, el establecimiento de contextos PDP utilizando SBLP requiere la participación activa de un equipo de usuario con capacidad para diferenciar la QoS.

El segundo mecanismo es la tarificación basada en flujos (FBC, *flow-based charging*). La FBC proporciona la forma de identificar, controlar y tarificar por los flujos IP que configuran una sesión utilizando un mecanismo de propuesta iniciado por la red similar al sistema multimedia IPCablecom. Sin embargo, la FBC no proporciona un mecanismo para el establecimiento de nuevos portadores (o flujos de servicio). Ni la SBLP ni la FBC tal como se definen en la versión 6 del IMS proporcionan la información completa necesaria para soportar el establecimiento de nuevos flujos de servicio utilizando el sistema multimedia IPCablecom. Es posible que se lleve a cabo una alineación futura con los trabajos relativos al control de la política y la tarificación que se están realizando para la versión 7 del IMS.

II.6.1 Modelo de referencia de la arquitectura para QoS

En la figura II.1 se ilustra la arquitectura para QoS de IPCablecom2. La infraestructura de QoS definida en la versión 6 del IMS no es suficientemente agnóstica respecto al acceso como para satisfacer los requisitos de IPCablecom2. Por lo tanto, IPCablecom2 utiliza los componentes del sistema multimedia IPCablecom incluyendo el servidor de política, el CMTS y el módem de cable. El gestor de aplicación de IPCablecom2 es un gestor de aplicación especializado que recibe peticiones de QoS a nivel de sesión a través de SOAP desde el P-CSCF y crea y gestiona las puertas multimedia IPCablecom para cada flujo de la sesión utilizando la interfaz pkt-mm-3 del sistema multimedia IPCablecom.

La arquitectura de QoS no prohíbe la utilización del punto de referencia Gq definido en el IMS para aquellos UE que puedan acceder a servicios a través de una red GPRS. En la figura II.1 se ilustra la coexistencia de la arquitectura de QoS definida en el IMS para dispositivos basados en GPRS con la arquitectura de QoS del sistema multimedia IPCablecom2 utilizada en los UE que acceden a los servicios a través de una red DOCSIS:

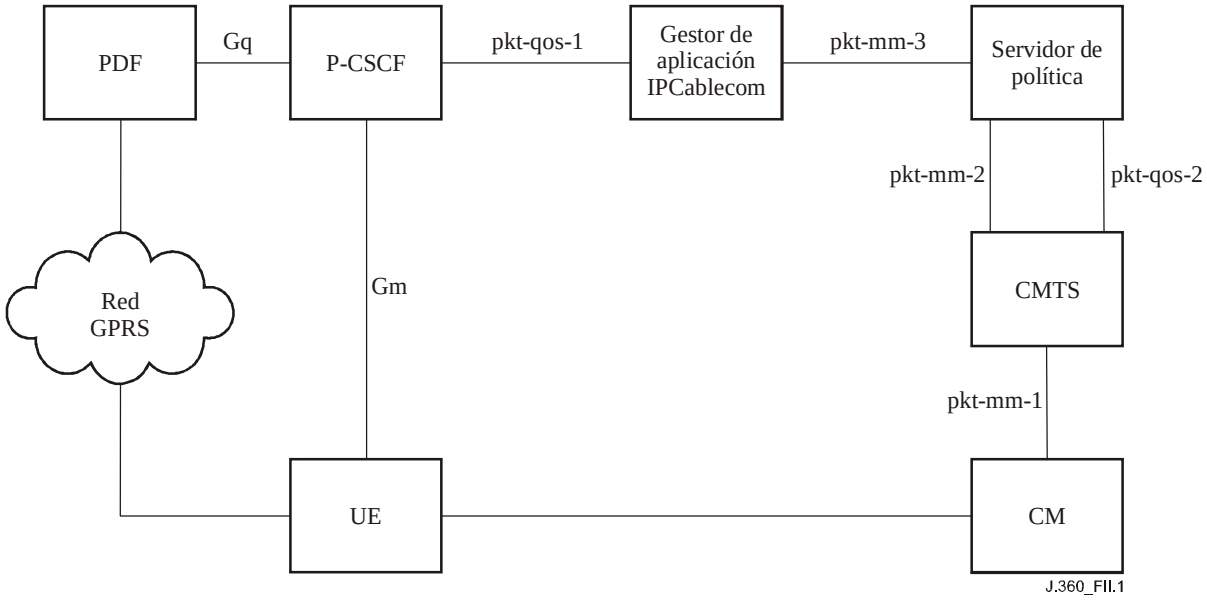


Figura II.1 – Puntos de referencia de señalización para QoS

El sistema multimedia IPCablecom define los puntos de referencia de pkt-mm-1 al pkt-mm-3. IPCablecom2 introduce los nuevos puntos de referencia de QoS pkt-qos-1 y pkt-qos-2. En el cuadro II.1 se describen brevemente estas interfaces y en el cuadro II.2 se hace una breve descripción de cada elemento de red.

Cuadro II.1 – Puntos de referencia de QoS

Punto de referencia	Elementos de red IPCablecom	Descripción del punto de referencia
pkt-mm-1	CMTS – CM	El CMTS utiliza señalización DSX definida para DOCSIS para ordenar al CM el establecimiento, desconexión o cambio del flujo de servicio DOCSIS a fin de satisfacer una petición de QoS.
pkt-mm-2	Servidor de política – CMTS	Interfaz que soporta las peticiones de QoS del intermediario (*proxy*) en nombre de un UE. Esta interfaz es fundamental para la gestión de la política. Controla las decisiones sobre la política que el servidor de política (PS, *policy server*) hace llegar al CMTS y se define en [UIT-T J.179]. En algunos casos, esta interfaz también se utiliza para informar al PS del momento en que quedan inactivos recursos de QoS.
pkt-mm-3	IPAM-PS	Interfaz que permite al gestor de aplicación de IPCablecom (IPAM, *IPCablecom application manager*), un gestor de aplicación especializado definido en IPCablecom, para solicitar al PS que implemente una decisión sobre política en el CMTS en nombre del UE y que se define en [UIT-T J.179]. Esta interfaz también puede utilizarse para informar al IPAM de cambios en el estado de los recursos de QoS.
Gm	UE – P-CSCF	Permite que el UE se comunique con el P-CSCF con fines de registro y control de sesión. Este punto de referencia está basado en SIP y se describe en [UIT-T J.366.4].
Mw	CSCF – CSCF	Permite la comunicación y reenvío de mensajes de señalización entre los CSCF para el registro y el control de sesión. Este punto de referencia se basa en SIP.
Gq	P-CSCF – PDF	La interfaz Gq se utiliza para el intercambio de información de establecimiento de política de sesión entre la función de decisión de política (PDF, *policy decision function*) y el P-CSCF.
pkt-qos-1	P-CSCF – IPAM	Esta interfaz basada en SOAP/XML entre el P-CSCF y el gestor de aplicación de IPCablecom transporta información de QoS a nivel de sesión. El IPAM utiliza esta información para constituir mensajes adecuados para la interfaz pkt-mm-3 y lo define [UIT-T J.365].
pkt-qos-2	Servidor de política – CMTS	El servidor de política utiliza el protocolo de descubrimiento del punto de control para determinar el CMTS servidor en la red para un UE dado. Este punto de referencia se basa en la especificación de IPCablecom [UIT-T J.362].

Cuadro II.2 – Elementos de red de QoS

Elemento de red IPCablecom	Breve descripción
UE	Un UE es un cliente e interactúa con la red para acceder a servicios y proporciona interfaces a usuarios o entidades.
P-CSCF	El P-CSCF analiza el SDP de los mensajes SIP e implementa la interfaz del cliente de servicios web para proporcionar QoS mediante la interacción con el gestor de aplicación. Reserva, compromete y suprime los criterios de QoS en la red de acceso.
Gestor de aplicaciones IPCablecom (IPAM)	El gestor de aplicación de IPCablecom es responsable de gestionar recursos de QoS en la red de acceso que solicita el P-CSCF. El gestor de aplicación de IPCablecom recibe mensajes de QoS a nivel de sesión desde el P-CSCF y formula y envía mensajes de QoS de IPCablecom multimedia al servidor de política.
Servidor de política (PS)	El servidor de política actúa como un intermediario entre el gestor o gestores de aplicación y el o los CMTS. Aplica políticas de red a los mensajes del gestor de aplicación y actúa como intermediario de los mismos ante el CMTS.
Sistema de terminación de módem de cable (CMTS)	El CMTS es un dispositivo en la cabecera de la red de cable que implementa el protocolo MAC RFI DOCSIS y se conecta con los CM a través de la red HFC.
Módem de cable (CM)	Módem de cable conforme con DOCSIS.

II.6.2 Relación con la versión 6 del IMS del 3GPP

Las Recomendaciones relativas a IPCablecom2 incluyen una versión mejorada de la versión 6 del IMS del 3GPP (TS 24.229) a fin de documentar los requisitos de QoS para el protocolo de control de llamada utilizando SIP y SDP. A continuación se resumen las modificaciones hechas a TS 24.229:

- Requisitos adicionales para incluir el descriptor de medios "b=" y el modificador de anchura de banda "TIAS" definido en [IETF RFC 3890] para describir la anchura de banda que requiere la sesión.
- Se añaden tipos de SDP adicionales a la definición del perfil de SDP para agentes de usuario. Los tipos de SDP incluyen:
  - Tiempo de paquete (a=ptime) – Este tipo debe ser incluido por el UEs para indicar el tiempo de paquetización que el UE espera para recibir tráfico.
  - Velocidad máxima de paquetes (a=maxprate) – Este tipo debe ser incluido cuando el UE utiliza un códec IPCablecom que no sea bien conocido.
  - AT (a=Local-Turn) – Este tipo debe ser incluido cuando por el UE cuando utiliza un servidor TURN para transitar un dispositivo NAT local.

II.6.3 Relación con el punto de referencia multimedia pkt-mm-11

La arquitectura multimedia de IPCablecom define también una interfaz basada en servicios web con el gestor de aplicación desde un servidor de aplicación situado aguas arriba en la red. Esta interfaz se etiqueta pkt-mm-11 en el informe técnico multimedia [UIT-T J.179 Ap.I]. Aunque dicha interfaz pueda ser utilizada por el P-CSCF como interfaz con el gestor de aplicación de IPCablecom2, se ha desarrollado una nueva interfaz para lograr un funcionamiento más eficiente del P-CSCF. La interfaz multimedia definida requeriría una doble traducción de los parámetros de sesión, generando una tara adicional para el P-CSCF para traducir los parámetros de sesión en una petición de QoS genérica. La interfaz definida por IPCablecom permite que el P-CSCF transfiera al gestor de aplicación de IPCablecom el conjunto de parámetros de sesión, que es responsable de la traducción

en un mensaje válido de QoS multimedia de IPCablecom. Ello reduce la cantidad de traducciones requeridas y permite que el P-CSCF se implemente de forma más agnóstica respecto a la red de acceso.

II.7 Descripción de la arquitectura

En la cláusula II.6 se describe un conjunto de entidades de red lógicas agrupadas según funciones de servicio específicas (QoS), así como un conjunto de puntos de referencia que soportan los flujos de información intercambiados entre grupos funcionales y entidades de red. En esta cláusula se presenta un análisis más detallado de los elementos lógicos y puntos de referencia asociados nuevos en la arquitectura de IPCablecom. También ofrece una visión general de otros asuntos relativos a la arquitectura de QoS no documentados en otro documento.

II.7.1 Componentes funcionales

En esta cláusula se facilita información adicional sobre el gestor de aplicación de IPCablecom2 y el P-CSCF y sus papeles en relación con la arquitectura de QoS.

II.7.1.1 P-CSCF

Además de su papel de proveedor de la conectividad del UE con la red IPCablecom, el P-CSCF también es responsable de reservar, comprometer y liberar recursos de QoS para una sesión dada. Es importante señalar que el P-CSCF no determina realmente los recursos de QoS necesarios para la sesión, más bien simplemente actúa como intermediario entre la información de descripción de sesión y el gestor de aplicaciones de IPCablecom2 e indica si se reservan o se comprometen los recursos para la sesión. Aunque la arquitectura permite que un operación de compromiso en dos fases (reserva seguida de compromiso), no se requiere que el P-CSCF adopte este enfoque. Puede utilizarse un compromiso en una sola fase (reservar y comprometer los recursos en una única petición).

Una vez que termina la sesión, el P-CSCF libera los recursos atribuidos a la misma.

II.7.1.2 Gestor de aplicación de IPCablecom2 (IPAM)

El gestor de aplicación de IPCablecom2 (IPAM, IPCablecom2 *application manager*) es básicamente responsable de determinar los recursos de QoS necesarios para la sesión en función de los descriptores de sesión recibidos, así como de gestionar los recursos de QoS atribuidos a dicha sesión.

El hecho de determinar los recursos de QoS para una sesión implica interpretar el descriptor de sesión y calcular la anchura de banda requerida, determinando el tipo de programación del tráfico y rellenando los clasificadores de tráfico. También implica determinar el número de flujos necesarios para la sesión (sesión de voz frente a sesión de voz y video) y gestionar la asociación de los flujos a la sesión.

II.7.1.3 Relación entre P-CSCF e IPAM

La arquitectura de IPCablecom multimedia proporciona una relación bien entendida y conocida entre el IPAM y el PS. Se describe a continuación la relación entre el P-CSCF y el IPAM. La arquitectura de QoS no se desarrolló con relaciones preconcebidas entre los dos elementos de red. Aunque la elección de cómo se despliegan los P-CSCF y los IPAM, y su cardinalidad asociada es principalmente una decisión de despliegue, en las figuras II.2 y II.3 se representan los escenarios de despliegue más habituales.

Figura II.2 – De uno a uno

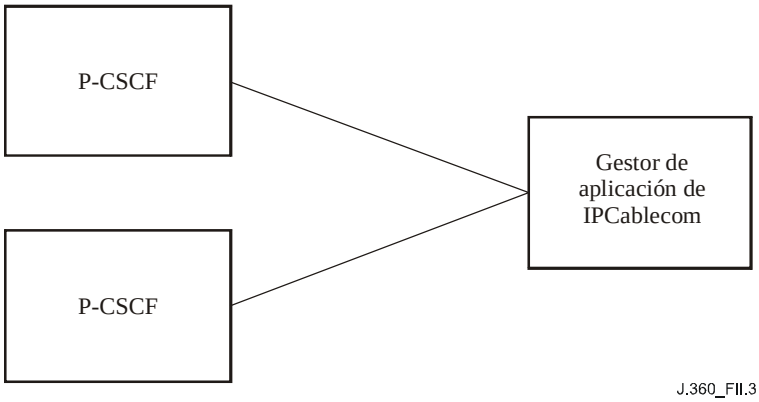


Figura II.3 – De varios a uno

En la figura II.2 se ilustra una relación biunívoca entre el P-CSCF y el IPAM. Aunque dicho despliegue es extremadamente sencillo de gestionar, puede no ser la forma más eficiente de utilizar los recursos. En la figura II.3 se ilustra una relación de varios a uno entre P-CSCF e IPAM. Este escenario mantiene la simplicidad de una relación biunívoca (puesto que el P-CSCF no tiene que determinar a qué IPAM ha de enviar su petición), pero puede ser una utilización más eficiente de recursos del IPAM.

Otro posible escenario que no se muestra es la relación de uno a varios (o de varios a varios). En este caso, el P-CSCF puede comunicarse con varios IPAM. Aunque este escenario se soporta, para el mismo no se proporcionan directrices sobre cómo el P-CSCF determina el IPAM al que ha de enviar sus peticiones. Este escenario puede llegar a ser necesario conforme la red evolucione y se invoquen distintos gestores de aplicación para diferentes redes de acceso o en determinados casos de itinerancia.

II.7.2 Interfaces del protocolo y puntos de referencia

En este apéndice se identifican varias interfaces o puntos de referencia en la arquitectura de QoS de IPCablecom2. La mayoría de dichos puntos de referencia son interfaces existentes definidos por IPCablecom multimedia. En esta cláusula se proporciona una visión general de la interfaz del protocolo entre P-CSCF y IPAM, ya que es la única interfaz definida por IPCablecom.

Esta interfaz puede no existir en la implementación de producto de un determinado suministrador. Por ejemplo, si un suministrador de P-CSCF decide integrar el IPAM en el P-CSCF, la interfaz entre P-CSCF e IPAM sería interna a dicho producto.

II.7.2.1 Descripción de la interfaz P-CSCF – IPAM

La interfaz entre P-CSCF e IPAM está basada en servicios Web. Permite que el P-CSCF solicite y suprima recursos de calidad de servicio en la red DOCSIS habilitada para IPCablecom multimedia.

La interfaz de los servicios web del gestor de aplicación de IPCablecom2 permite al P-CSCF solicitar la gestión de la QoS en la red de acceso en base a los parámetros del protocolo de descripción de sesión (SDP) incluidos en la oferta y la respuesta, tal como se define en [IETF RFC 3264]. El IPAM utiliza la interfaz pkt-mm-3 de IPCablecom multimedia para comunicar dichos requerimientos al servidor de política de IPCablecom multimedia.

II.7.3 Aplicación de una política de calidad de servicio en IPCablecom

El término control de política se ha utilizado frecuentemente para describir el proceso en virtud del cual se crea en la red de acceso un nuevo flujo o portador de servicio dinámico a petición de una aplicación. Ello tiene pleno sentido puesto que el establecimiento de un nuevo flujo de servicio en la red de acceso implica la inclusión de una nueva política dinámica en el punto de vigilancia del cumplimiento de la política. Esta política dinámica determina el tratamiento de los paquetes del nuevo flujo de servicio en la red de acceso durante la sesión.

Esta cláusula se centra en niveles más elevados de la política que pueden afectar a una petición de usuario que se procesa en la red. Dichas políticas pueden ser implementadas a varios niveles de la red a fin de responder a las necesidades de negocio de los operadores de red. La política puede aplicarse en los niveles siguientes:

- Nivel de aplicación: las aplicaciones pueden emplear la política para limitar el uso de un aplicación en base a la suscripción u otra información.
- Nivel de red de señalización: por ejemplo, el P-CSCF o el S-CSCF pueden imponer en una red IPCablecom restricciones basadas en la red o en la suscripción relativas a la utilización de determinados parámetros de medios en una oferta SDP enviando una respuesta negativa al mensaje SIP tal como se describe en las cláusulas 6.2 y 6.3 de [UIT-T J.366.4].
- Nivel de red portadora: cada uno de los elementos de red de la red portadora (gestor de aplicación de IPCablecom2, servidor de política y CMTS) tiene papeles singulares en relación con la política de control. A continuación se analiza más detalladamente el papel de cada elemento de red:
  - El gestor de aplicación de IPCablecom2 es el punto de entrada desde la red SIP al sistema de QoS de la red de acceso. El IPAM puede aplicar una política que tenga en cuenta el servicio limitado que proporciona el P-CSCF y potencialmente información basada en la suscrición.
  - El servidor de política puede recibir mensajes de varios gestores de aplicación incluyendo, aunque no exclusivamente, los gestores de aplicación de IPCablecom. Las políticas aplicadas en el PS pueden optimizar la utilización de recursos de la red de acceso entre múltiples aplicaciones y tipos de tráfico.
  - El CMTS es responsable del control de admisión y puede aplicar políticas que controlen la atribución de recursos entre varios tipos de tráficos en función de la clase de sesión y posiblemente del modelo de autorización utilizado, como IPCablecom e IPCablecom multimedia.

En algunos casos, podrían tomarse decisiones de política similares en más de un nivel de la red. La elección del nivel en que se implementa un determinada política será función de criterios tales como:

- El acceso a la información requerida.
- Los efectos sobre la calidad de funcionamiento de la política de implementación a dicho nivel.
- La facilidad de implementación de una política a un nivel dado.

Finalmente, la política se implementará al nivel de red que responda mejor a las necesidades de negocio del operador de cable.

II.7.4 Encaminamiento de peticiones de calidad de servicio

Asumiendo una relación entre P-CSCF e IPAM como la descrita en la cláusula II.7.1.3, el encaminamiento de las peticiones de QoS es estático, es decir, cada P-CSCF dispone de un único gestor de aplicación (con la posibilidad de un segundo gestor en caso de fallo del primero) al que se envían todas sus peticiones de QoS. En caso de que se utilice una relación entre varios P-CSCF y varios gestores de aplicación, el encaminamiento de peticiones queda fuera del campo de aplicación.

La arquitectura multimedia vigente no señala explícitamente nada sobre cómo se encaminan las peticiones de QoS entre el IPAM y el PS y entre el PS y el CMTS. A la vista de este vacío, IPCablecom ha definido un mecanismo dinámico para el encaminamiento de mensajes de QoS desde PS a CMTS. Este procedimiento se describe en [UIT-T J.362] y se basa en un enfoque de consulta asociada al trayecto. Una consulta asociada al trayecto es aquella consulta que sigue el mismo trayecto a través de la red que seguiría cualquier otro paquete destinado a un UE dado. Este mecanismo permite al PS aprovechar los protocolos de encaminamiento subyacentes para garantizar que se identifica el CMTS adecuado en base a la dirección IP del UE en cuestión.

En IPCablecom no se define el encaminamiento de las peticiones de QoS desde IPAM a PS.

II.8 Ejemplos de procedimientos

En esta cláusula se describe un ejemplo de comportamiento operacional basado en las interfaces y requisitos definidos en IPCablecom. Los flujos de llamadas que se muestran sólo son referencias destinadas a facilitar la comprensión de la arquitectura de QoS de IPCablecom2.

II.8.1 Llamada exitosa iniciada por el UE

En la figura II.4 se ilustra el caso de una llamada exitosa iniciada por el UE. En este ejemplo, el P-CSCF inicia el proceso de QoS cuando recibe un mensaje SIP con una oferta SDP (normalmente un mensaje INVITE). La P-CSCF pasa la oferta SDP al IPAM a través de la interfaz de QoS definida. EL IPAM puede traducir entonces las necesidades preliminares de la sesión en peticiones multimedia IPCablecom. Normalmente, ello conlleva la creación de varias puertas multimedia IPCablecom (por ejemplo, una llamada de audio normalizada tendría una puerta en sentido ascendente y otra puerta en sentido descendente).

La petición multimedia IPCablecom generada por el IPAM se pasa al servidor de política para verificaciones sobre la política aplicada. Dichas verificaciones se realizan normalmente a nivel de red, es decir, el servidor de política vela por que las peticiones satisfagan las políticas basadas en la red (la cantidad de recursos solicitados esté dentro de límites, el tipo de programación es el adecuado para el servicio, etc.). Una vez que dichos requisitos superan las verificaciones del servidor de política, se pasan al CMTS para su realización.

Cuando recibe la petición de recursos, el CMTS es responsable del control de admisión y de la atribución de recursos. Este proceso garantiza que el CMTS tiene los recursos adecuados para satisfacer la petición. Una vez que la petición ha pasado el control de admisión y se han atribuido los recursos, el CMTS inicia los flujos necesarios y realiza la notificación al módem de cable que atiende al UE a través de la interfaz de mensajería para intercambio dinámico de servicios (DSX, *dynamic service exchange*) definida de conformidad con DOCSIS. En esta etapa, los recursos solamente se reservan, no estando aún disponibles para su utilización. Una vez que la atribución de recursos se ha notificado con éxito al CM, el CMTS devuelve un identificador de flujo al servidor de política, y lo pasa al IPAM solicitante.

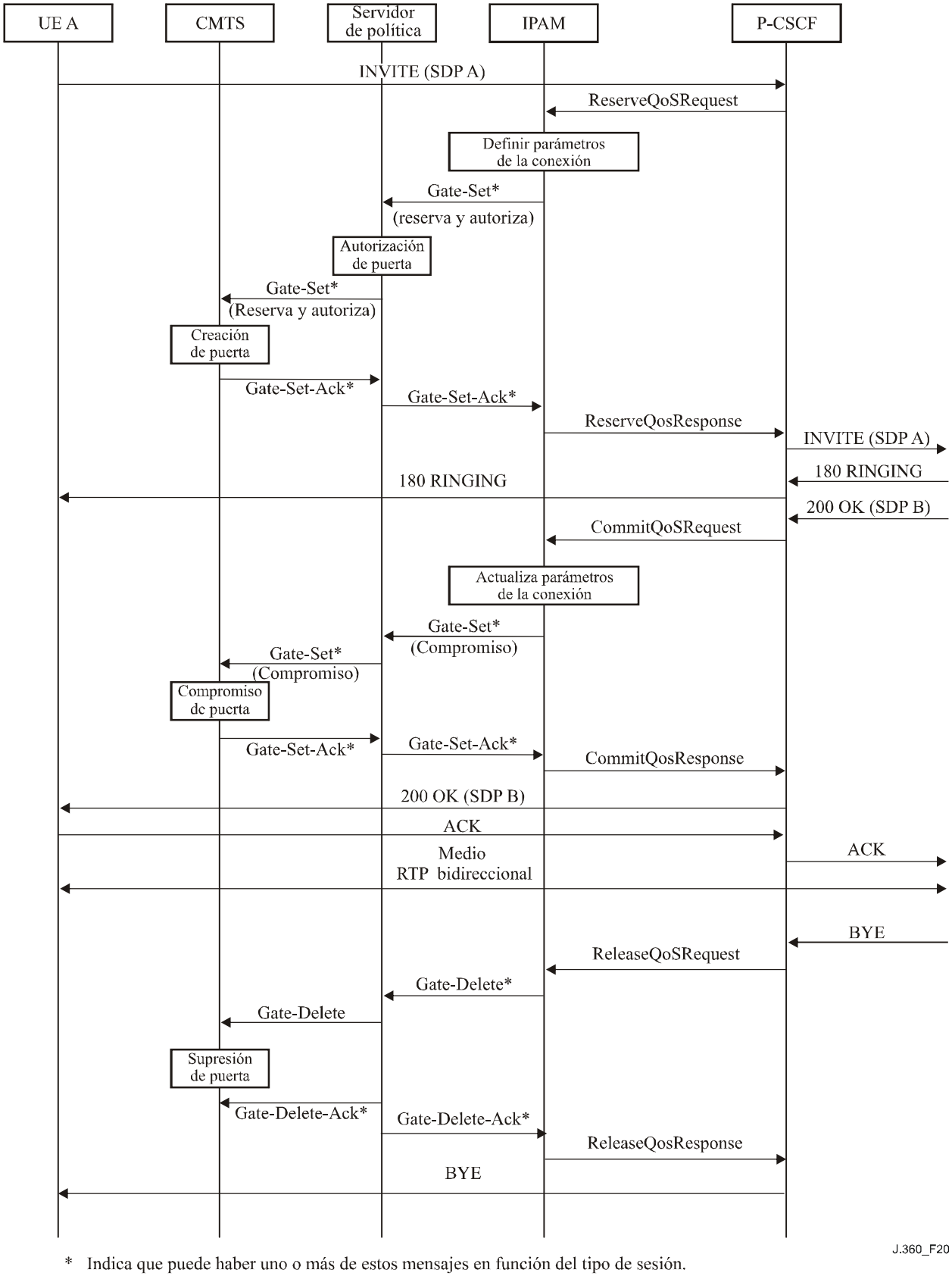
Una vez que el P-CSCF recibe la respuesta SDP, tiene suficiente información acerca de la parte distante como para comprometer los recursos para la sesión. Lo hace pasando la respuesta SDP al IPAM. El IPAM (conjuntamente con la oferta SDP) la traduce en una nueva petición IPCablecom

multimedia que actualiza los recursos previamente reservados. En la medida en que la petición actualizada sea igual o inferior en términos de recursos reservados, se garantiza su concesión.

Una vez que los recursos están comprometidos, la sesión puede empezar utilizando los flujos establecidos y recibir la QoS deseada.

Cuando se recibe un mensaje BYE, el P-CSCF libera los recursos asociados a la sesión mediante la petición ReleaseQoSResources.

En la figura II.4 se ilustra un ejemplo de llamada exitosa iniciada por un UE.



* Indica que puede haber uno o más de estos mensajes en función del tipo de sesión.

Figura II.4 – Ejemplo de llamada exitosa iniciada por un UE

Apéndice III

Visión general de la seguridad de IPCablecom2

(Este apéndice no es parte integrante de esta Recomendación)

III.1 Introducción

La arquitectura de seguridad de IPCablecom2 protege los datos, interfaces y componentes que conforman la arquitectura de IPCablecom2. En este apéndice se describen las relaciones de seguridad entre los elementos de la arquitectura de IPCablecom2.

Los objetivos de diseño de la arquitectura de IPCablecom2 incluyen:

- Soporte de mecanismos de confidencialidad, autenticación, integridad y control de acceso.
- Protección de la red frente a ataques por denegación de servicio, de interrupción de red y de apropiación indebida de servicios.
- Protección de los UE (es decir, de los clientes) de los ataques por denegación de servicio, vulnerabilidades de la seguridad, acceso no autorizado (desde la red).
- Soporte de la privacidad del usuario final mediante la encriptación y mecanismos de control del acceso a los datos de abonado, como por ejemplo, información de presencia.
- Mecanismos para la autenticación del dispositivo, UE y usuario, aprovisionamiento seguro, señalización segura y descarga segura de software.
- Aprovechamiento y ampliación de la arquitectura de seguridad del IMS para lograr los objetivos anteriores.

III.2 Referencias

En este apéndice se utilizan las referencias información adicionales siguientes:

[UIT-T J.366.4] Recomendación UIT-T J.366.4 (2006), *Subsistema multimedia IP (IMS) IPCablecom2: Protocolo de inicio de sesión (SIP) y protocolo de descripción de sesión (SDP) – Especificación nivel 3*. (3GPP TS 24.229)

[UIT -T J.366.7] Recomendación UIT-T J.366.7 (2006), *Subsistema multimedia IP (IMS) IPCablecom2: Seguridad de acceso IPCablecom2 para servicios pasados en IP*. (3GPP TS 33.203)

[UIT J.366.8] Recomendación UIT-T J.366.8 (2006), *Subsistema multimedia IP (IMS) IPCablecom2: Especificación de seguridad del dominio de red*. (3GPP TS 33.210)

[UIT J.366.9] Recomendación UIT-T J.366.9 (2006), *Subsistema multimedia IP (IMS) IPCablecom2: Especificación de arquitectura genérica de autenticación*. (3GPP TS 33.220)

[IETF RFC 1750] IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

[IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.

[IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

[IETF RFC 3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile*.

[IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*.

[IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP)*.

[IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

[ID SIP-OUTBOUND] *Managing Client Initiated Connections in the Session Initiation Protocol (SIP)*, http://www.ietf.org/internet-drafts/draft-ietf-sip-outbound 02.txt.

[ID TURN] *Obtaining Relay addresses from Simple Traversal of UDP Trough NAT (STUN)*, draft-ietf-behave-turn-00, March 2006.

[TS 23.002] 3GPP TS 23.002 v6.10.0 (2005), *Network architecture*.

[TS 33.222] 3GPP TS 33.222 v6.5.0 (2005), *Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)*.

III.3 Términos y definiciones

En este apéndice se utilizan los términos y definiciones adicionales siguientes:

III.3.1 módulo de identidad de servicio IM (ISIM, *IM services identity module*): el conjunto de datos y funciones de seguridad del IMS en un UICC, puede constituir una aplicación diferenciada.

III.3.2 IPCablecom multimedia: Una arquitectura de QoS agnóstica respecto a la aplicación para servicios en redes DOCSIS.

III.4 Abreviaturas, siglas o acrónimos

En este apéndice se utilizan las siguientes abreviaturas, siglas o acrónimos adicionales.

AKA Autenticación y acuerdo de clave (*authentication and key agreement*)

BSF Función de servidor de arranque (*bootstrapping server function*)

DDoS Ataque distribuido de denegación de servicio (*distributed denial of service attack*)

DNSSEC Seguridad del DNS (DNS *security*)

DoS Denegación de servicio (*denial of service*)

GBA Arquitectura genérica de arranque (*generic bootstrapping architecture*)

IDS Sistema de detección de intrusiones (*intrusion detection system*)

MiM Ataque que por intrusión (*man in the middle*)

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

SA Asociación de seguridad (*security association*)

UICC Tarjeta UMTS con circuitos integrados (*UMTS integrated circuit card*)

USIM Módulo universal de identidad de abonado (*universal subscriber identity module*)

III.5 Seguridad de IPCablecom2

La arquitectura de seguridad de IPCablecom2 describe los puntos de referencia y los componentes lógicos, así como los flujos de datos entre dichos componentes.

En esta cláusula se incluye:

- Una descripción de la relación entre las versiones del IMS de IPCablecom2 y 3GPP;
- Una visión general de la arquitectura de IPCablecom2;
- Una descripción de las amenazas a la arquitectura de IPCablecom2;
- Una descripción de los mecanismos de seguridad de IPCablecom2.

III.5.1 Relación con el IMS del 3GPP

IPCablecom2 se basa en el IMS definido por el proyecto de colaboración para la tercera generación (3GPP). El 3GPP es un acuerdo de colaboración entre varios organismos de normalización con el objetivo de elaborar especificaciones e informes técnicos para las redes de los sistemas móviles GSM y de Tercera Generación (3G).

En el marco del objetivo general de IPCablecom de aprovechar las normas existentes de la industria, siempre que ello sea posible, existe el objetivo concreto de la alineación con la arquitectura y especificaciones del IMS que desarrolle el 3GPP. Específicamente, IPCablecom2 reutilizará muchas de las entidades e interfaces básicas del IMS. Aunque en este apéndice se analiza el IMS, su objetivo principal es describir las mejoras y modificaciones a las especificaciones del 3GPP. Para más información sobre la arquitectura del IMS del 3GPP véase [TS 23.002].

III.5.2 Arquitectura de referencia de IPCablecom2

En la figura III.1 se muestra una visión general de los elementos y agrupaciones funcionales de la arquitectura de IPCablecom2.

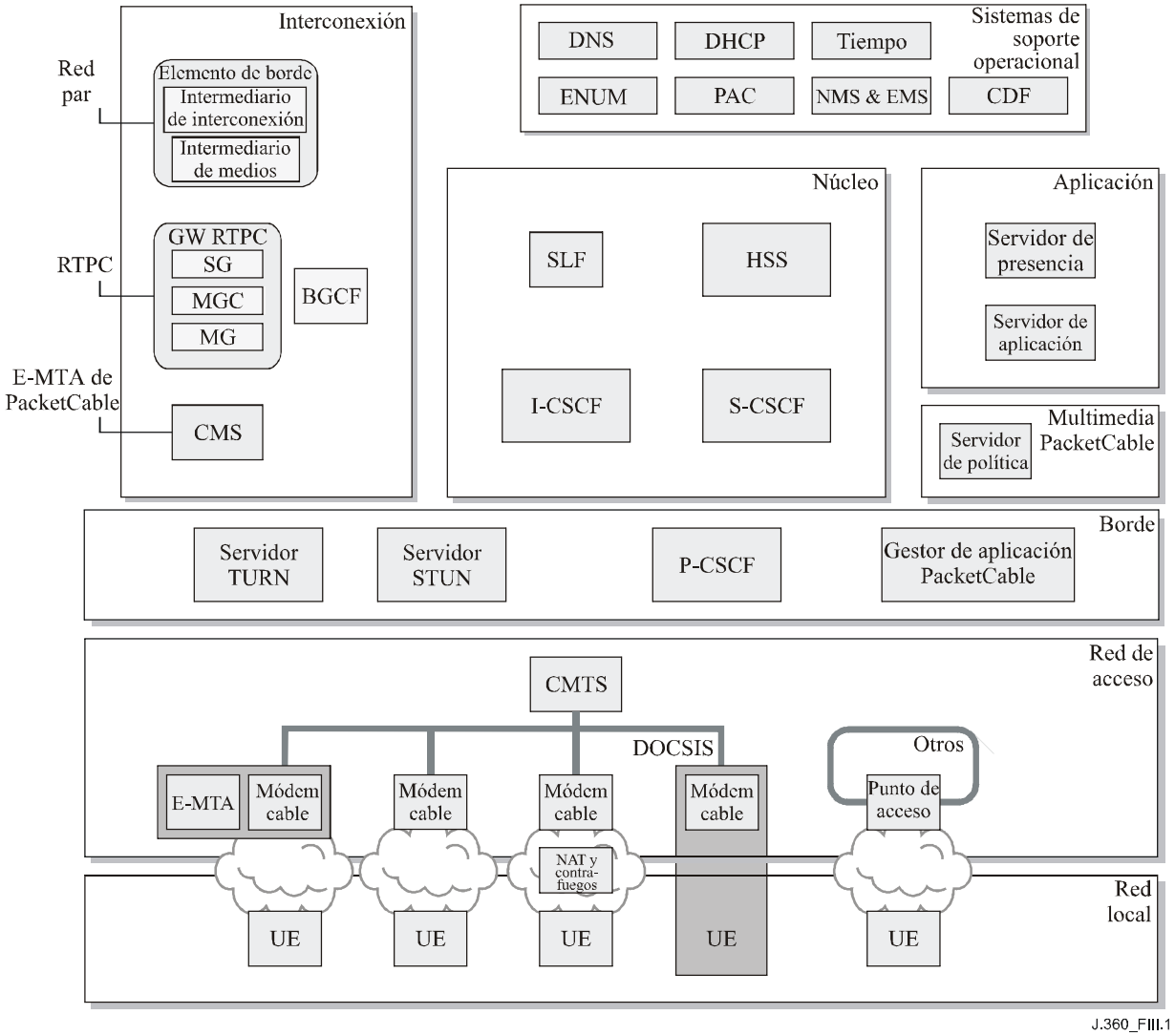


Figura III.1 – Arquitectura de referencia de IPCablecom

La arquitectura de IPCablecom2 se basa en la arquitectura del IMS con las ampliaciones adicionales necesarias para soportar las redes de cable. Dichas ampliaciones incluyen la utilización componentes adicionales o alternativos, así como mejoras de las capacidades que proporcionan los componentes funcionales del IMS.

Algunas de las principales mejoras que IPCablecom2 incorpora al IMS son las siguientes:

- Soportar calidad de servicio para aplicaciones basadas en IMS sobre redes de cable, aprovechando la arquitectura multimedia de IPCablecom;
- Soportar que la señalización y los medios transiten los dispositivos de traducción de direcciones de red (NAT, *network address translation*) y las barreras contrafuegos (FW, *firewall*) en base a mecanismos establecidos por el IETF;
- Soportar la identificación inequívoca y la comunicación con un UE individual cuando se hayan registrado varios UE con la misma identidad pública;
- Soportar seguridad de la señalización de acceso y mecanismos de autenticación de UE adicionales para los UE de IPCablecom;
- Soportar la provisión, activación, configuración y gestión de los UE de IPCablecom.

IPCablecom2 incluye los componentes lógicos y los puntos de referencia del IMS existentes, así como elementos lógicos y puntos de referencia añadidos para soportar los requisitos de IPCablecom2.

III.5.3 Amenazas a la seguridad en IPCablecom2

III.5.3.1 Amenazas generales: clasificación y análisis

A continuación se presenta una visión global de las amenazas generales en el contexto de una arquitectura genérica de comunicaciones multimedia basadas en IP.

III.5.3.1.1 Amenazas a dominios confiables

Un dominio confiable es una agrupación de elementos de red que son confiables para comunicarse de forma consistente con un conjunto de políticas de seguridad relevantes. Los dominios confiables pueden estar delimitados por fronteras físicas o lógicas. La comunicación a través de dominios confiables siempre está sujeta a revisión a los efectos de autenticación y autorización. Las interfaces de interés en una infraestructura multimedia IP son las siguientes:

- Interfaces en el dominio interno de la red (intra-red), que conectan los elementos de red en el dominio de un proveedor de servicio. Un compromiso relativo a un elemento de red puede ir en detrimento del funcionamiento adecuado de la red. En esta cláusula se recogen casi todas las amenazas que pueden producirse.
- Interfaces en el dominio entre redes, que conectan dos dominios. Los dominios pueden corresponder a proveedores de servicio diferentes o al mismo proveedor. Los niveles de confianza entre dominios pueden determinar el nivel de confianza que se pueden tener dentro de un dominio (intra dominio), y por tanto, es imperativo que dichas interfaces sean seguras. Además, la seguridad de dos dominios conectados de esa forma descansa en todas las demás conexiones establecidas por cada dominio individual.
- Interfaces en el dominio de acceso, que permiten que los UE se conecten con un proveedor de servicio. Este conjunto de interfaces es altamente vulnerable a multitud de amenazas de seguridad, debidas en su mayor parte al hecho de que los dominios típicamente contienen UE y elementos de red que pueden ser confiables y no confiables. Cualquiera que sea la red de acceso, una autenticación robusta es vital para un proveedor de servicio. Si la autenticación desaparece, deben minimizarse los servicios ofrecidos y los elementos de red a los que se proporciona acceso no autenticado.

III.5.3.1.2 Apropiación indebida del servicio

La "apropiación indebida del servicio" hace referencia a múltiples amenazas, incluyendo de forma no exhaustiva las siguientes:

- Manipulación del equipo de usuario (UE) – Los UE, especialmente los basados en software, son vulnerables a ataques troyanos y a la manipulación de su comportamiento. Las técnicas de mitigación incluyen la utilización de código firmado y de UEs integrados.
- Explotación de las debilidades de los protocolos – La explotación de medidas criptográficas débiles puede tener un gran impacto, ya que típicamente conlleva la necesidad de un redespliegue importante. Para mitigarlo existen diversas técnicas, entre las que se incluye la aplicación de una arquitectura con características de diseño muy defensivas.
- Falsificación o suplantación de identidad – Es la acción de hacerse pasar por otro usuario para conseguir el acceso a los servicios. Ello puede conducir a una pérdida de credibilidad y de ingresos. Para mitigarlo se puede utilizar una autenticación robusta y la educación del usuario.
- Clonación de UE – Es el acto de imitar un UE legítimo. Es típicamente un asunto relevante cuando las identidades de los UE se consideran suficientes para ofrecer servicios, como es el caso en arquitecturas que no distinguen entre "usuario" y "cliente". La recomendación es

exigir las credenciales a los UE a fin de autenticar a los usuarios antes de ofrecerles servicios y construir infraestructuras que puedan identificar la clonación y mitigar las amenazas

- Fraude de suscripción e impago de servicios – Las suscripciones establecidas con información falsificada y la detección de impagos estén fuera del alcance de esta especificación

III.5.3.1.3 Interrupción y denegación del servicio

Los ataques generales de denegación de servicio (DoS) tratan de provocar la interrupción del servicio saturando algunas o todas las entidades proveedoras de servicios de la red. Estos ataques se realizan a los niveles 2 a 4 del modelo de referencia de interconexión de sistemas abiertos. Los ataques por denegación de servicio se basan en hacer que un elemento dado de la red quede inutilizable mediante alguno de varios mecanismos posibles. Los ataques por DoS incluyen:

- Ataques por mensajes malformados – El atacante genera mensajes malformados para detectar alguna debilidad en la robustez de una pila de protocolos. Las debilidades incluyen el desbordamiento de memorias intermedias o la insuficiencia de la capacidad para tratar fallos de múltiples parámetros y de errores. Para mitigar este tipo de ataque se requieren pilas de protocolos software bien diseñadas y pruebas de robustez.
- Ataques por vaciamiento de la capa cuatro – El atacante hace que el dispositivo víctima se vea obligado a manejar una cantidad excesiva de información de estado, a menudo en el contexto de pilas de protocolo conscientes del estado. Un ejemplo de ello es un ataque a nivel TCP, como es el caso de inundación con mensajes de sincronismo (SYN), técnica utilizada para agotar los recursos de la pila que verifica cuál es el estado de la sesión. Estos ataques pueden mitigarse mediante sistemas de detección de intrusiones (IDS, *intrusion detection systems*) y contrafuegos, así como mediante pilas de protocolo bien dimensionados y pruebas de robustez.
- Ataques por inundación a nivel portador – Son ataques por denegación de servicio basados en que un determinado elemento de red quede indisponible, normalmente mediante el envío de una cantidad excesiva de tráfico de medios desde la red a sus interfaces. Para prevenir este tipo de ataque se requieren barreras contrafuegos con capacidad para conocer el estado y que abran puntos de acceso a los medios solamente si la conexión la inicia el lado confiable de la barrera contrafuegos. Los ataques por inundación a menudo utilizan direcciones de origen falsificadas para abrir agujeros de acceso en la barrera contrafuegos. La amenaza puede mitigarse verificando la dirección de origen con tomas de contacto tridireccionales. La calidad de servicio (QoS) puede asimismo prevenir que exista un número excesivo de flujos a través de un encaminador dado.

Los ataques por inundación utilizan paquetes IP con direcciones de origen falsificadas (*spoofed*). Algunos ataques por inundación pueden evitarse rechazando los paquetes con direcciones falsificadas. Existen varios mecanismos para evitar la falsificación de direcciones:

- Utilización de un mecanismo de desafío/respuesta como STUN o TURN;
- Utilización de TCP, que hace más sencilla la verificación de dirección (toma de contacto tridireccional);
- Retransmisión de trayecto inverso en unidifusión (uRPF, *unicast reverse path forwarding*), que utiliza tablas de encaminamiento para determinar si la ruta a la fuente del paquete (el trayecto inverso) apunta a la interfaz por la que entra el paquete.

Los ataques zombi son ataques por denegación de servicio lanzados desde un punto extremo autenticado. Además, la mayoría de los ataques zombi utilizan un gran número de zombis, produciendo así un ataque de denegación de servicio distribuido (DDoS, *distributed denial of service attack*). Típicamente, un troyano pone en peligro un punto extremo aprovechando la

autenticación del mismo. La defensa frente a un ataque zombi es muy difícil porque el punto extremo está autenticado y autorizado. Los ataques zombi pueden ser minimizados detectando un comportamiento anómalo del tráfico y filtrando el tráfico malicioso.

III.5.3.1.4 Amenazas al canal de señalización

En un entorno multimedia, como es el caso de una arquitectura SIP, los mensajes de señalización incluyen datos relativos a la identidad, servicios, encaminamiento y otros datos sensibles y críticos. En el dominio de acceso existen componentes multimedia, como los intermediarios, que los exponen a un gran número de amenazas.

Los ataques a la seguridad de la señalización incluyen:

- Riesgo de pérdida de confidencialidad – La información de señalización, como la identidad del llamante y los servicios suscritos por el cliente, son vulnerables a ser descubiertos. La información de identificación del llamante también puede utilizarse para localizar al llamante aunque éste desee mantener en privado su localización.
- Ataques por interposición (MiM, *man in the middle*) – Se trata de ataques que son consecuencia de la interceptación y posible modificación del tráfico entre dos partes de la comunicación. Estos ataques tienen éxito si las partes de la comunicación no pueden distinguir las comunicaciones con el receptor deseado de las que se tienen con el atacante. Los ataques, algunos de los cuales se describen en otras cláusulas, incluyen la usurpación de la personalidad del intermediario, el redireccionamiento indeseado y la pérdida de privacidad debido a una intervención de interposición (MiM).
- Ataques por denegación de servicio (DoS) – Los ataques DoS en el canal de señalización van desde la creación de peticiones falsas que dan lugar a ataques por amplificación, hasta la falsificación de las cabeceras de encaminamiento. La utilización de multidifusión para transmitir peticiones SIP aumenta notablemente las posibilidades de ataques por denegación de servicio.

Muchas de estas amenazas pueden mitigarse exigiendo autenticación mutua, confirmación de identidad, confidencialidad e integridad en el plano de señalización.

III.5.3.1.5 Amenazas al canal portador

Las amenazas sobre el canal portador están relacionados con el tráfico de medios transferido entre las partes de la comunicación.

Los ataques a la seguridad del portador incluyen:

- Riesgo de pérdida de confidencialidad – En este sentido, la confidencialidad hace referencia a la protección de los propios mensajes de medios, que podrían ser de una sesión de audio, mensajería instantánea u otra transferencia de mensajes multimedia. En función de los mecanismos de seguridad negociados, la confidencialidad extremo a extremo puede estar o no bajo el control del emisor.
- Riesgo de pérdida de la integridad – El canal portador puede sufrir ataques por modificación, supresión y repetición.
- Ataques por interrupción – Como ocurre con cualquier tecnología de medios, la capacidad de las partes para comunicarse introduce comunicaciones indeseadas. Esta categoría incluye todos los ataques a la red telefónica pública conmutada (RTPC) "normal" tales como los ataques por hostigamiento, así como algunas nuevas amenazas relativas a la degradación e interrupción del servicio en el modelo de IP.

Los ataques sobre el canal portador se mitigan requiriendo la autenticación mutua, la confidencialidad y la integridad en el plano portador a fin de evitar la manipulación de los datos en el mismo y garantizar la privacidad de información sensible.

III.5.3.1.6 Reconocimiento

Los ataques bien planificados a proveedores de servicio comienzan normalmente consiguiendo el reconocimiento en una red. Las amenazas por reconocimiento pueden mitigarse utilizando mecanismos de ocultación de la topología, incluyendo la introducción de elementos de borde. La obligatoriedad de utilizar técnicas de filtrado en el dominio de acceso permite aplicar con carácter obligatorio una política de tráfico en el borde de la red.

III.5.3.1.7 Consideraciones sobre el modelo de itinerancia

Los modelos de itinerancia pueden minimizar o incrementar las amenazas de seguridad. Los UE que acceden a servicios a través de entornos que les son ajenos pueden exponer al UE y a su red origen a mayores riesgos. En el límite de seguridad entre los respectivos dominios se obliga a la adopción de una relación de confianza entre las redes origen y visitada.

III.5.3.2 Amenazas de seguridad específicas del protocolo

En las cláusulas siguientes se ilustran amenazas que se ciernen sobre protocolos multimedia. Aunque la lista no incluye todos los protocolos multimedia, incluye los principales protocolos analizados en la arquitectura y en las cláusulas anteriores.

III.5.3.2.1 SIP

A continuación se exponen ejemplos de ataques que pueden realizarse a partir de información obtenida capturando mensajes SIP en la red:

- Manipulación del cuerpo del mensaje (por ejemplo, enviando mensajes SIP malformados para interrumpir el funcionamiento de un elemento de red SIP, enviado mensajes REGISTER falseados para redireccionar los mensajes de señalización, dejando al UE secuestrado incapaz de iniciar o aceptar sesiones);
- Terminación indeseada de sesiones (por ejemplo, enviando mensajes BYE o CANCEL para terminar prematuramente una sesión);
- Suplantación de un servidor (por ejemplo, enviando mensajes INVITE falsos);
- Enmascaramiento y falseado de respuestas del servidor, induciendo la indisponibilidad o denegación de servicio (por ejemplo, inundando la red con mensajes 302 Redirect o 401 Unauthorized).

En las subcláusulas siguientes se explican algunas de las vulnerabilidades más relevantes.

III.5.3.2.1.1 Secuestro de registro

En el secuestro de registro un punto extremo malicioso cambia el registro de otro punto extremo existente para que apunte al atacante o a otro lugar diferente. El secuestro de registro puede tener varias formas:

- Clonación de punto extremo SIP – Un agente de usuario (UA) atacante pude intentar registrarse como un UE víctima existente. El UE atacante se convierte en un clon del UA víctima, robando la identidad de la víctima.
- Explotación de identidad débil – Si un registro evalúa la identidad de un UA, la cabecera "From:" de una petición SIP puede ser modificada arbitrariamente y quedar así expuesta a un registro malicioso.
- Los atacantes pueden desregistrar a alguno o todos los usuarios de un dominio administrativo, impidiendo que dichos usuarios sean invitados a nuevas sesiones y produciendo así un tipo de ataque DoS.

Para más información sobre secuestro de registro véase la cláusula 26.1.1 de [IETF RFC 3261]. El método general para prevenir el secuestro de registro es realizar una confirmación segura de la identidad.

III.5.3.2.1.2 Falseamiento de identidad de usuario

Salvo que estén autenticados, los mensajes SIP son vulnerables a la falsificación o suplantación de la identidad. No es necesario rellenar campos tales como "From:", mientras que "P-Asserted-Identity" puede ser manipulado salvo que sea rellenado de forma segura por un elemento confiable.

Las siguientes son posibles soluciones para mitigar dicha amenaza:

- Utilización de credenciales fuertes y establecimiento de túneles seguros para los flujos de mensajes.
- Utilización de mecanismos de identidad SIP adecuados, tales como "identidad SIP" que apoye confirmaciones criptográficamente verificables.

III.5.3.2.1.3 Mensajes SIP malformados

Un atacante puede enviar mensajes SIP malformados que intenten explotar una debilidad en la robustez de una pila SIP o del propio protocolo. Dicha debilidad incluye el inicio de DoS injustificados, el desbordamiento de memorias intermedias o la insuficiencia de capacidad para el tratamiento de fallos de múltiples parámetros. Para mitigar este tipo de ataque se debe realizar una prueba de robustez de la pila. Entre los escenarios que conducen a ataques DoS se encuentran los siguientes:

- Utilización de campos de cabecera "Via" falsificados que identifican un anfitrión objetivo como origen de la petición, enviando dichas peticiones a un gran número de elementos de red SIP.
- Utilización de campos de cabecera "Route" falsificados en una petición que identifica el anfitrión objetivo, enviando dichos mensajes a intermediarios con bifurcaciones, amplificando así el número de mensajes enviados al objetivo.

Los servidores intermediarios SIP aceptan por naturaleza las peticiones procedentes de puntos extremos IP diferentes y, consecuentemente, están expuestos a un número creciente de amenazas.

III.5.3.2.1.4 Tormentas de mensajes SIP

Las tormentas de mensajes SIP pueden consistir en el envío de mensajes SIP de forma aleatoria para que la memoria o la capacidad de proceso quede agotada por el almacenamiento de estados o por los pasos de encriptación requeridos, respectivamente. Las tormentas de mensajes SIP pueden proceder de la propia red o del exterior de la misma. Las técnicas de mitigación destinadas a reducir el efectos de dichos ataques incluyen lo siguiente:

- Depuración de pilas para el vaciado de recursos;
- Utilización de contramedidas anti-repetición;
- Evitar múltiples respuestas a un único evento (por ejemplo, múltiples mensajes 401 para un desafío de autenticación);
- Detección de tormentas y utilización de los filtros adecuados para clausurar los UE con un comportamiento anómalo.

Las tormentas de mensajes pueden producirse por inundaciones de eventos de registro, cuando un gran número de puntos extremos intentan registrarse, pero la autenticación falla en el borde de la red y los intermediarios de borde se bloquean. Además, los intermediarios de borde pueden permitir que los puntos extremos se registren sin autenticación y trasladan el desafío del UE a servidores internos de la red, siendo entonces dichos servidores internos susceptibles de sufrir inundaciones de DoS. Existen varias formas de mitigar este tipo de ataques:

- Requerir la autenticación en los intermediarios de borde, para así distribuir la carga debida a la autenticación y defenderse de las inundaciones de DoS por eventos de registro;

- Imponer medidas de control de inundación – proporcionar una palabra singular (una "nonce") a un UE que se autentica por vez primera, que puede utilizarse posteriormente al amparo de una limitación de tasa uso de menos estricta;
- Permitir que el P-CSCF otorgue prioridad a la señalización, en base a desafíos exitosos anteriores del mismo UE.

III.5.3.2.1.5 Secuestro de sesión

El ataque por secuestro de sesión puede realizarse de varias formas, entre las que se encuentran las siguientes:

- Modificación de información del SDP;
- Utilización de mensajes tales como "301 moved permanently" para la redirección de mensajes INVITE a otra ubicación (asumiendo que el atacante conoce los campos Call-ID, To, From, Cseq).

El método general para prevenir el secuestro de sesión es requerir la autenticación de todos los mensajes SIP.

III.5.3.2.1.6 Suplantación de un servidor

Los servidores SIP pueden ser suplantados en la red por un atacante. La suplantación de un servidor SIP puede dar lugar a una situación de denegación de servicio o de quebrantamiento de la privacidad. Presenta un problema probablemente mayor cuando se considera la movilidad SIP. El método general de prevenir la suplantación es la autenticación de servidor por los agentes de usuario.

Para más información véase la cláusula 26.1.2 de [IETF RFC 3261].

III.5.3.2.1.7 Manipulación de cuerpos de mensajes

Para más información véase la cláusula 26.1.3 de [IETF RFC 3261].

III.5.3.2.1.8 Terminación de sesión

Para más información véase la cláusula 26.1.4 de [IETF RFC 3261].

III.5.3.2.1.9 Reconocimiento de amenazas

Determinados campos y mensajes SIP facilitan el reconocimiento de amenazas. La mitigación de dichas amenazas pueden facilitarse evitando la utilización de determinados campos (por ejemplo, OPTIONS) en los mensajes.

III.5.3.2.2 TUN

En general, los ataques sobre STUN pueden clasificarse como ataques por denegación de servicio y ataques por escucha. Los ataques por denegación de servicio pueden lanzarse contra un servidor STUN o contra otros elementos que utilicen el protocolo STUN.

Muchos de los ataques requieren que el atacante genere una respuesta a una petición STUN legítima a fin de proporcionar al UE una MAPPED-ADDRESS (dirección correspondiente) falseada. Los ataques que pueden lanzarse utilizando esta técnica incluyen:

- Denegación de servicio distribuido (DDoS) contra un objetivo
- Silenciamiento de un UE
- Asunción de la identidad de un UE
- Escucha

Para una información más detallada de estos ataques y de cómo los trata el protocolo STUN véase [IETF RFC 3489].

III.5.3.2.3 TURN

Un servidor TURN actúa como redireccionador para canalizar los trenes de medios a través de un NAT hacia un destino. Por lo tanto, un servidor TURN tiene la potencialidad de convertirse en origen de un ataque por DoS que utilice trenes de medios de gran anchura de banda. Para prevenir una utilización indebida de un servidor TURN resulta crítico disponer de una forma criptográficamente verificable de establecer un mecanismos de autenticación y autorización que permita a los receptores de trenes de medios autorizar al servidor TURN un reenvío de medios.

III.5.3.2.4 TLS

Debido a que la seguridad de la capa de transporte (TLS, *transport layer security*) se realiza tramo a tramo, puede ponerse en riesgo en un servidor que termina y re-origina señalización

La TLS también se basa en un mecanismo que establece la confianza entre dos entidades de comunicación, como es la infraestructura de clave pública (PKI, *public key infrastructure*) en un dominio administrativo. El establecimiento de TLS entre servidores implica autenticación mutua.

La TLS en general se basa en una confianza de naturaleza transitiva para la seguridad tramo a tramo. Si cada punto extremo tiene su servidor local y entre los servidores locales existe confianza, los puntos extremos pueden asumir, en virtud del carácter transitivo de la confianza, que la comunicación extremo a extremo es segura.

III.5.3.2.5 HTTP Digest

La amenaza principal que existe para la autenticación HTTP Digest son los ataques por interposición (MiM, *man in the middle*). HTTP Digest actúa verificando que un usuario tiene una contraseña previamente compartida. Una vez que el UE solicita acceso a un recurso, el servidor desafía al UE para que entregue una contraseña. Durante el desafío, el servidor envía una palabra única (*nonce*) sin cifrar que es utilizada por el UE para generar de forma segura una función de resumen y troceo (*hash*) de la contraseña. La contraseña troceada y resumida se envía al servidor sin cifrar. Este método de autenticación es susceptible de un ataque por interposición (MiM) que utilice un ataque por diccionario en un intento por encontrar una palabra que genere el mismo resumen (*hash*) seguro como valor a devolver al servidor. En consecuencia, la autenticación HTTP Digest debería utilizarse sobre trayectos de datos seguros.

III.5.3.2.6 DNS

El servicio de nombres de dominio (DNS, *domain name service*) es en general inseguro si no se utiliza DNSSEC. Las posibles amenazas de seguridad incluyen la manipulación de consultas de petición o respuesta que generan una redirección o denegación de servicio, y la utilización de una funcionalidad de DNS dinámico, si está permitida, para manipular servidores DNS y reflejar topologías incorrectas.

Para mitigar algunas de estas amenazas, el DNS sólo debe utilizarse para información general, utilizando otros mecanismos de configuración, como la autenticación, para validar elementos de red.

III.5.3.2.7 UE basados en software

IPCablecom soporta UE basados en software para autenticar y utilizar servicios de red. Los UE basados en software presentan desafíos que conducen a determinadas vulnerabilidades:

- Aunque los UE basados en software pueden tener prevista la conexión a un dispositivo hardware de almacenamiento de claves, como por ejemplo, una tarjeta inteligente, generalmente almacenan las credenciales en un sistema de almacenamiento desprotegido
- La imagen software en un UE basado en software no está protegida contra la manipulación
- Las aplicaciones sobre UE basados en software pueden almacenar una contraseña de usuario para una posterior entrada automatizada.

III.5.4 Arquitectura de seguridad de IPCablecom2

En esta cláusula se describe la arquitectura de seguridad de IPCablecom2, incluyendo las mejoras del IMS. Los dominios confiables descritos en la cláusula III.5.3 se utilizan para descomponer la arquitectura de IPCablecom2. En las cláusulas siguientes se discute en detalle cada dominio confiable.

III.5.4.1 Dominio de acceso

Los UE se conectan a la red a través del dominio de acceso. En la figura III.2 se muestran las interfaces y componentes presentes en el dominio de acceso.

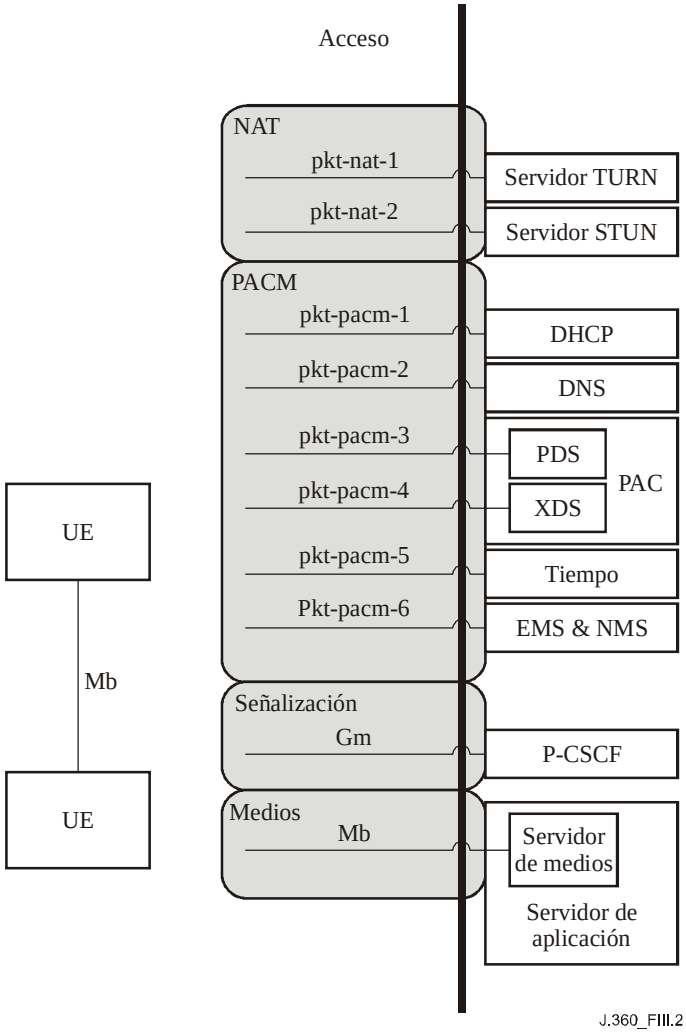


Figura III.2 – Puntos de referencia del dominio de acceso

Las interacciones del UE con la red tienen lugar en el dominio de acceso. Los métodos de acceso son diversos e incluyen DOCSIS y sistemas inalámbricos. Debido a dichas características, el dominio de acceso es objeto de numerosas amenazas, tal como se describe en la cláusula III.5.3.

En el cuadro III.1 se incluye una visión general de alto nivel de la arquitectura de seguridad resultado de las mejoras que IPCablecom2 introduce en el IMS. Se incluye cada punto de referencia del dominio de acceso junto con el mecanismo de seguridad empleado en dicha interfaz.

Cuadro III.1 – Descripción de los puntos de referencia del dominio de acceso

Punto de referencia	Elementos de red de IPCablecom2	Descripción de la seguridad de los puntos de referencia
pkt-nat-1	UE – Servidor TURN	TURN: las peticiones TURN se autentican y autorizan en el propio protocolo TURN.
pkt-nat-2	UE – Servidor STUN externo	STUN: integridad del mensaje mediante mecanismos STUN.
pkt-pacm-1	UE – Servidor DHCP	DHCP: IPCablecom2 no define seguridad para el protocolo DHCP.
pkt-pacm-2	UE – Servidor DNS	DNS: IPCablecom2 no define seguridad para el protocolo DNS.
pkt-pacm-3	UE – Servidor PDS	SIP: integridad y privacidad de mensajes mediante IPsec o TLS.
pkt-pacm-4	UE – Servidor XDS	XCAP: integridad y privacidad de mensajes mediante HTTP sobre TLS
pkt-pacm-5	UE – Servidor de tiempo	SNTP: IPCablecom2 no define seguridad para el protocolo SNTP.
pkt-pacm-6	UE – Servidor EMS y NMS	La seguridad de la interfaz de gestión está fuera del alcance de esta especificación.
Gm	UE – P-CSCF	SIP: integridad y privacidad de mensajes mediante IPsec o TLS. STUN: integridad del mensaje mediante mecanismos STUN (dado que las peticiones STUN se envían al puerto SIP normalizado, el P-CSCF debe contener lógicamente la funcionalidad STUN).
Mb	UE – UE UE – Servidor de medios UE – MG UE – E-MTA	RTP: la seguridad de los medios está fuera del alcance de esta especificación.

III.5.4.2 Dominio interno a la red

Los puntos de referencia y componentes intra-dominio están dentro de la red de un proveedor de servicio, y consecuentemente, al amparo de una política de seguridad global.

El IMS define la seguridad de las conexiones internas del dominio mediante la interfaz Zb, tal como se describe en [UIT-T J.366.8]. En el IMS la integridad es obligatoria y la confidencialidad opcional cuando se implementa la interfaz Zb. Se utiliza ESP IPSec para proporcionar servicios de seguridad para la interfaz Zb entre los componentes internos al dominio.

IPCablecom mejora la interfaz Zb añadiendo TLS para proporcionar servicios de seguridad a los flujos de datos TCP internos al dominio. En la cláusula III.6.6 se describen los requisitos de TLS del punto de referencia Zb.

III.5.4.3 Dominio entre redes

Los puntos de referencia entre dominios conectan el dominio de seguridad del operador con asociados y redes externas. Estas conexiones permiten el interfuncionamiento de la red del operador y otras redes y proveedores de servicio, incluyendo la RTPC. En la figura III.3 se muestra la frontera de confianza entre dominios.

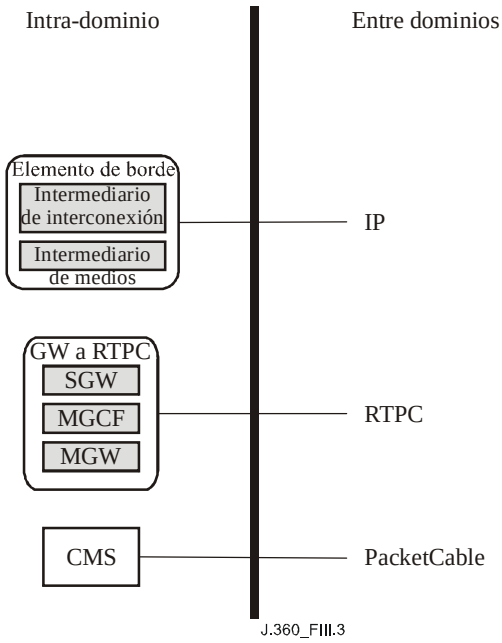


Figura III.3 – Puntos de referencia del dominio entre redes

El IMS define la seguridad de la conectividad entre dominios mediante la interfaz Za, tal como se describe en [UIT-T J.366.8]. Para la interfaz Za, se requiere tanto la integridad como la confidencialidad sobre la base de ESP IPSec. En el IMS el tráfico entre dominios ha de pasar a través de una pasarela de seguridad (SEG, *security gateway*). La SEG termina los túneles IPSec del punto de referencia Za e impone una política de seguridad a los flujos de tráfico entre dominios. En la figura III.3 se muestra una arquitectura que incluye la funcionalidad SEG en el elemento de borde, aunque el SEG puede ser un elemento separado.

La pasarela RTPC con el punto de referencia RTPC se hace segura empleando mecanismos de seguridad de la RTPC.

IPCablecom2 soporta el interfuncionamiento con redes IPCablecom. El servidor de gestión de llamadas (CMS, *call management server*) proporciona la traducción de los mensajes de IPCablecom. En [UIT-T J.170] se describe con detalle la seguridad para el punto de referencia del CMS.

III.6 Requisitos de seguridad de IPCablecom

En las cláusulas siguientes se describen las mejoras que IPCablecom2 aporta a la arquitectura de seguridad del IMS.

III.6.1 Autenticación de usuario y de UE

El IMS del 3GPP se apoya completamente en credenciales almacenadas en tarjetas UMTS con circuitos integrados (UICC, *UMTS integrated circuit card*) para la seguridad en el acceso. La UICC es una plataforma para aplicaciones de seguridad utilizada para autenticación y acuerdo de clave (AKA, *autheticacion and key agreement*). Un requisito de IPCablecom es soportar múltiples tipos de UE, tales como UE basados en software, que podrán tener o no acceso a los UICC.

En [UIT-T J.366.7] se describe el enfoque del IMS a la autenticación y al establecimiento de seguridad de transporte entre el UE y el P-CSCF. El IMS utiliza una combinación de IPSec para la integridad y la confidencialidad opcional e IMS AKA para la autenticación. Para cumplir los requisitos del IMS relativos a tiempos de ida y vuelta mínimos, los elementos de seguridad de la negociación "descansan" en el flujo de mensajes de registro SIP. La [IETF RFC 3329] se utiliza

para negociar la seguridad entre el UE y el P-CSCF, y el IMS AKA [IETF RFC 3310] se utiliza entre el UE y el S-CSCF para realizar la autenticación mutua. La [IETF RFC 2617] se amplía para la transferencia de datos de autenticación entre el UE y el S-CSCF. Las comunicaciones entre el UE y el P-CSCF y las comunicaciones entre el UE y el S-CSCF están relacionadas porque el material para las claves de las asociaciones de seguridad entre el UE y el P-CSCF se calcula utilizando el secreto compartido a largo plazo almacenado en el servidor de abonado de la red de origen (HSS) y en la UICC en el UE. En la figura III.4 se muestra los flujos de mensajes de alto nivel para la autenticación durante el registro. En aras de la simplificación no se muestran algunos elementos y mensajes.

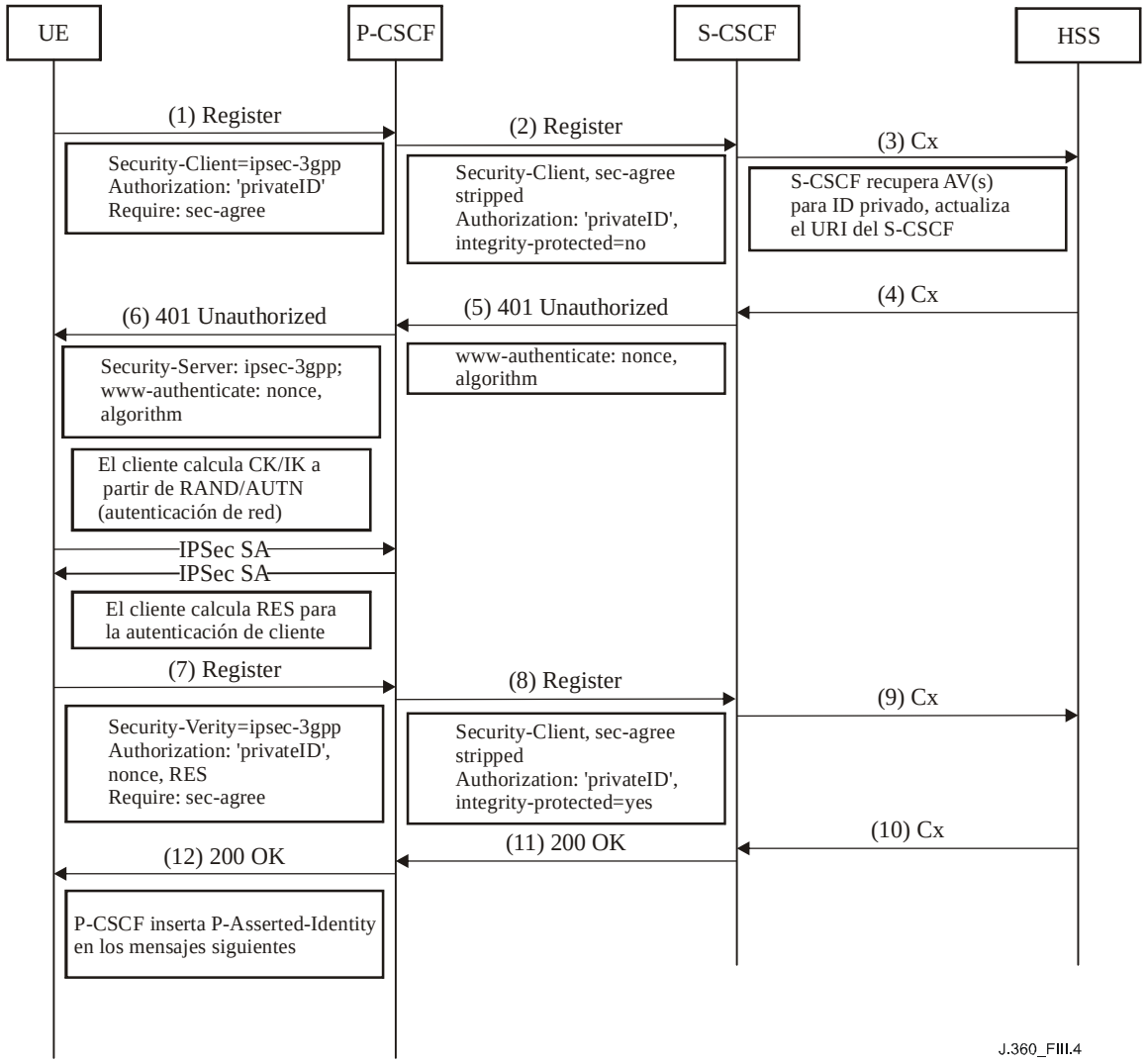


Figura III.4 – Flujos de mensajes de registro del IMS

Para la autenticación durante el registro, se realizan los pasos básicos siguientes:

1) El UE envía una petición de registro al P-CSCF. El mensaje incluye una cabecera "Security-Client" (seguridad-cliente) de [IETF RFC 3329] con los mecanismos de seguridad que soporta el UE. El IMS establece que "ipsec-3gpp" sea obligatorio. El mensaje también incluye una cabecera "authorize" (autorizar) con la identidad privada del abonado.

2) El P-CSCF retira las cabeceras del acuerdo de seguridad, inserta "integrity-protected=no" en la cabecera "Authorized" (autorizado) y retransmite la petición de registro al I-CSCF adecuado, que envía la petición al S-CSCF adecuado de la red origen del abonado.

3) El S-CSCF contacta con el HSS para actualizar el URI del S-CSCF para dicho usuario y, si es necesario, solicita uno o más vectores de autenticación.

4) El HSS devuelve uno o más vectores de autenticación si se solicita. Los vectores de autenticación proporcionan los datos necesarios para que el S-CSCF cree una cabecera de "www-authenticate" y desafíe al usuario.

5) El S-CSCF crea y envía una respuesta SIP 401 (Unauthorized), que contiene la cabecera "www-authenticate" e incluye un desafío. Esta respuesta se encamina de vuelta al P-CSCF.

6) El P-CSCF retira la clave de integridad (IK, *integrity key*) y la clave de confidencialidad (CK, *confidentiality key*) de la respuesta 401 para usar los servidores de aplicación (SA) IPSec entre el P-CSCF y el UE, y envía el resto de la respuesta al UE.

7) Cuando recibe el mensaje de desafío, el UE determina la validez del desafío de autenticación recibido. El UE establece asociaciones de seguridad con el P-CSCF utilizando la IK y la CK obtenidas de los datos enviados por el HSS, utilizando la clave compartida a largo plazo en su UICC. El UE calcula entonces una respuesta (RES) y envía una segunda petición de registro con una cabecera "Authorization" que incluye la respuesta al desafío. Este mensaje incluye cabeceras "Security-Verify" (seguridad-verificación) de acuerdo con [IETF RFC 3329].

8) El P-CSCF retira las cabeceras del acuerdo de seguridad, inserta "integrity-protected=yes" en la cabecera "authorize" (autorizar) y lo remite al I-CSCF que, a su vez, lo envía al S-CSCF pertinente.

9) El S-CSCF compara la respuesta al desafío de autenticación recibida del UE con la respuesta esperada recibida del HSS. Si concuerdan, el S-CSCF actualiza los datos del HSS utilizando la interfaz Cx.

10) El HSS proporciona al S-CSCF datos de abonado a través de la interfaz Cx, incluyendo perfiles de servicio, que contienen los criterios de filtrado iniciales.

11) El S-CSCF envía una respuesta 200 OK al UE. La respuesta 200 OK contiene una cabecera "P-Associated-URI" con la lista de identidades públicas del usuario que están asociadas a la identidad pública que se está registrando.

12) El P-CSCF envía 200 OK al UE. Debido a que el usuario se ha autenticado y existe una asociación de seguridad entre el P-CSCF y el UE, el P-CSCF inserta una cabecera "P-Asserted-Identity" en todos los mensajes subsiguientes desde dicho UE.

IPCablecom tiene requisitos destinados a soportar UE y esquemas de autenticación no considerados en la arquitectura del IMS, así como mecanismos de transporte adicionales. IPCablecom2 mejora las especificaciones del IMS en varias áreas para soportar dichos requisitos.

III.6.1.1 Descripción

La arquitectura de IPCablecom2 soporta los mecanismos de autenticación siguientes:

- IMS AKA
- Autenticación SIP Digest
- Autenticación basada en certificado

La arquitectura también debe acomodar equipos de usuario (UE) que tengan varias credenciales de autenticación. Por ejemplo, un UE puede tener un certificado para acceder a servicios mientras se encuentre en una red de cable y un UICC para acceder a servicios cuando se encuentre en una red celular.

Un abonado puede tener varias credenciales para la misma identidad privada. Un abonado puede tener varios UE cada uno con diferentes capacidades relativas a dichas credenciales. Por ejemplo, un abonado puede tener un MTA con un certificado para su uso en el hogar y un UE basado en UICC para cuando se encuentre de viaje.

III.6.1.1.1 Autenticación IMS AKA

La autenticación IMS AKA con credenciales UICC seguirá funcionando tal como se describe en las especificaciones del 3GPP.

III.6.1.1.2 Autenticación SIP Digest

IPCablecom2 soporta la autenticación SIP tal como se describe en [IETF RFC 3261]. La autenticación SIP utiliza un esquema de desafío – respuesta para la autenticación de mensajes SIP y el acceso a servicios. En este enfoque, se desafía a un usuario para que demuestre cual es su identidad, ya sea durante el registro o durante otros inicios de diálogos SIP.

La autenticación SIP de IPCablecom2 se maneja de forma similar al IMS AKA, y es conforme con [IETF RFC 3261] y con [IETF RFC 2617]. Este enfoque minimiza el impacto sobre el flujo de autenticación del IMS existente, manteniendo las cabeceras y los tiempos de ida y vuelta existentes. A diferencia de IMS AKA, los desafíos no se calculan previamente. A fin de maximizar la seguridad de la autenticación SIP Digest, se utilizan directivas "auth-int" "cnonces" y "qop", que requieren que el S-CSCF calcule los desafíos en tiempo real.

En la figura III.5 se muestra el flujo de mensajes de la autenticación basada en SIP durante un registro.

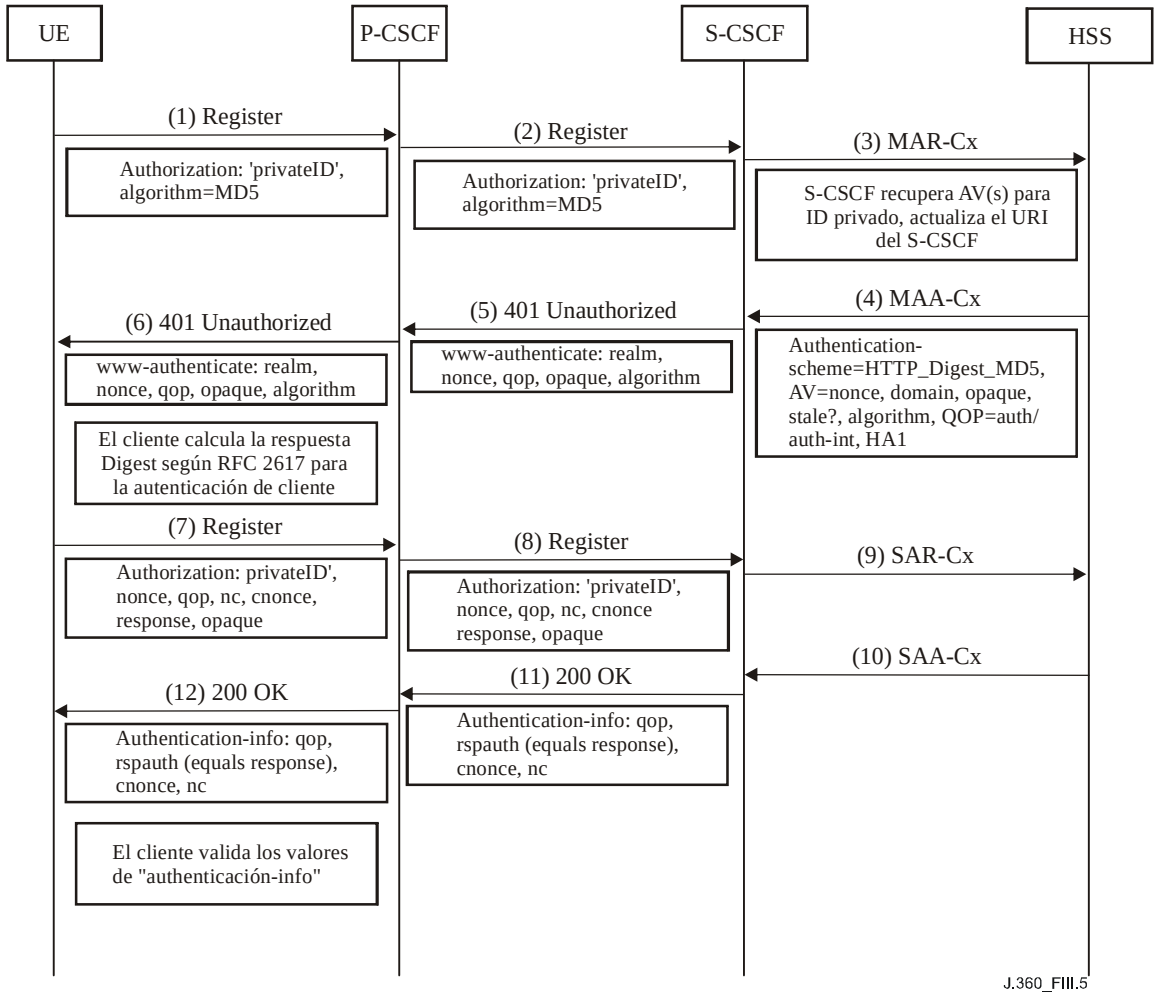


Figura III.5 – Autenticación SIP Digest

Para la autenticación SIP Digest durante el registro, tienen lugar los pasos básicos siguientes. Por simplicidad, no se muestra el contenido de las cabeceras [IETF RFC 3329] y de otras cabeceras SIP.

1) El UE envía una petición de registro al P-CSCF. El mensaje incluye una cabecera "Authorization" (autorización) que incluye la identidad privada del abonado. A continuación se muestra un ejemplo de dicha cabecera:

```
REGISTER sip:home.atlanta.com SIP/2.0
Authorization: Digest username="alice_private@atlanta.com",
      realm=" atlanta.com", nonce="", uri="sip:home.atlanta.com",
      response="", algorithm="MD5"
```

IPCablecom añade el parámetro "algorithm" al mensaje de registro IMS inicial a fin de informar a la red del tipo de desafío a crear. Ello permite soportar varios tipos de credenciales por cada usuario.

2) El P-CSCF retransmite la petición del registro al I-CSCF apropiado, que envía la petición al S-CSCF de la red origen del abonado.

3) El S-CSCF contacta con el HSS utilizando una instrucción MAR dirigida al HSS sobre la interfaz Cx. El mensaje MAR incluye la identidad privada del abonado, la información del S-CSCF y el número de vectores de autenticación solicitados. El HSS utiliza esta información para actualizar el URI del S-CSCF para la identidad privada y entregar la información correcta del vector de autenticación al S-CSCF.

4) El HSS devuelve un mensaje MAA sobre la interfaz Cx. El mensaje MAA incluye las identidades públicas y los vectores de autenticación para dicho abonado. En una cláusula posterior se detallan el contenido del vector de autenticación para SIP Digest. Las principales diferencias son la falta de CK e IK, y el contenido del elemento de datos autenticación SIP (SIP-Authenticate). En lugar de los datos AKA, la pareja de valores de atributos AVP (Attribute-Value-Pair) de autenticación SIP (SIP-Authenticate) contiene los datos que requiere el S-CSCF para calcular una respuesta Digest, básicamente HA1.

5) El S-CSCF crea una respuesta SIP 401 (Unauthorized), que incluye un desafío en el campo cabecera "www-authenticate" (autenticación www) y en otros campos [IETF RFC 3261]. A continuación se muestra un ejemplo de cabecera:

```
SIP/2.0 401 Unauthorized
      WWW-Authenticate: Digest realm="atlanta.com",
        nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
        qop=auth,auth-int, opaque="5ccc069c403ebaf9f0171e9517f40e41",
              algorithm="MD5"
```

En una cláusula posterior se incluye información sobre la creación de "nonce" (palabra singular). En función de la política local, el servidor devuelve los parámetros qop entre los que debe elegir el cliente.

6) Esta respuesta de encamina de vuelta al P-CSCF, y de allí al UE.

7) Una vez que el UE recibe el desafío, éste calcula la respuesta en base a elementos presentes en la cabecera WWW-Authenticate y en otros elementos adicionales (por ejemplo, cnonce) generados por el UE. Los valores de la cabecera "Authorize" se calculan según [IETF RFC 3261] y [IETF RFC 2617]. El valor "qop" se selecciona de entre los que proporciona el S-CSCF. Los valores de "Cnonce" se calculan tal como se describe en una cláusula posterior. El UE envía una segunda petición de registro con la cabecera "Authorization". A continuación se muestra un ejemplo de cabecera "Authorization":

```
REGISTER sip:home.atlanta.com SIP/2.0
      Authorization: Digest
              username="alice_private@atlanta.com", realm="atlanta.com",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              uri="sip:home.atlanta.com", qop=auth-int, nc=00000001,
              cnonce="0a4f113b",
              response="6629fae49393a05397450978507c4ef1",
              opaque="5ccc069c403ebaf9f0171e9517f40e41", algorithm="MD5"
```

8) El P-CSCF retransmite el mensaje al I-CSCF adecuado que, a su vez, lo envía al S-CSCF pertinente.

9) Cuando recibe el segundo registro del UE, el S-CSCF calcula el desafío igual que el UE, a fin de comparar los dos resultados y autenticar al abonado. Utilizando parámetros del HSS tales como HA1, y los parámetros procedentes de la cabecera "Authorization" tal como "cnonce", el S-CSCF calcula la respuesta del desafío según [IETF RFC 3261] e [IETF RFC 2617]. El cálculo se hace de una forma consistente con el parámetro "qop" enviado por el UE.

   Si los dos resultados del desafío son idénticos, el S-CSCF realiza un procedimiento SAR sobre la interfaz Cx, informando al HSS que el usuario está registrado y solicitando el perfil de usuario.

10) El HSS devuelve un mensaje SAA al S-CSCF que contiene el perfil de usuario, y que incluye, entre otras cosas, el conjunto de todas las identidades de usuario públicas asignadas para la autenticación de la identidad de usuario privada, así como los criterios de filtrado iniciales.

11) El S-CSCF envía una respuesta 200 OK a la petición de registro. La respuesta incluye una cabecera "Authentication-Info" (información de autenticación), que permite al UE autenticar la red o el S-CSCF. El valor "rspauth" se calcula según [IETF RFC 2617]. La cabecera también incluye un valor de "nextnonce". El mensaje 200 OK se envía al UE. A continuación se muestra un ejemplo de cabecera "Authentication-Info":

```
SIP/2.0 200 OK
        Authentication-Info:
        qop=auth-int, rspauth="7729fae49393a05397450978507c4ef1",
        cnonce="0a4f113b",nc=00000001,
        nextnonce="8829fae49393a05397450978507c4ef1"
```

12) La respuesta 200 OK se encamina al P-CSCF adecuado y desde allí al UE.

13) El UE valida el valor de "rspauth" para autenticar la red o el S-CSCF.

Debido a que el usuario ya ha sido autenticado y existe una asociación de seguridad entre el P-CSCF y el UE, el P-CSCF inserta una cabecera "P-Asserted-Identity" en todos los mensajes subsiguientes procedentes de dicho UE.

El hecho de añadir la capacidad de soportar SIP Digest afecta a las especificaciones del IMS de la forma siguiente:

- Se permite que existan nuevos algoritmos Digest (resumen) en las cabeceras "www-authenticate" y "Authorization".
- El HSS debe calcular y almacenar los nuevos tipos de respuestas Digest.
- Los UE deben poder soportar y calcular nuevos tipos de respuestas Digest.
- La red de origen (o S-CSCF) autentica al UE incluyendo una cabecera "Authentication-Info" en la respuesta 2xx después de una autenticación exitosa del UE.

En la cláusula III.6.1.2 se analizan los efectos sobre componentes concretos.

III.6.1.1.3 Autenticación basada en certificados

La autenticación basada en certificados queda fuera del alcance de esta versión del apéndice.

III.6.1.2 Componentes afectados

En las cláusulas siguientes se describen los efectos en los componentes del IMS a fin de acomodar los requisitos de autenticación IPCablecom.

III.6.1.2.1 UE

A fin de soportar nuevas formas de autenticación, los UE de IPCablecom deben enviar el parámetro "algorithm" adecuado en las peticiones de registro.

Los UE de IPCablecom que soportan la autenticación Digest deben ser conformes con [IETF RFC 3261], y por tanto con [IETF RFC 2617]. Los UE deben enviar el parámetro "algorithm" con el valor del algoritmo Digest adecuado en la petición de registro inicial. Cuando se recibe un desafío desde el S-CSCF en un mensaje 401 Unauthorized, los UE deben crear una cabecera "Authorization" que incluya una respuesta a desafío, tal como se describe en [IETF RFC 2617] basada en el parámetro algoritmo incluido en la cabecera "www-Authenticate". Los parámetros "Cnonce" y "nc" deben estar incluidos en la respuesta al desafío. El parámetro "cnonce" debe tener 32 octetos codificados en ASCII hexadecimal, tal como se indica en [IETF RFC 2617], de conformidad con las directrices de [IETF RFC 1750]. El valor de "qop" utilizado en los cálculos de respuesta y devueltos en la cabecera "Authorization" debe ser uno de los valores recibidos en la cabecera 401 "www-Authenticate" del S-CSCF. Los UE deben poder validar los valores de la cabecera "Authentication-Info" que devuelve el S-CSCF con el mensaje 200 OK.

Los UE deben poder almacenar de forma segura nombres de usuario y contraseñas minimizando el riesgo. Los UE pueden, opcionalmente, pedir que los usuarios introduzcan el nombre de usuario y la contraseña.

III.6.1.2.2 S-CSCF

Con el objetivo de soportar nuevas formas de autenticación, el S-CSCF debe entender los nuevos valores del parámetro "algorithm" incluidos en las cabeceras "Authorization" enviadas por los UE. Dicho valor debe utilizarse para la AVP "Authentication-Scheme" (esquema de autenticación) en los procedimientos Cx.

Para soportar SIP Digest, el S-CSCF debe poder calcular respuestas Digest tal como se describe en [IETF RFC 3261] e [IETF RFC 2617]. El S-CSCF recibirá un HA1 del HSS sobre la interfaz Cx, y debe utilizar dicho valor HA1 para crear la respuesta digest (resumen) correspondiente a esta identidad privada. Esta respuesta se compara con la respuesta recibida por el UE, que debe calcularse de la misma forma. El valor de "qop" recibido del UE debe utilizarse para calcula la respuesta. Si la respuesta calculada por el S-CSCF es idéntica a la respuesta recibida del UE, el S-CSCF envía un mensaje 200 OK que incluye la cabecera "Authentication-Info" según [IETF RFC 2617]. El parámetro "nextnonce" debe utilizarse en la cabecera "Authentication-Info".

Debido a que la seguridad de Digest depende en gran medida del cálculo del parámetro "nonce", el S-CSCF debe seguir las directrices siguientes relativas a la creación y utilización de "nonce":

- El parámetro "nonce" debe tener 32 octetos codificados en hexadecimal ASCII según [IETF RFC 2617].
- "Nonce" debe generarse de acuerdo al procedimiento de generación de número pseudoaleatorio de [IETF RFC 1750].
- "Nextnonce" siempre se envía en respuestas "Authentication-Info" (por ejemplo, respuestas 2xx) para la autenticación exitosa del UE.

En función de la política local, el S-CSCF debería:

- Aceptar un "nonce" que haya sido previamente utilizado con un cómputo de "nonce" (nonce-count) válido, por ejemplo, para permitir PRACK u otros tipos de peticiones recibidas antes de una respuesta 2xx.
- Aceptar un "nonce" previamente utilizado sólo durante un periodo de tiempo especificado. Se recomienda que dicho tiempo sea de 10 minutos o menos.
- Aceptar un "nonce" previamente utilizado sólo un número especificado de veces. Se recomienda que sean 5 veces o menos.
- Aceptar un "nonce" antiguo en base a las reglas de política anteriores, aunque se haya enviado "nextnonce".

Las reglas de política anteriores están principalmente relacionadas con el caso en que se ha deshabilitado la seguridad de señalización en la red.

III.6.1.2.3 HSS

A fin de soportar nuevos esquemas de autenticación, la interfaz y procedimientos Cx deben ser ampliados. La autenticación Digest añade nuevos parámetros a la interfaz Cx, específicamente la AVP "SIP-Auth-Data-Item" presente en los procedimientos MAR y MAA. El vector de autenticación proporciona al S-CSCF el HA1 y otros elementos que le permiten calcular respuestas. Para más información, véase el apéndice IV.

III.6.1.3 Seguridad de la señalización

El IMS define IPsec para que la señalización sea segura entre los UE y los intermediarios del borde. UICC proporciona credenciales para la autenticación e IPsec. El mecanismo de seguridad se negocia utilizando el acuerdo de seguridad SIP [IETF RFC 3329]. Sin embargo, el único mecanismo permitido para la negociación en IMS es ipsec-3gpp.

IPCablecom2 añade TLS como una opción para la seguridad de la señalización entre el UE y el P-CSCF. La utilización del TLS por el UE es opcional y se basa en que ofrece las ventajas siguientes:

- TLS es el mecanismo de seguridad recomendado especificado en [IETF RFC 3261].
- Existe una tendencia general a la utilización de TCP para un mejor manejo de mensajes más largos.
- TLS soporta el tránsito de NAT en la capa del protocolo.
- TLS está implementado al nivel de aplicación en lugar de al nivel de núcleo (kernel). Ello proporciona algunas ventajas, como que se soporte más fácilmente en diversos entornos.

El hecho de soportar TLS para la señalización, lleva a considerar las credenciales TLS.

- TLS mutuamente autenticado – El UE y el servidor proporcionan certificados cuando se establece la seguridad de la señalización. El servidor debe validar el certificado del UE y el UE debe validar el certificado del servidor. La autenticación mutua proporciona un elevado grado de seguridad.
- Autenticación desde el lado del servidor– Solo el servidor proporciona un certificado al establecerse la seguridad de la señalización. Este enfoque evita la carga computacional extra propia de la aplicación de un sistema PKI en el UE. Proporciona un nivel medio de seguridad, con menores exigencias sobre la CPU del UE. Puede ser utilizado para asegurar sesiones HTTP Digest.

Ambos modelos requieren que el P-CSCF y el UE soporten las funcionalidades de los sistemas PKI, tales como validación de certificado y gestión de certificados.

El hecho de que se soporte TLS lleva también considerar las asignaciones de puertos TLS y la gestión de la conexión TLS. IPCablecom2 utilizará los puertos SIP normalizados para UDP, TCP y TLS. Los UE que negocian el TLS opcional antes de la mensajería SIP, se conectan al puerto SIPS 5061. En cualquier otro caso, los UE utilizan el puerto normalizado UDP/TCP SIP 5060. Las peticiones y las respuestas se realizan de acuerdo con los procedimientos descritos en [ID SIP-OUTBOUN].

IPCablecom2 soporta una sesión TLS opcional previa a la señalización SIP siempre que el UE y el P-CSCF la soporten. Ello proporciona seguridad al mensaje de registro inicial. Las cabeceras [IETF RFC 3329] se utilizan durante el proceso de registro con el fin de proporcionar seguridad contra ataques por reducción de opciones de autenticación y mantener la coherencia con el flujo de mensajes de registro IMS existente.

La figura III.6 muestra la negociación de la seguridad de señalización durante un diálogo de registro exitoso. Por simplicidad, sólo se muestran las cabeceras de seguridad de la señalización.

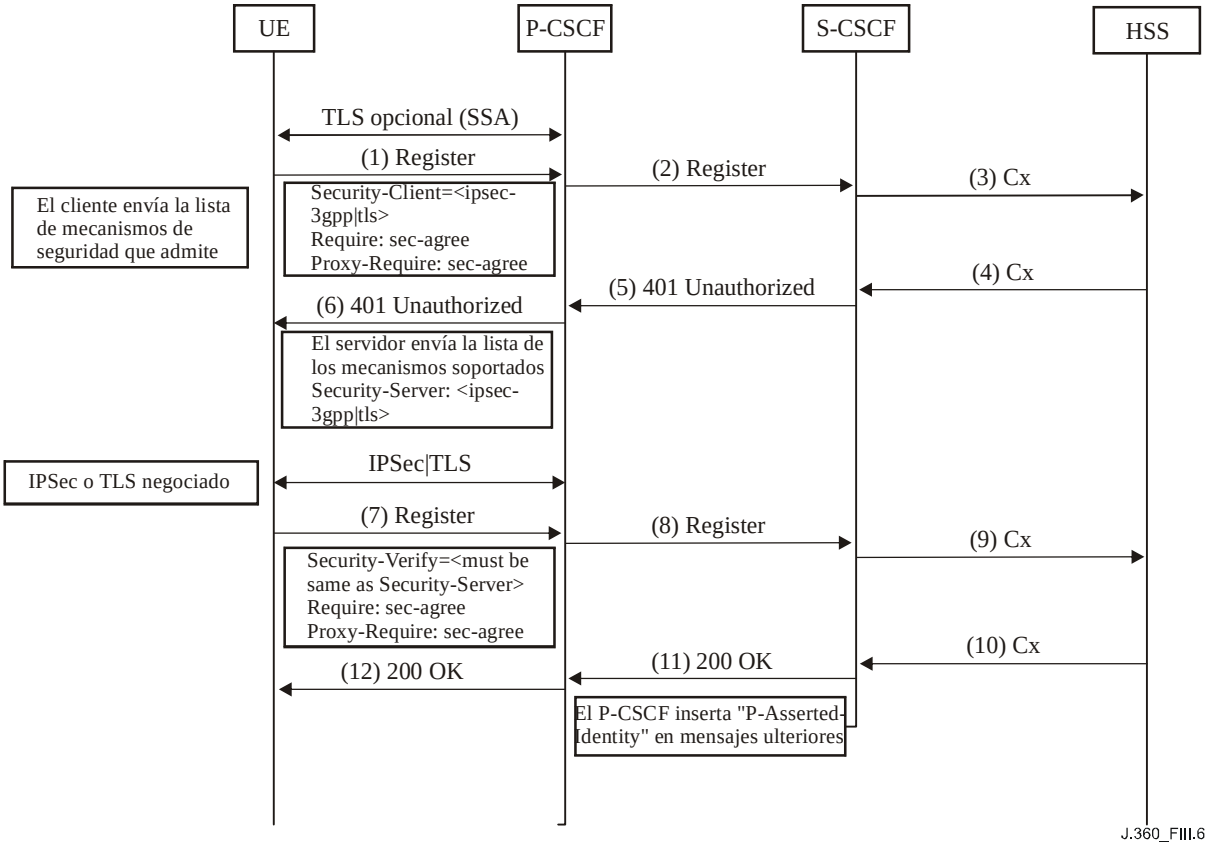


Figura III.6 – Seguridad en el transporte

Para que TLS pueda utilizarse para la seguridad de la señalización entre el UE y el P-CSCF, han de mejorarse las especificaciones del IMS para permitir que TLS sea un mecanismo de seguridad SIP adicional que pueda ser negociado. En [IETF RFC 3329] TLS es un mecanismo de seguridad que puede ser negociado, por lo que el único cambio afecta a las especificaciones del IMS.

Tal como se muestra, los UE que soportan TLS pueden negociar un TLS autenticado en el lado del servidor antes de iniciar los mensajes SIP, por ejemplo, cuando un usuario requiere privacidad. Las cabeceras [IETF RFC 3329] se utilizan para negociar la seguridad de señalización utilizada durante el registro SIP a fin de proteger contra ataques por reducción de opciones de autenticación (*bid-down*), y mantener la coherencia con los flujos de mensajes del IMS.

A alto nivel, los efectos sobre los componentes del IMS son los siguientes:

- el UE debe soportar la capacidad de negociar TLS utilizando [IETF RFC 3329];
- el UE puede establecer TLS antes de los mensajes SIP;
- el P-CSCF debe soportar la capacidad de negociar TLS utilizando [IETF RFC 3329];
- el P-CSCF puede soportar TLS antes de los mensajes SIP.

III.6.1.3.1 Componentes afectados

En las cláusulas siguientes se describe el impacto en los componentes del IMS a fin de poder negociar la seguridad de la señalización.

III.6.1.3.1.1 Equipo de usuario (UE)

A fin de soportar la negociación de la seguridad de la señalización, los UE de IPCablecom deben soportar TLS tal como se define en [IETF RFC 2246].

Los UE deben soportar la construcción e interpretación de cabeceras [IETF RFC 3329] que contienen el nombre de mecanismo ("mechanism-name") "tls".

III.6.1.3.1.2 P-CSCF

El P-CSCF debe ser capaz de establecer sesiones TLS basadas en la petición de un UE. El P-CSCF siempre debería solicitar los certificados del UE, pero si no recibe ninguno, debería establecer TLS autenticado desde lado del servidor. Si se establece TLS mutuamente autenticado, el P-CSCF debe fijar integrity-protected=yes en las cabeceras "Authorization". Si no se establece TLS mutuamente autenticado, el P-CSCF fija integrity-protected=no. Estas reglas son adicionales a las reglas existentes relativas al establecimiento de IPSec. Si bien TLS autenticado desde lado servidor proporciona integridad, el TLS mutuamente autenticado es más parecido al caso del 3GPP que utiliza IPSec combinado con AKA.

El P-CSCF debe soportar el nombre de mecanismo ("mechanism-name") "tls" de [IETF RFC 3329]. Éste puede negociarse como TLS mutuamente autenticado o como autenticado desde lado servidor, en función de las capacidades del UE. Se aplican las mismas reglas para la asignación de valores con integridad protegida que las anteriormente mencionadas.

Los certificados deberían validarse de conformidad con [IETF RFC 3280].

III.6.1.3.1.3 S-CSCF

El S-CSCF puede desafiar cualquier mensaje SIP. Los mensajes que contienen cabeceras "Authorize" con integridad protegida fijada en "no" siempre deberías ser desafiados, ya que dicha bandera indica falta de seguridad de señalización entre el UE y el P-CSCF en peticiones de registro no iniciales. Si el S-CSCF desafía exitosamente a un abonado, el S-CSCF debe insertar la cabecera "P-Asserted-Identity" en los mensajes subsiguientes procedentes de dicho abonado en caso de que dicha cabecera no estuviera ya incluida en los mismos.

III.6.1.3.2 Inhabilitación de la seguridad de señalización

Aunque no se recomienda, la seguridad de señalización puede ser inhabilitada en el P-CSCF. Al inhabilitar la seguridad de la señalización, los UE y la red quedan expuestos a muchas de las amenazas descritas en la cláusula III.5.3, especialmente cuando ello se combina con una forma más débil de autenticación, como SIP Digest.

El apéndice I de señalización SIP de IPCablecom2 y la especificación complementaria de IPCablecom2 [UIT-T J.366.4] contienen información detallada sobre los procedimientos para inhabilitar la seguridad de señalización. La mayor diferencia en los procedimientos cuando se inhabilita la seguridad de señalización es que las peticiones de diálogo no registrado deberían ser desafiadas.

III.6.2 Confirmación de la identidad

Los entornos IPCablecom requieren que los elementos de red confiables transporten de alguna forma la identidad de los abonados a otros elementos o servicios, y puedan eliminar la identidad cuando se comuniquen con redes no confiables. La confirmación de la identidad es el mecanismo por el que los elementos y servicios pueden confiar en la identidad de un usuario.

Tal como se describe en [UIT-T J.366.4], el IMS asigna la tarea de confirmación de la identidad a las P-CSCF para todos los mensajes SIP, en base al flujo estricto descrito en la cláusula III.6.1. Una vez que se establecen las asociaciones de seguridad (SA, *security associations*) IPSec y el abonado se autentica, el P-CSCF confirma la identidad del mismo. Supervisando los mensajes SIP dirigidos al UE, el P-CSCF observa el mensaje 200 OK desde el S-CSCF de los abonados. Esta información, más la presencia de las asociaciones de seguridad con el UE permiten que el P-CSCF haga una autenticación exitosa del UE.

IPCablecom2 mejora el IMS con los requisitos siguientes:

- Un P-CSCF que tenga establecida una sesión TLS con un UE y que observe una respuesta 200 OK desde el S-CSCF dirigida a dicho abonado, puede confirmar la identidad de la identidad pública utilizada por el UE.
- Un P-CSCF que no tenga establecida una sesión TLS y que observe una respuesta 200 OK desde el S-CSCF del UE durante la autenticación SIP, no puede confirmar la identidad de dicho UE. En este caso, el S-CSCF confirma la identidad después de la autenticación exitosa del abonado.

III.6.3 Seguridad del tránsito de un NAT

En las cláusulas siguientes se describe la seguridad STUN y TURN.

III.6.3.1 STUN

El protocolo STUN [IETF RFC 3489] define las contramedidas a los ataques descritos en la cláusula III.5.3.2.2. Ello incluye recomendaciones sobre la arquitectura de red así como mecanismos para la integridad de los mensajes que proporciona STUN. Para esta versión del apéndice no se proponen mecanismos adicionales.

III.6.3.2 TURN

El servidor TURN representa un recurso de red utilizado durante una conexión por lo que su seguridad es importante.

El protocolo TURN [ID TURN] define las contramedidas a los ataques descritos en la cláusula III.5.3.2.3. Ello incluye recomendaciones sobre la arquitectura de red así como mecanismos para la integridad de los mensajes que proporciona TURN. No se proponen mecanismos adicionales.

NOTA – La seguridad de TURN está siendo actualizada. Se dispondrá de información adicional tan pronto como esté disponible el proyecto de texto sobre TURN.

III.6.4 Seguridad de la configuración

III.6.4.1 Arquitectura genérica de arranque

La infraestructura de autenticación del 3GPP tiene la virtud de permitir que las funciones de aplicaciones en el lado de red y en el lado del usuario establezcan claves compartidas. En este sentido, el 3GPP diseñó el "arranque de la seguridad de las aplicaciones " para autenticar al abonado definiendo una arquitectura genérica de arranque (GBA, *generic bootstrapping architecture*) basada en el protocolo AKA. En la figura III.7 se muestran los componentes y puntos de referencia de la GBA.

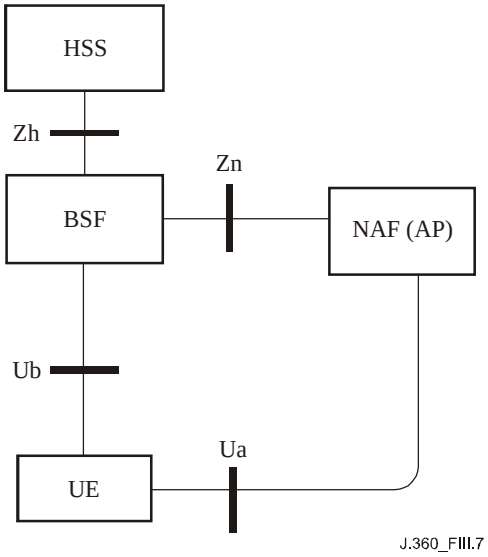


Figura III.7 – Componentes y puntos de referencia de la GBA

El IMS describe actualmente la arquitectura genérica de arranque (GBA) basada en el protocolo AKA. Esta arquitectura establece cómo un UE se arranca con un servidor para recibir información de configuración y para obtener claves que pueden utilizar tanto el UE como los servidores de aplicación a fin de que las comunicaciones sobre la interfaz Ua sean seguras.

De conformidad con [UIT-T J.366.9], una función de arranque de servidor (BSF, *bootstrapping server function*) y un UE se autenticarán mutuamente utilizando un protocolo AKA y llegarán a un acuerdo sobre las claves de sesión posteriormente utilizadas entre el UA y la función de aplicación de red (NAF, *network application function*). A tal fin, la BSF adquiere los valores de seguridad de usuario GBA (GUSS, *GBA user security settings*) del HSS y restringe la aplicabilidad de las claves a NAF específicas utilizando un procedimiento de obtención de claves. Tal como se describe en [UIT-T J.366.9], el IMS utiliza el GBA para autenticar y recibir información de configuración mediante IPsec. El IMS requiere un ISIM basado en UICC para este proceso, ya que utiliza el IMS AKA para la autenticación e IPsec para el transporte.

Dado que IPCablecom2 amplía el IMS para soportar escenarios de despliegue no basados en UICC, el protocolo AKA no puede ser utilizado por todos los clientes de IPCablecom para conseguir una autenticación mutua entre el UE y la BSF. En consecuencia, es necesario un nuevo procedimiento. IPCablecom añade una opción para que la interfaz Ub pueda soportar HTTP Digest sobre TLS para la autenticación y obtención de clave GBA.

Obsérvese que en IPCablecom2, la NAF es un servidor XCAP que proporciona la configuración al UE.

En el caso de UEs que no soporten IPsec ni AKA, en el momento en que el UE comience la comunicación con la NAF, debe establecer un túnel TLS con ella. La NAF se autentica con el UE mediante un certificado de clave pública. El UE debe verificar que el certificado del servidor se corresponde con la FQDN de la NAF con la que estableció el túnel. La autenticación del UE no se lleva a cabo como parte del TLS (es decir, no es necesario un certificado del UE). Las interfaces Zh, Zn y Ua son interfaces normalizadas definidas en [UIT-T J.366.9].

La interfaz Ub utiliza el mecanismo HTTP Digest para establecer las credenciales (por ejemplo, la clave o claves de la sesión) entre el UE y la BSF.

En la figura III.8 se ilustra el nuevo intercambio de arranque sobre la interfaz Ub.

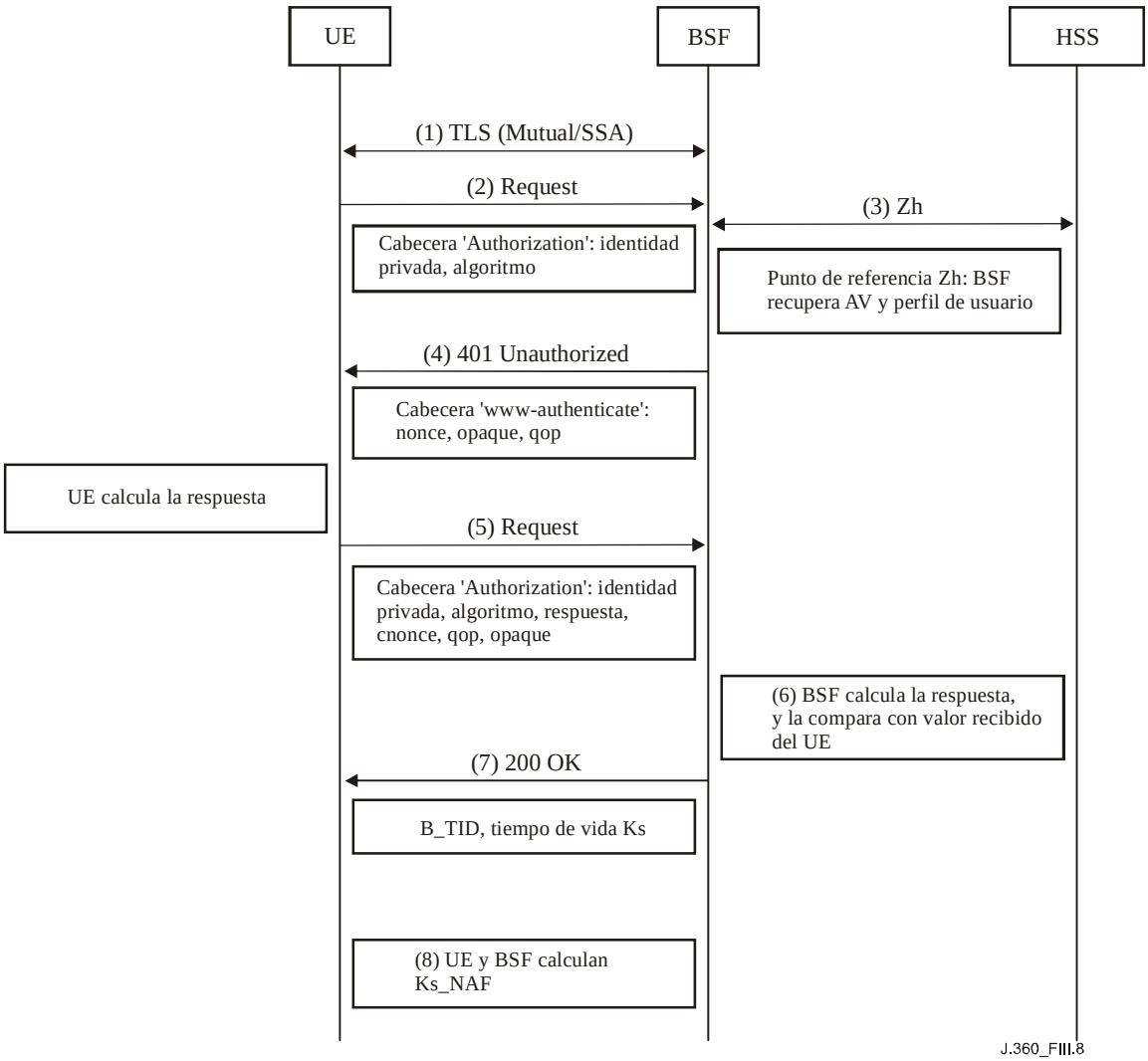


Figura III.8 – Flujos de mensajes GAB

Los pasos siguientes describen el procedimiento de arranque para HTTP Digest sobre TLS.

1) El UE comienza el procedimiento de arranque iniciando una sesión TLS con la BSF. El UE y la BSF negocian el TLS autenticado por el lado del servidor. El UE autentica la BSF con el certificado que presenta la BSF. Ésta no requiere la autenticación del UE en este momento.

2) El UE inicia el procedimiento de arranque enviando un mensaje HTTP Request (petición) a la BSF incluyendo la identidad privada en una cabecera "Authorization". El UE indica el algoritmo que soporta en el parámetro "algorithm" de la cabecera "Authorization".

3) La BSF envía una instrucción MAR al HSS a fin de obtener un vector de autenticación para dicho usuario. El HSS responde con el vector de autenticación adecuado para dicho usuario y algoritmo en un mensaje MAA. El contenido del vector de autenticación se mejora tal como se hace en SIP Digest para permitir que la BSF calcule un desafío al UE tal como se describe en [IETF RFC 2617].

   NOTA 1 – En un entorno con varios HSS, la BSF puede obtener la dirección del HSS en el que se ha almacenado la suscripción del usuario consultando a la SLF antes del paso 3.

4) La BSF responde a la petición del UE con un mensaje 401 Unauthorized que contiene una cabecera "www-authenticate" para forzar que el UE se autentique. La cabecera "www-authenticate" incluye un "nonce", creado de conformidad con las directrices descritas anteriormente en este apéndice (es decir, 32 octetos codificados en hexadecimal ASCII). El parámetro "algorithm" informa al UE del algoritmo que debería utilizar para calcular su respuesta.

5) Cuando recibe el desafío, el UE utiliza los datos recibidos en la cabecera "www-authenticate" para crear una segunda petición HTTP (HTTP Request) con la respuesta al desafío en una cabecera "Authorization". La respuesta al desafío se calcula según [IETF RFC 2617]. Debe incluirse un "cnonce". El UE debe seleccionar un valor de "qop" de la lista de valores de "qop" enviados por la BSF. El mensaje se envía a la BSF sobre la sesión TLS.

6) La BSF verifica la validez de la respuesta al desafío que envía el UE calculando por sí misma la respuesta y comparando los valores. La BSF calcula la respuesta según [IETF RFC 2617]. Utiliza el valor HA1 que suministra el HSS sobre el punto de referencia Zh.

7) Si la respuesta al desafío que envía el UE es idéntica a la respuesta calculada por la BSF, ésta debe enviar un mensaje 200 OK incluyendo la B-TID al UE para indicar autenticación exitosa. Además, la BSF suministrará la duración de la clave Ks en un mensaje 200 OK.

   El valor B-TID debe generarse en el formato de NAI tomando el valor de "nonce" codificado en base64 del paso 4 y el nombre del servidor BSF, es decir, base64encode(nonce)@BSF_servers_domain_name.

   NOTA 2 – Antes de codificar el "nonce" obtenido del paso 4 en base64, dicho "nonce" debe convertirse de un valor hexadecimal codificado en ASCII a un valor codificado en binario.

8) El UE y la BSF deben utilizar el secreto maestro de TLS de la sesión TLS existente para Ks. Tanto el UE como la BSF deben utilizar Ks para obtener Ks_NAF. Dicho Ks_NAF debe utilizarse para que el punto de referencia Ua sea seguro.

   Ks_NAF se calcula como Ks_NAF=KDF(Ks, "gba-h", RAND, IMPI, NAF_Id) donde KDF es la función de obtención de clave descrita en el anexo B de [UIT-T J.366.9]. El parámetro "nonce" codificado en binario se sustituye por la variable RAND basada en AKA cuando se calcula Ks_NAF. Ks es el secreto maestro de la sesión TLS existente.

   El UE y la BSF deben almacenar la clave Ks con el B-TID asociado para su utilización ulterior, hasta que haya expirado la vida de Ks, o hasta que se actualice la clave.

   La clave Ks se utiliza para obtener claves para comunicaciones con servidores de aplicación, tales como el elemento de provisión, activación y configuración (PAC), utilizando el punto de referencia Ua.

III.6.4.2 Descarga segura del software

La descarga segura del software está fuera del ámbito de esta versión del apéndice.

III.6.5 Seguridad de los medios

La seguridad de los medios está fuera del ámbito de esta versión del apéndice.

III.6.6 Utilización de TLS para la seguridad dentro del dominio

Tal como se define en la especificación complementaria al IMS [UIT-T J.366.8], el punto de referencia Zb conecta de forma segura los componentes del IMS del mismo dominio de confianza. La implementación de la interfaz Zb es opcional. Si se implementa, la interfaz Zb debe utilizar IPsec ESP para la autenticación e integridad. La confidencialidad (encriptación) es opcional.

IPCablecom2 añade el soporte de TLS para la seguridad interna a un dominio por los motivos siguientes:

- TLS es el mecanismo de seguridad recomendado especificado en [IETF RFC 3261].
- TLS soporta el tránsito de NAT en la capa de protocolo.
- TLS se implementa en el nivel de aplicación en lugar del nivel núcleo (kernel), lo cual proporciona algunas ventajas, como es un soporte mucho más fácil en numerosos entornos.

Los componentes de IPCablecom2 con interfaces SIP se requieren a fin de soportar TLS para la seguridad dentro de un dominio, además del IPsec del IMS.

Salvo que se especifique en esta cláusula, las interfaces SIP que requieren TLS DEBEN ser conformes con la especificación de TLS [IETF RFC 2246] y con cualquiera de los requisitos especificados en [IETF RFC 3261] relativos a su utilización en SIP.

TLS [IETF RFC 2246] soporta la negociación y utilización de métodos de compresión. Sin embargo, ya que dichos métodos no están especificados en la [IETF RFC 2246] sobre TLS, la compresión NO DEBE utilizarse.

III.6.6.1 Algoritmos de autenticación TLS

El algoritmo HMAC-SHA-1 (con clave de 160 bis) ha de soportarse para proporcionar la autenticación del origen de los datos y los servicios de integridad de datos en TLS. No se requiere AES-XCBC.

III.6.6.2 Algoritmos de intercambio de claves para TLS

Los siguientes son los requisitos relativos a los métodos para intercambio de claves en el protocolo TLS:

- Debe soportarse Rivest Shamir Adleman (RSA).
- Debe soportarse Diffie Hellman (DH).

III.6.6.3 Utilización de certificados X.509 en TLS

Los certificados X.509 se utilizan para la autenticación en TLS, debiendo estar todos los certificados X.509 firmados por una parte confiable. Pueden utilizarse certificados autofirmados.

III.6.6.4 Generador de número aleatorio para TLS

Las implementaciones de generación de números aleatorios tienden a ser una debilidad del sistema. Muchos fabricantes de semiconductores están añadiendo generadores de números pseudoaleatorios seguros a sus circuitos integrados que, cuando existan, deberían utilizarse. Si no hay disponible una solución basada en hardware, puede utilizarse opcionalmente un generador fuerte de números pseudoleatorios a fin de respetar la conformidad con [IETF RFC 1750].

Los siguientes son requisitos relativos a la generación de números pseudoaleatorios:

- Puede soportarse un generador de números pseudoaleatorios basado en hardware.
- Si no se dispone de un generador de números pseudoaleatorios basado en hardware debe soportarse un generador de números pseudoaleatorios basado en software.

III.6.6.5 Algoritmos de encriptación TLS

Los siguientes son los requisitos del cliente TLS y del servidor TLS relacionados con algoritmos criptográficos para proporcionar servicios de encriptación para TLS-SA:

- Debe soportarse 3DES en modo CBC (con tres claves independientes de 56 bits).
- Debe soportarse AES CBC (con clave de 128 bits).
- Puede soportarse la encriptación nula.

III.6.6.6 Conjuntos de cifrado para TLS

TLS especifica varios conjuntos de cifrado (*ciphersuites*) para su utilización en el protocolo TLS, tal como se analiza con detalle en [IETF RFC 3268]. Los conjuntos de cifrado representan las combinaciones recomendadas para la autenticación de la encriptación y el intercambio de claves a utilizar en TLS.

Los requisitos relativos a los conjuntos de cifrado son los siguientes:

- Puede soportarse "TLS_RSA_WITH_NULL_SHA".
- Debería soportarse "TLS_RSA_WITH_3DES_EDE_CBC_SHA".
- Debe soportarse "TLS_RSA_WITH_AES_128_CBC_SHA".
- Debería soportarse "TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA".
- Debe soportarse "TLS_DH_RSA_WITH_AES_128_CBC_SHA".

III.6.6.7 Autenticación TLS

TLS permite la autenticación unidireccional, en la que sólo el servidor se autentica al cliente, o la bidireccional, en la que cliente y servidor se autentican mutuamente. La autenticación unidireccional es el método habitualmente utilizado en la internet pública; sin embargo, para la señalización de red y el control de aplicaciones, la autenticación bidireccional es obligatoria para que ambas partes sepan que se están comunicando con el punto extremo deseado.

Los requisitos siguientes están relacionados con la autenticación TLS:

- debe soportarse la autenticación bidireccional para aplicaciones TLS.

III.6.7 Validación de certificado

[IETF RFC 3280] debería ser utilizada como directriz para la validación de certificados.

III.6.8 Revocación de certificado

La revocación de certificados queda fuera del alcance es esta versión del apéndice.

Apéndice IV

Visión general del servidor de abonado de la red de origen en IPCablecom2 (HSS, *home subscriber server*)

(Este apéndice no es parte integrante de esta Recomendación)

Queda en estudio.

Apéndice V

Visión general del tránsito del NAT y de la barrera contrafuego en IPCablecom2

(Este apéndice no es parte integrante de esta Recomendación)

V.1 Introducción

En este apéndice se presenta una visión general sobre cómo la arquitectura de IPCablecom2 y los UE asociados permiten el tránsito a través de dispositivos NA(P)T y de barreras contrafuegos (a los que habitualmente se hace referencia como NAT) de flujos de medios y de señalización así como de provisión y gestión. Para ayudar al lector a entender el enfoque y las metodologías de tránsito del NAT de IPCablecom2, en este apéndice se analizan objetivos de alto nivel y componentes lógicos e interfaces específicas definidos.

V.2 Referencias

En este apéndice se utilizan las referencias informativas adicionales siguientes.

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

[UIT-T J.364] Recomendación UIT-T J.364 (2006), *Alta, activación, configuración y gestión de IPCablecom2*.

[IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) terminology and considerations*.

[IETF RFC 3489] IETF RFC 3489 (2003), *Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NAT) (STUN).*

[ID BEHAVE] IETF draft, draft-ietf-behave-nat-udp-04, *Network Address Translation (NAT) Behavioural Requirements for Unicast UDP*, 6 September 2005.

[ID ICE] IETF draft, draft-ietf-mmusic-ice-07, *Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*, 6 March 2006.

[ID OUTBOUND] IETF draft, draft-ietf-sip-outbound-03, *Managing Client Initiated Connections in the Session Initiation Protocol (SIP)*, 20 March 2006.

[ID TURN] IETF draft, draft-ietf-behave-turn-00, *Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)*, February 2005.

V.3 Términos y definiciones

En [IETF RFC 2663] se definen varios términos relacionados con el NAT; para una descripción de términos y definiciones NAT no incluidos a continuación véase dicho documento. Además, en este documento se utilizan los términos siguientes:

V.3.1 ALG: Pasarela de la capa de aplicación (ALG, *application layer gateway*) incluida en un dispositivo NAT que intenta inspeccionar la señalización de aplicación y modificar las direcciones de la aplicación a fin de tener en cuenta los cambios introducidos por el NAT.

V.3.2 NAT, NAPT: Los NAT realizan la traducción de direcciones IP, generalmente interconectando dominios de direcciones públicos y privados. Los dispositivos NAPT también traducen puertos a fin de ahorrar direcciones IP. En este documento, el término NAT también hace referencia a dispositivos NAPT.

V.4 Abreviaturas, siglas o acrónimos

En este apéndice se utilizan las siguientes abreviaturas, siglas o acronimos adicionales.

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

RPV Red privada virtual

UDPTL Capa de transporte del protocolo UDP (*UDP transport layer*)

V.5 Requisitos y campo de aplicación del nat de IPCablecom2

El objetivo de este apéndice es proporcionar una definición de la arquitectura necesaria para que un UE consiga acceder a la red IPCablecom2 en presencia de uno o más dispositivos NAT. En particular, se presenta un conjunto completo de mecanismos destinados a que el UE mantenga los vínculos de señalización y de medios para garantizar que el tráfico de medios y de señalización destinado al UE pueda atravesar el NAT, así como permitir que el UE sea aprovisionado y gestionado cuando se encuentre detrás de un NAT.

Además, esta arquitectura proporciona es útil en caso de fallo de trayectos de señalización a través de un intermediario CSCF (P-CSCF, *proxy-CSCF*) de respaldo.

Finalmente, esta arquitectura asume que los UE tendrán que interfuncionar con dispositivos que no sean IPCablecom2 y que no soporten los mecanismos de tránsito de NAT requeridos, velando por que estos casos sean viables.

En la cláusula siguiente se recoge el conjunto de requisitos necesarios para conseguir dicho objetivo.

V.5.1 Requisitos

La lista siguiente refleja los requisitos que debería satisfacer una solución de propósito general para el tránsito del NAT para soportar los servicios previstos en IPCablecom2.

- Permitir que existan varios UE (uno o más dispositivos) detrás de un único NAT.
- No imponer requisitos a los dispositivos NAT, ni exigir que la red sea consciente de la presencia del NAT.
- Permitir peticiones entrantes y salientes hacia y desde equipos de usuario a través de los NAT.
- Mantener vinculaciones con varios P-CSCF para la entrega fiable de mensajes entrantes en caso de fallo de un P-CSCF.
- Soportar el tránsito de NATs entre el UE y la red (NAT en origen y NAT en la red visitada).
- Ser independiente de la aplicación, es decir, la solución no debería utilizar mecanismos específicos de las aplicaciones que podrían no ser útiles para aplicaciones no basadas en SIP. Las soluciones actualmente utilizadas pueden requerir soportar la aplicación.
- Evitar trayectos de medios innecesariamente largos debido al retardo introducido en dichos medios.
- Restablecer las comunicaciones en situaciones de fallo (por ejemplo, cuando el dispositivo NAT re-arranca y se pierden las vinculaciones).

V.5.2 Campo de aplicación

El campo de aplicación de la solución para el tránsito de NAT está limitado a los NAT situados en la red de acceso. En el caso del acceso por cable, ello significa los NAT entre el UE y el CMTS. Obsérvese que los E-MTA de IPCablecom quedan fuera del ámbito de este documento. No obstante, pueden imponerse algunos requisitos adicionales sobre los E-MTA de IPCablecom a fin

de garantizar su interoperabilidad con los UE de IPCablecom2 de acuerdo con los procedimientos de tránsito descritos en este documento y en otras especificaciones.

V.5.3 Limitaciones

En este apéndice no se trata el tránsito de NAT y de barreras contrafuegos por parte de trenes de medios de facsímil de la Rec. UIT-T T.38 sobre la capa de transporte del protocolo de datagramas de usuario (UDPTL, *user datagram protocol transport layer*).

No se soporta la retrollamada del operador en caso de llamadas de emergencia (como por ejemplo, 911 en los Estados Unidos de América) realizadas sin un registro previo.

V.6 Aspectos básicos del NAT

Los traductores de direcciones de red (NAT, *network address translators*) traducen las direcciones entre dos dominios de direcciones IP. La correspondencia se realiza en la mayoría de los casos entre un espacio de direcciones privadas de internet, que se reservan para un fin específico, y un espacio de direcciones públicas de internet. A dicha correspondencia se hace referencia como vinculación del NAT, ya que el NAT vincula la dupla PrivateIP:PrivatePort (IP privada: puerto privado) a la dupla PublicIP:PublicPort (IP pública: puerto público) para permitir que los subsiguientes paquetes de respuesta desde el punto extremo externo sean remitidos al pertinente anfitrión interno. En este apéndice, el término NAT también hace referencia a los dispositivos de traducción de puertos de direcciones de red (NAPT, *network address port translation*) que también traducen las direcciones de los puertos para reducir el número de direcciones públicas utilizadas en el lado de direcciones públicas del NAT (para más información véase la sección 4 de [IETF RFC 2663]).

Además de la traducción de direcciones, los dispositivos NAT tienen funcionalidad como barrera contrafuegos. En otras palabras, bloquean tráfico que pretende atravesar el NAT (desde el exterior al interior del dispositivo NAT/FW) en base a determinadas reglas de filtrado.

V.6.1 Tipos de dispositivos NA(P)T y barrera contrafuegos

En las cláusulas siguientes se utilizan definiciones tomadas del grupo de trabajo BEHAVE del IETF tal como se define en [ID BEHAVE].

V.6.1.1 Tipos de NAT

Por conveniencia, se incluyen las definiciones de [ID BEHAVE]:

Correspondencia independiente del punto extremo: el NAT reutiliza la correspondencia de puertos para ulteriores paquetes enviados desde la misma dirección IP y puerto interno a cualquier dirección IP y puerto externo.

Correspondencia dependiente de la dirección: el NAT reutiliza la correspondencia de puerto para ulteriores paquetes enviados desde la misma dirección IP y puerto interno a la misma dirección IP externa, con independencia de cual sea el puerto externo. Si los paquetes se envían a distintas direcciones IP externas, la correspondencia será distinta.

Correspondencia dependiente de la dirección y el puerto: el NAT reutiliza la correspondencia de puertos para ulteriores paquetes enviados desde la misma dirección IP y puerto interno a la misma dirección y puerto externos. Si los paquetes se envían a distintas direcciones IP y/o puertos externos, se utilizará una correspondencia distinta.

Este comportamiento de correspondencia de direcciones se describe en el cuadro V.1 y en la figura V.1.

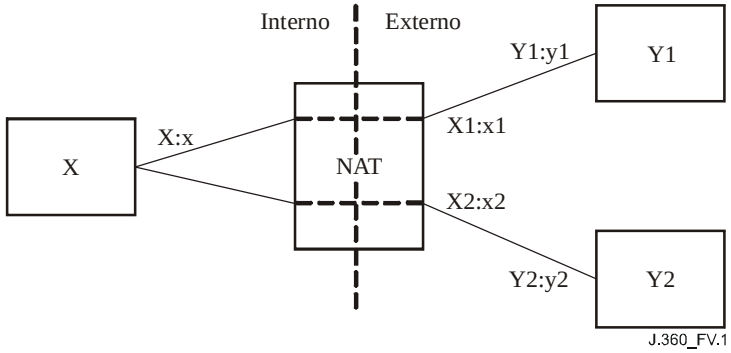


Figura V.1 – Tipos de NAT (correspondencia de direcciones)

En la figura V.1, la dirección X:x interna al NAT se traduce a la dirección X1:x1 cuando se comunica con Y1:y1 que es externo al NAT. La misma dirección X:x se traduce en X2:x2 cuando la comunicación es con Y2:y2.

Cuadro V.1 – Tipos de NAT (correspondencia de direcciones)

Tipo de NAT	Descripción de la correspondencia
Correspondencia independiente del punto extremo	X1:x1 siempre es X2:x2 para todos los valores de Y2:y2
Correspondencia dependiente de la dirección	X1:x1 es X2:x2 sólo si Y1 coincide con Y2
Correspondencia dependiente de la dirección y el puerto	X1:x1 es X2:x2 sólo si Y1:y1 coincide con Y2:y2

Obsérvese que para NAT pequeños (NAT de CPE residenciales), normalmente se asigna una única dirección IP (generalmente del espacio público) como dirección IP externa (es decir, X1 = X2). Sin embargo, los NAT de mayor tamaño asignarán la dirección IP externa de entre un conjunto de direcciones IP disponibles.

V.6.1.2 Comportamiento del filtrado

El comportamiento del filtrado de [ID BEHAVE] se describe en términos de categorías similares:

- Filtrado independiente del punto extremo: para enviar paquetes desde el lado interno del NAT a cualquier dirección IP externa es suficiente permitir la recepción de cualquier paquete en el punto extremo interno.
- Filtrado dependiente de la dirección: para poder recibir paquetes desde un punto extremo externo determinado, es necesario que el punto extremo interno haya enviado antes paquetes a la dirección IP de dicho punto extremo externo
- Filtrado dependiente de la dirección y el puerto: para recibir paquetes desde un punto extremo externo determinado, es necesario que el punto extremo interno haya enviado antes paquetes a la dirección IP y al puerto de dicho punto extremo externo

En el cuadro V.2 se describe este comportamiento de filtrado tomando los ejemplos de la figura V.1.

Cuadro V.2 – Tipos de comportamiento de filtrado

Tipo de NAT	Ejemplo de filtrado
Filtrado independiente del punto extremo	El envío de paquetes desde X:x a Y1:y1 permitirá recibir paquetes enviados desde Y1:y1 o desde Y2:y2.
Filtrado dependiente de la dirección	El envío de paquetes desde X:x a Y1:y1 permitirá recibir paquetes desde Y1:z para cualquier puerto z, pero no permitirá recibir paquetes desde cualquier otra dirección IP.
Filtrado dependiente de la dirección y el puerto	El envío de paquetes desde X:x a Y1:y1 sólo permitirá que se envíen paquetes desde Y1:y1 a X:x.

V.6.2 Consideraciones sobre el tránsito del NA(P)T y la barrera contrafuegos

Aunque el NAT proporciona una solución bastante sencilla para prevenir el agotamiento de las direcciones IP, la consecuencia es que estos dispositivos rompen muchas de las aplicaciones existentes, en particular, aplicaciones y protocolos de comunicación en tiempo real, tales como SIP, que dependen del intercambio de información de direccionamiento en el propio protocolo (algunas veces en las líneas de la cabecera SIP, o más generalmente, dentro del cuerpo del mensaje SDP de algunos mensajes SIP). Si la dirección incluida en el protocolo no es alcanzable, el receptor del mensaje será incapaz de responder satisfactoriamente dando lugar a sesiones infructuosas. Debido al creciente problema que los dispositivos NAT representan para los protocolos de comunicaciones, hasta ahora se han utilizado varias soluciones y también se han propuesto nuevas soluciones futuras. A continuación se presenta una visión sinóptica de algunos de los enfoques más utilizados y de sus inconvenientes:

- Pasarela de capa de aplicación (ALG, *application-layer gateway*): solución consistente en que el dispositivo NAT incluya una pasarela de capa de aplicación que analice el contenido de los mensajes del protocolo y los modifique en base a las vinculaciones del NAT que haya creado. Sin embargo, requiere la actualización constante del ALG conforme evolucionen los protocolos de forma que se preserve la operación esperada. Además, este enfoque fracasa cuando el protocolo incluye una verificación de integridad o está encriptado.
- Otro enfoque es el propuesto por el grupo MIDCOM del IETF. En este enfoque, un elemento de señalización controla directamente el dispositivo NAT a fin de abrir agujeros en la barrera contrafuegos para los medios y obtener la información de vinculación del NAT necesaria para actualizar cualquier información de direccionamiento IP (por ejemplo, SDP) interior al protocolo. Sin embargo, ello requiere que el dispositivo NAT lo soporte y que el dispositivo de señalización sea capaz de determinar cuál es el dispositivo NAT que debe controlar.
- Otras soluciones propuestas incluyen la inserción directa de un retransmisor de medios (un traductor de direcciones adicional) en el trayecto, o bien, la tunelización a través del dispositivo NAT mediante tecnología VPN. Cada uno de dichos métodos tiene sus ventajas e inconvenientes, pero la principal desventaja es que obligan a que los medios utilicen el mismo trayecto que la señalización. Ello puede resultar en que el encaminamiento de medios no sea el óptimo en determinadas circunstancias.
- La actual situación a corto plazo definida por el IETF consiste en utilizar la metodología ICE [ID ICE] con STUN [IETF RFC 3489] y TURN [ID TURN] para los medios y la metodología saliente [ID OUTBOUND] para la señalización. El método ICE permite que un punto extremo descubra, anuncie y encuentre la mejor dirección para la comunicación utilizando los mecanismos descritos en el documento que está siendo elaborado por el IETF [ID ICE] relativo al ICE, al tiempo que la metodología saliente (*outbound*) permite que el punto extremo gestione activamente su conectividad con la red SIP creando y manteniendo

flujos con su intermediario o intermediarios aprovisionados, tal como se describe en el documento en elaboración por el IETF [ID OUTBOUND].

- El grupo de trabajo BEHAVE del IETF está analizando otras soluciones. Sin embargo, ello implica realizar modificaciones del comportamiento del NAT a más largo plazo para solucionar estos problemas.

Además del problema de los protocolos que incluyen información de direcciones IP en su cabida útil, los dispositivos NAT son causa de otros problemas, tales como:

- Los dispositivos NAT tienen temporizadores asociados con las vinculaciones NAT y con los agujeros de las barreras contrafuegos. En el caso de transporte UDP, estas vinculaciones tienden a tener tiempos de vida bastante breves, y si no existe tráfico durante un periodo de tiempo, las vinculaciones quedan invalidadas y los agujeros cerrados. Para evitar esta situación, deben implantarse mecanismos que mantengan las vinculaciones/agujeros tanto para medios como para señalización.
- El protocolo RTP del IETF especifica que, para el protocolo UDP y otros similares, RTP debería utilizar un número puerto de destino par, y el correspondiente flujo RTCP debería utilizar el número de puerto de destino (impar) siguiente más alto. Sin embargo, las traducciones del NAT hacen que esta práctica sea inválida ya que normalmente no mantienen estas relaciones de puertos a través del NAT.
- Otro asunto de interés es el encaminamiento de señalización entrante a dispositivos UE. Esta señalización debe encaminarse a través del NAT sobre una conexión para la que exista una vinculación del NAT.

Dados los requisitos de la cláusula V.5.1, la solución actual del IETF que utiliza ICE (para medios) y OUTBOUND (para señalización) ha sido la elegida para IPCablecom2. Estas soluciones no solo satisfacen los requisitos establecidos, sino que además gozan de un apoyo creciente por parte de la industria.

V.7 Arquitectura del NAT de IPCablecom2

La figura V.2 representa un diagrama de referencia que muestra los componentes e interfaces más importantes relativos al tránsito de NAT/FW en la arquitectura de IPCablecom2. El módem de cable no se muestra ya que no contiene ninguna función específicamente relacionada o que afecte al tránsito del NAT.

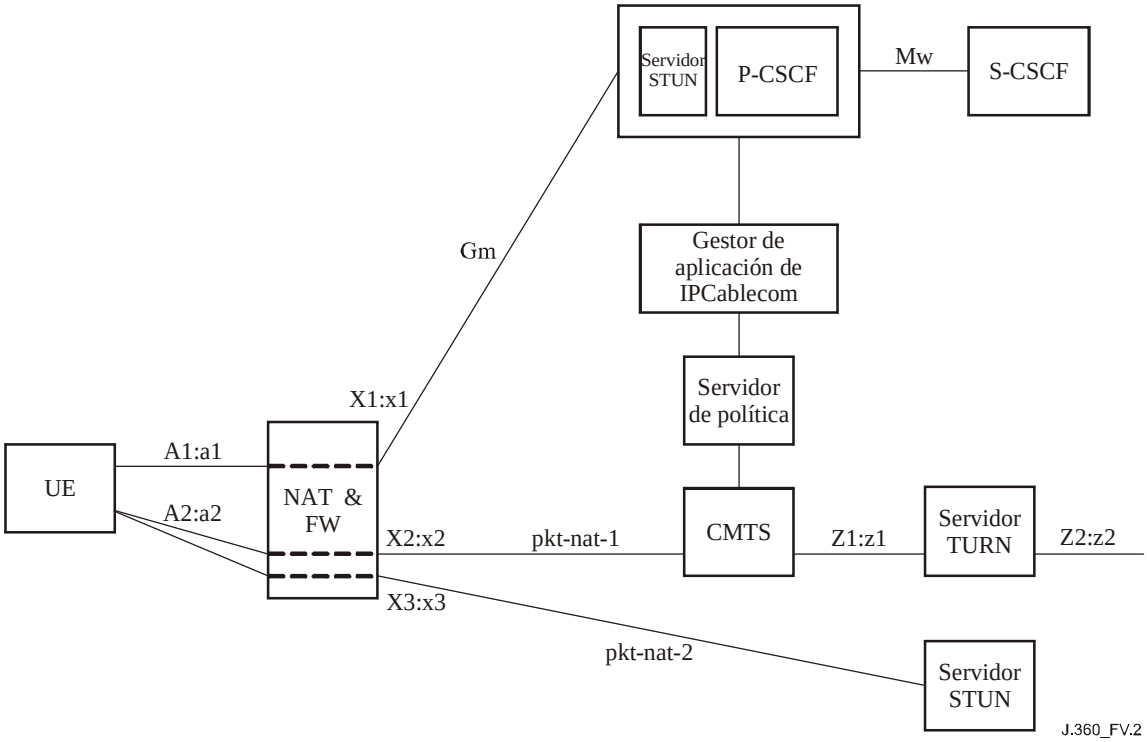


Figura V.2 – Puntos de referencia de tránsito del NAT y de la barrera contrafuegos (FW)

Las direcciones de red que se muestran en la figura V.2 tienen la forma "IP_address:port" ("IP_dirección:puerto"). Obsérvese que:

- Para dispositivos UE, normalmente se utiliza la misma dirección IP para medios y para señalización: A1 = A2.
- Para dispositivos NAT/FW en domicilio de cliente (CPE) residencial (desplegado en un entorno residencial) normalmente X1=X2=X3. Para NATs de mayor tamaño, con un número elevado de dispositivos cliente, la dirección IP externa puede elegirse de entre un conjunto de direcciones IP.

Se sobrentiende que existen otras topologías de red con dispositivos NAT, tal como un NAT de red. Estas redes están actualmente fuera del campo de aplicación de IPCablecom2 y no son objeto de este documento. Algunas topologías de red (tales como puntos de interconexión) pueden considerarse dentro del ámbito y objeto de atención de otros documentos.

Cuadro V.3 – Puntos de referencia del NAT de IPCablecom2

Puntos de referencia	Elementos de red de IPCablecom2	Descripción del punto de referencia
Gm	UE – P-CSCF	Permite que el UE se comunique con el P-CSCF para registro y control de sesión. Este punto de referencia está basado en SIP y se define en [UIT-T J.366.4].
Mw	CSCF – CSCF	Permite la comunicación y envío de mensajes de señalización entre los CSFC para apoyar el registro y el control de sesión. Este punto de referencia está basado en SIP y se define en [UIT-T J.366.4].

Cuadro V.3 – Puntos de referencia del NAT de IPCablecom2

Puntos de referencia	Elementos de red de IPCablecom2	Descripción del punto de referencia
pkt-nat-1	UE – Servidor STUN/P-CSCF	Interfaz basada en STUN definida por [IETF RFC 3489] y que utiliza el UE para determinar la dirección IP asignada a su NAT servidor o para mantener las vinculaciones NAT activas con un P-CSCF a través de un mecanismo de supervivencia.
pkt-nat-2	UE – Servidor TURN	Interfaz basada en TURN definida por [ID TURN] y que utiliza el UE para solicitar recursos del servidor TURN para la retransmisión de paquetes de medios hacia/desde el UE solicitante.

V.7.1 Relación con IPCablecom para multimedia

En la figura V.2 se muestran los elementos funcionales de la arquitectura de IPCablecom para multimedia [UIT-T J.179]. Incluye el gestor de aplicación (AM) y el servidor de política (PS). Aunque este documento no afecta al funcionamiento de IPCablecom para multimedia, es un requisito que el AM suministre las definiciones de clasificador de paquetes adecuadas para los flujos de medios al CMTS.

El AM construye clasificadores de paquetes para flujos de medios utilizando la dirección IP y puerto por defecto, tal como se anuncia en las líneas "m=" y "c=" del SDP. Cuando un UE invoca el procedimiento ICE y recopila direcciones candidatas, ha de utilizar el puerto y dirección asignadas al servidor TURN como dirección por defecto en el SDP.

Cuando se utiliza un servidor TURN, la dirección por defecto anunciada en el SDP es, como se ilustra en la figura V.2, "Z2:z2". Sin embargo, no aporta valor alguno el hecho de definir un clasificador de paquetes por lo que en el SDP debe haber algún filtro singular que describa los flujos desde las direcciones "X2:x2" y "Z1:z1". Puesto que el cliente conoce adónde enviar los paquetes, conoce el valor de "Z1:z1" y habrá de suministrarlo a través de SDP (un nuevo atributo del SDP definido en [UIT-T J.366.4]).

V.7.2 Relación con la versión 6 del IMS del 3GPP

IPCablecom2 se basa en la versión 6 del subsistema multimedia IP (IMS) definido por el 3GPP. El 3GPP es un acuerdo de colaboración entre varios organismos de normalización. El objeto del 3GPP es elaborar especificaciones técnicas e informes técnicos para las redes de los sistemas móviles GSM y de tercera generación (3G).

La actual arquitectura de la versión 6 del IMS no soporta el tránsito de NAT y de barrera contrafuegos. Dada esta limitación y el requisito de que IPCablecom2 soporte dispositivos para el tránsito del NAT y de l< barrera contrafuegos, IPCablecom2 ha añadido los requisitos necesarios a los documentos de la versión 6 del IMS. Los cambios al IMS se limitan a lo incluido en dos especificaciones técnicas, a saber, Rec. UIT-T J.366.3 y [UIT-T J.366.4].

Los cambios introducidos por Rec. UIT-T J.366.3 añaden requisitos para soportar el tránsito del NAT y de la barrera contrafuegos desde la perspectiva de la arquitectura.

Los cambios de procedimientos introducidos por [UIT-T J.366.4] se refieren al tránsito de señalización y de medios a través de los dispositivos de NAT y de barrera contrafuegos. Dichos cambios incluyen añadir lo incluido en el documento IETF Outbound Internet-Draft [ID OUTBOUND] para señalización, y en lo incluido en el documento IETF Interactive Connectivity Establishment Internet-Draft [ID ICE] para medios. En la cláusula V.8 de este documento se presenta una visión de alto nivel de las interfaces asociadas y de los diferentes papeles de los elementos de red en relación con el tránsito del NAT.

V.7.3 Relación con los E-MTA de IPCablecom

Este documento no aplica a los E-MTA de IPCablecom. Sin embargo, la solución propuesta conlleva que los E-MTA de IPCablecom acepten un paquete RTP vacío (sin cabida útil) con un tipo de cabida útil de 20 a modo de campo de supervivencia destinado a mantener las vinculaciones NAT para los medios.

V.7.4 Provisión y gestión

Además de permitir el tránsito de dispositivos NAT para señalización y para medios, es imperativo que el UE pueda ser aprovisionado y gestionado cuando se encuentra tras un NAT. La provisión hace referencia a los procesos necesarios para inicializar los atributos del usuario y los recursos del equipo de usuario y componentes de red necesarios para proveer servicios al usuario. La gestión se refiere a los protocolos, metodologías e interfaces que permiten supervisar, regular y garantizar la disponibilidad de los servicios ofrecidos en la red de un proveedor de servicio.

V.7.4.1 Provisión

Los procesos de provisión de IPCablecom2 utilizan señalización SIP normalizada, en particular los métodos SUBSCRIBE/NOTIFY. El aspecto singular del proceso de provisión es que ocurre antes del registro del UE, que es cuando típicamente se crean las vinculaciones del NAT. Debido a este procedimiento de registro previo, el P-CSCF necesita emplear los conceptos de "saliente" (*Outbound*) del IETF para asegurar que puede responder a la petición suscripción ("subscribe") y la posterior notificación. La forma más sencilla de hacerlo es requiriendo que el P-CSCF añada una cabecera ruta de registro ("record route") e insertando un testigo de flujo en la parte de usuario del URI utilizado en el valor del campo cabecera "record route". El testigo de flujo actúa como un identificador del flujo en el que se ha recibido el mensaje SUBSCRIBE. El flujo permite al P-CSCF identificar la dirección IP y puerto fuentes contenidos en la cabecera IP de la petición SUBSCRIBE.

Además, el UE necesita garantizar que las vinculaciones del NAT permanecen activas durante la vida de la suscripción, de forma que pueda entregarse el mensaje NOTIFY asociado.

V.7.4.2 Gestión

La gestión del UE queda actualmente fuera del ámbito de este apéndice y por tanto no se han desarrollado procedimientos sobre cómo gestionar un UE situado tras un NAT.

V.8 Descripción de la arquitectura

En la cláusula V.7 se describen un conjunto de entidades de red lógicas agrupadas de acuerdo a funciones de servicio específicas (NAT), así como un conjunto de interfaces que soportan los flujos de información intercambiados entre grupos funcionales y entidades de red. En esta cláusula se presenta un análisis más detallado de dichos elementos lógicos y de las interfaces asociadas a la arquitectura de IPCablecom2. También se ofrece una visión general de otros asuntos relacionados con la arquitectura NAT que no han sido documentados.

V.8.1 Componentes funcionales

En esta cláusula se presenta información adicional de cada uno de los elementos funcionales de la arquitectura de IPCablecom2 y su papel en el tránsito del NAT y la barrera contrafuegos.

V.8.1.1 P-CSCF

El papel principal del P-CSCF en el tránsito del NAT es garantizar que las peticiones y las respuestas se realizan a través de un flujo para el que existe una vinculación del NAT. Cuando se produce el registro, el P-CSCF almacena un testigo identificador de flujo en la cabecera "path" (trayecto) de SIP, de forma que puede identificar cuál es el flujo que debe utilizarse para las peticiones entrantes que contienen un URI con dicho testigo identificador de flujo.

El P-CSCF también soporta la extensión "rport" (puerto de la petición) para garantizar que todas las respuestas al UE, incluidas las de peticiones durante el diálogo (mid-dialog), se envían a la misma dirección IP y puerto sobre los que se recibió la petición a fin de asegurar su capacidad de transitar el NAT.

El P-CSCF también actúa como servidor STUN para permitir que el UE utilice STUN como mecanismo de supervivencia y para verificar los cambios que se produzcan en las vinculaciones del NAT (por ejemplo, para detectar re-arranques de NAT que puedan suprimir el flujo).

V.8.1.2 S-CSCF/Registro

El S-CSCF/Registro es responsable de generar y asignar el identificador de recurso uniforme de agente usuario encaminable globalmente (GRUU, *globally routable user agent uniform resource identifier*) para el UE, así como el P-CSCF asociado. El S-CSCF/Registro almacena el identificador de instancia (instance-id) asociado con el GRUU así como el identificador de registro (reg-id) y cabecera "path", e incluye a todos ellos como parte de la información de contacto.

V.8.1.3 UE

El UE es responsable de gestionar el proceso global de descubrimiento del NAT e invocar los mecanismos del protocolo necesarios para implementar el tránsito del NAT. En función del tipo de UE (autónomo, integrado, etc.) son necesarios los protocolos o mecanismos siguientes:

- Mecanismo saliente ("Outbound") para señalización.
- Cliente y servidor STUN para mantener las vinculaciones del NAT (señalización y medios), verificaciones de conectividad (ICE) y recopilación de direcciones candidatas (ICE).
- Cliente TURN para retransmisión de medios.
- Metodología ICE para medios.

Antes de que el UE pueda recibir peticiones de sesión entrantes (o respuestas a peticiones de sesión salientes), ha de invocar los procedimientos definidos en [ID OUTBOUND] durante el proceso de registro para crear un flujo con su P-CSCF asignado. Una vez que se han creado los flujos, el UE puede iniciar las sesiones y recibir peticiones de sesión a través del NAT.

Durante el proceso de establecimiento de sesión, el UE inicia la metodología ICE para recopilar, anunciar y probar direcciones candidatas.

El UE también utiliza el parámetro de extensión "rport" de la cabecera "Via" tal como se define en IETF RFC 3581 para el encaminamiento de respuesta simétrica de mensajes SIP.

V.8.1.4 Servidores STUN

Los servidores STUN reciben peticiones de vinculación STUN y proporcionan una respuesta que incluye la dirección IP y el puerto de origen en la cabecera IP de la petición de vinculación STUN. En la figura V.2 se incluyen dos servidores STUN:

- El servidor STUN representado como un componente funcional del P-CSCF lo utiliza el UE para mantener las vinculaciones del NAT para señalización. Estos mensajes STUN también pueden actuar como indicador de supervivencia que permite al UE determinar la disponibilidad del P-CSCF.
- El servidor STUN externo de la esquina inferior derecha de la figura V.2 se utiliza como parte de la metodología ICE [ID ICE] para determinar una de las posibles direcciones de medios candidata utilizando STUN [IETF RFC 3489]. En el ejemplo de flujo de medios representado con la dirección IP fuente "A2:a2", el UE obtiene la dirección traducida "X3:x3" a través del servidor STUN.

V.8.1.5 Servidor TURN

Además de los servidores STUN, la arquitectura contiene un servidor TURN. Este puede ser necesario si el dispositivo NAT no utiliza la correspondencia independiente del punto extremo (véase la cláusula V.6.1.1). Cuando se utiliza para transferir medios, el servidor TURN actúa como un retransmisor de medios. El UE envía paquetes desde la dirección "A2:a2" a la dirección del servidor TURN "Z1:z1". El NAT traduce en primer lugar la dirección fuente de dichos paquetes a "X2:x2", y son entonces retransmitidos por el servidor TURN de forma que la dirección fuente pasa a ser "Z2:z2". El servidor TURN también retransmite paquetes de medios en sentido contrario, es decir, paquetes enviados a "Z2:z2" serán enviados a "X2:x2" y entonces, a través del NAT, a "A1:a2". Obsérvese que el servidor TURN proporciona un filtrado independiente de la dirección (véase la cláusula V.6.1.2) que mantiene algunas de las características de filtrado de un NAT, pero no mantiene las restricciones de puertos, es decir, si el tráfico se envía a una dirección IP, se puede recibir desde la misma con independencia del puerto del que proceda.

Obsérvese que en la figura V.2 sólo se representa un ejemplo con un único flujo de medios. De hecho, puede haber varios flujos de medios y cada uno de ellos puede tener un flujo RTP, así como un canal de control RTCP utilizando RTCP. Las traducciones del NAT y los correspondientes mecanismos para la comunicación son relevantes para ambos.

V.8.2 Interfaces y puntos de referencia del protocolo

En este apéndice se han identificado varias interfaces o puntos de referencia de la arquitectura asociada al tránsito del NAT de IPCablecom2. En esta cláusula se presenta una visión general de las interfaces del protocolo.

V.8.2.1 Tránsito del NAT por los medios

Los UE se comunican a través de una red que proporciona componentes de señalización, así como de servidores STUN y TURN que permiten el tránsito del NAT. Los UE soportan los protocolos STUN y TURN así como la metodología ICE. En las cláusulas siguientes se describen los requisitos asociados. El diagrama de la figura V.3 ilustra una visión abstracta de la arquitectura.

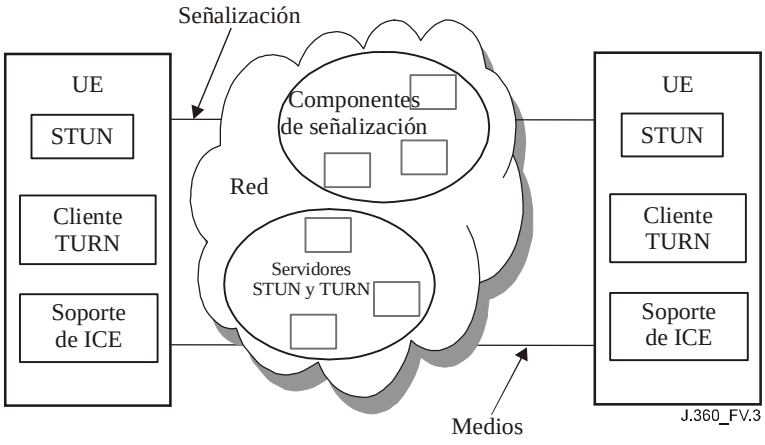


Figura V.3 – Diagrama abstracto de referencia

V.8.2.1.1 ICE

La metodología ICE [ID ICE] se compone de los pasos siguientes:

- Recopilación de direcciones candidatas para las comunicaciones de medios.
- Anunciar las direcciones candidatas junto con la dirección de transporte activa en las líneas m/c del SDP.

- Realizar verificaciones de conectividad con las direcciones candidatas a fin de seleccionar una dirección adecuada para las comunicaciones.
- En función del resultado de las verificaciones de conectividad, se puede seleccionar una de las direcciones candidatas como la dirección de transporte activa.
- Mantener las vinculaciones para los medios.

Si uno de los puntos extremos no soporta la metodología ICE, dicho punto extremo ignorará cualquiera de los atributos "a = candidate" y no proveerá ninguno de dichos atributos. En tal caso, se utilizará el valor por defecto de las líneas m/c y no se harán verificaciones de conectividad.

V.8.2.1.2 PKT-NAT-1

El tránsito simple de UDP a través del NAT (STUN, *simple traversal of UDP through NAT*) proporciona un conjunto de funciones. Dichas funciones permiten a las entidades situadas detrás de un NAT conocer las vinculaciones de direcciones atribuidas por el NAT a fin de mantener dichas vinculaciones abiertas, y comunicarse con otros dispositivos que conocen el STUN para validar la conectividad. El STUN no requiere cambios en los NAT y funciona con un número arbitrario de NAT en cascada entre la entidad de la aplicación y la internet pública.

STUN es un protocolo cliente – servidor sencillo. Un cliente envía una petición a un servidor y éste devuelve una respuesta. Existen dos tipos de peticiones, a saber, peticiones de vinculación, enviadas sobre UDP, y peticiones de secreto compartido, enviadas sobre TLS sobre TCP. Las peticiones de secreto compartido solicitan al servidor que devuelva un nombre de usuario y contraseña temporales. Dicho nombre de usuario y contraseña se utilizan en subsiguientes peticiones de vinculación y en respuestas de vinculación para la autenticación y la integridad de los mensajes.

Las peticiones de vinculación se utilizan para determinar las vinculaciones realizadas por los NAT. El cliente envía una petición de vinculación al servidor sobre UDP. El servidor analiza la dirección IP y el puerto fuentes de la petición y los copia en la respuesta que se devuelve al cliente.

Una vez que el cliente aprende cuál es la dirección WAN de su NAT local, anuncia dicha dirección como dirección candidata en el SDP para que puntos extremos distantes intenten y efectivamente la alcancen mediante el proceso ICE.

V.8.2.1.3 PKT-NAT-2

TURN es útil para aplicaciones que requieran que un cliente incluya una dirección de transporte en un mensaje del protocolo, con la expectativa de que el cliente pueda recibir los paquetes que un anfitrión enviará a dicha dirección. SIP es un ejemplo de ese tipo de protocolo, que utiliza el protocolo de descripción de sesión (SDP). El SDP transporta una dirección IP sobre la que el cliente recibirá paquetes de medios de su par. TURN es un protocolo cliente – servidor sencillo. Su sintaxis y funcionamiento general son equivalentes a STUN a fin de facilitar una implementación conjunta de ambos. TURN define un mensaje de petición, denominado "Allocate" (atribución), que solicita al servidor TURN la atribución de una dirección IP pública y un puerto. TURN puede ejecutarse sobre UDP y TCP, puesto que permite que un cliente solicite parejas de dirección y puerto para la recepción tanto en UDP como en TCP.

Un cliente TURN descubre, en primer lugar, la dirección de un servidor TURN en base a la configuración (véase [UIT-T J.364]). Ésta puede haber sido previamente configurada como una dirección IP, un nombre de dominio o un FQDN. Ello permite utilizar servidores TURN diferentes para UDP y TCP. Una vez conocido el servidor TURN, el cliente envía una petición TURN "Allocate" al servidor TURN. TURN proporciona un mecanismo para autenticación mutua y para verificaciones de integridad de peticiones y respuestas en base a un secreto compartido. Suponiendo que la petición es autenticada y no ha sido alterada, el servidor TURN atribuye una dirección de transporte al cliente TURN, denominada dirección de transporte atribuida, y la devuelve en la respuesta a la petición "Allocate". Normalmente, la dirección de trasporte atribuida será una de las interfaces en el propio servidor TURN. Sin embargo, también se permite que el servidor TURN esté

detrás de un NAT, en cuyo caso la dirección de transporte atribuida puede ser la del NAT, en cuyo caso se hace corresponder con la dirección privada del servidor TURN. Un funcionamiento adecuado del servidor TURN requerirá que tenga numerosas vinculaciones establecidas en el NAT con anterioridad; los medios para hacerlo quedan fuera del alcance de este apéndice.

Una vez que al cliente se le asigna una dirección TURN, la anuncia en la línea "c=" del SDP. En consecuencia, el servidor TURN será la primera dirección que se utilice hasta que mediante el proceso ICE se encuentre otra dirección candidata que constituya un trayecto más adecuado.

V.8.2.2 Gm (tránsito del NAT por la señalización)

En esta cláusula se proporciona una visión de alto nivel del procedimiento definido en el proyecto de documento del IETF "draft-ietf-sip-outbound-03" [ID OUTBOUNDD] y de los papeles de los distintos elementos de red de IPCablecom2. Obsérvese que el término flujo ("*flow*") se utiliza en [IP OUTBOUND] y en las cláusulas siguientes para describir una conexión en la capa de red que utiliza la mismas direcciones IP y puertos (UDP o TCP) en cualquier extremo de la conexión.

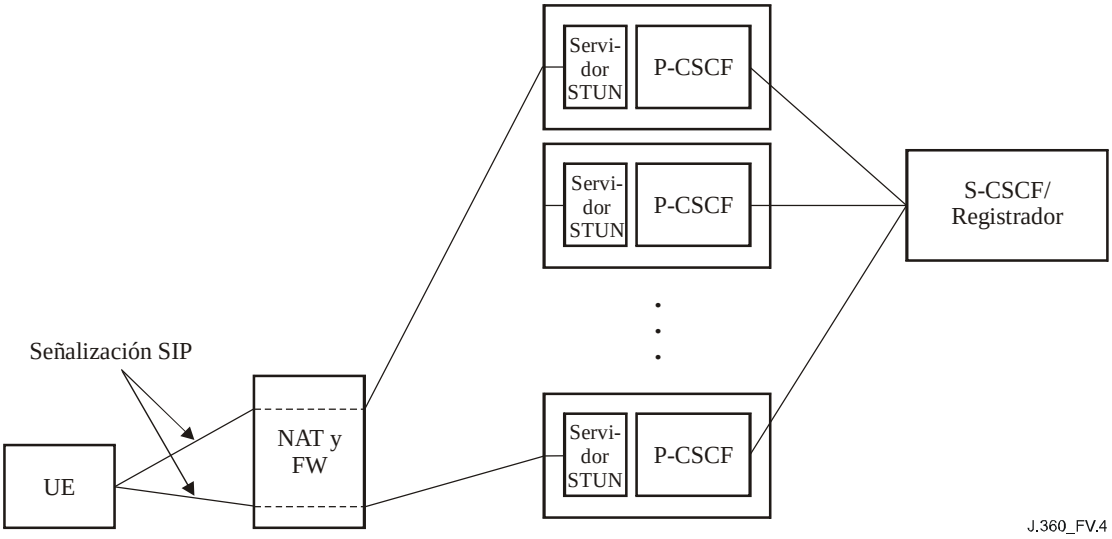


Figura V.4 – Tránsito del NAT por la señalización SIP

Tal como se ilustra en la figura V.4, un UE puede conectarse con un número cualquiera de P-CSCF. No obstante, para que un UE reciba llamadas entrantes, la señalización debe seguir un trayecto para el que exista un vinculación del NAT. Pueden existir varias de dichas vinculaciones sobre múltiples flujos con intermediarios de borde (por ejemplo, para disponer de redundancia). Los problemas del tránsito del NAT por parte de la señalización SIP implican lo siguiente:

- establecimiento de una conexión saliente: establecimiento de una o varias conexiones o flujos de señalización con el P-CSCF;
- mantenimiento de las vinculaciones del NAT y de los agujeros de la barrera contrafuego abiertos para dichos flujos; y
- señalización entrante: capaz de encaminar la señalización a un P-CSCF adecuado y desde allí al UE sobre un flujo para el que exista una vinculación del NAT.

V.8.2.2.1 Establecimiento de una conexión saliente

El registro SIP se utiliza para establecer una conexión saliente y las vinculaciones del NAT para dicho flujo. Durante el registro:

- El UE establece un identificador de instancia (instance-id) exclusivo que permanece constante cuando se produce un re-arranque.

- El UE también utiliza un identificador de registro (reg-id) como se describe en [ID OUTBOUND] para identificar cada flujo que se establece con un P-CSCF. Se utiliza STUN para mantener activo el flujo (es decir, las vinculaciones del NAT y los agujeros).
- El UE incluye el identificador de instancia (instance-id) y el identificador de registro (reg-id) cuando se registra. Si se registra en varios flujos, utiliza el mismo identificador de instancia (instance-id) pero un identificador de flujo (flow-id) diferente para cada flujo.
- El P-CSCF transmite el REGISTER e incluye una cabecera "Path" [ID OUTBOUND] para establecer un trayecto de señalización entre el P-CSCF que termina la conexión/flujo específica y el S-CSCF/Registrador. El P-CSCF incluye en la parte de usuario de una ruta flexible en la cabecera "path" un identificador exclusivo para identificar el flujo sobre el que se realiza el registro. El P-CSCF hará corresponder a dicho flujo cualquier petición futura que incluya dicho identificador.

El Registro almacena:

- El identificador de instancia (instance-id) y el identificador de registro (reg-id) como parte de la información de contacto, además del instante de tiempo en que se realizó la última actualización de la vinculación.
- La cabecera "Path".

Obsérvese que la existencia de múltiples registros en flujos alternativos (con diferentes identificadores de registro) permite que el UE preestablezca canales de señalización redundantes.

Si se permite que UE no registrados establezcan diálogos (por ejemplo, llamadas de emergencia, suscripción a perfiles de configuración, etc.), cualquier señalización que se produzca durante el tiempo de vida de dicha sesión debe mantenerse en el flujo establecido para dicha sesión. Ello obliga a que el P-CSCF registre la ruta y vele porque la señalización de dicha sesión se establezca sobre dicho flujo hasta que termine la sesión.

V.8.2.2.2 Mantenimiento de las vinculaciones del NAT

Tal como se ha indicado anteriormente, el UE utiliza STUN para:

- mantener las vinculaciones del NAT y los agujeros de la barrera contrafuego abiertos a la señalización;
- determinar si se produce un fallo de la conexión; y
- determinar si la vinculación del NAT ha cambiado como consecuencia de un re-arranque del mismo.

El servidor STUN utiliza en el P-CSCF el mismo puerto que se utiliza para la señalización de dicho flujo. El UE hace peticiones STUN sobre el flujo a modo de mecanismo de supervivencia del flujo, así como para determinar si las vinculaciones del NAT se han modificado como consecuencia de un re-arranque del NAT.

V.8.2.2.3 Señalización entrante

Obsérvese la señalización en ambos sentidos debe establecerse sobre un flujo con vinculaciones del NAT vigentes. En el caso de UDP, ello implica que los mensajes SIP se envían y se reciben sobre el mismo puerto UDP.

Como consecuencia de los registros, el S-CSCF/Registrador puede mantener información de contacto (incluyendo los identificadores de registro, reg-id) y cabeceras "Path" para poder acceder a una instancia de UE sobre uno o más flujos. Por lo tanto, puede encaminar una llamada entrante a una instancia de UE sobre un flujo dado, y si falla, reintentarlo sobre un flujo alternativo.

Apéndice VI

Visión general de la estrategia IPv6 e IPv4 de IPCablecom2

(Este apéndice no es parte integrante de esta Recomendación)

Queda en estudio.

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

Impreso en Suiza
Ginebra, 2008