

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.160

(11/2005)

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

IPCablecom

**Arquitectura para la distribución de servicios
dependientes del tiempo por redes de televisión
por cable que utilizan módems de cable**

Recomendación UIT-T J.160

UIT-T



Recomendación UIT-T J.160

Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable

Resumen

En esta Recomendación constituye un marco de referencia de alto nivel en el que se identifican los componentes funcionales y define las interfaces necesarias para suministrar servicios de voz digital y telefonía. A fin de implementar esta arquitectura, se elaboró una familia de Recomendaciones (Recs. UIT-T J.161-J.178).

Orígenes

La Recomendación UIT-T J.160 fue aprobada el 29 de noviembre de 2005 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.

© UIT 2006

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

ÍNDICE

| | Página |
|---|---------------|
| 1 Alcance | 1 |
| 2 Referencias | 1 |
| 3 Términos y definiciones | 2 |
| 4 Abreviaturas, acrónimos y convenios..... | 3 |
| 4.1 Abreviaturas y acrónimos..... | 3 |
| 4.2 Convenios | 4 |
| 5 IPCablecom | 4 |
| 5.1 Marco arquitectural IPCablecom..... | 4 |
| 5.2 Zonas y dominios IPCablecom..... | 5 |
| 5.3 Recomendaciones IPCablecom | 6 |
| 5.4 Consideraciones de diseño IPCablecom..... | 7 |
| 6 Componentes funcionales IPCablecom | 10 |
| 6.1 Adaptador de terminal de medios (MTA, <i>media terminal adapter</i>) | 10 |
| 6.2 Módem de cable (CM, <i>cable modem</i>) | 12 |
| 6.3 Red de acceso HFC | 12 |
| 6.4 Sistema de terminación de módem de cable (CMTS)..... | 12 |
| 6.5 Servidor de gestión de llamadas (CMS)..... | 13 |
| 6.6 Pasarela RTPC..... | 13 |
| 6.7 Componentes auxiliares del OSS | 16 |
| 6.8 Servidor de anuncios (ANS)..... | 17 |
| 7 Interfaces de protocolo | 17 |
| 7.1 Interfaces de señalización de llamada | 18 |
| 7.2 Trenes de medios..... | 20 |
| 7.3 Aprovisionamiento de dispositivo MTA..... | 22 |
| 7.4 Interfaces de capa de gestión de elemento SNMP..... | 23 |
| 7.5 Interfaces de mensajes de evento | 23 |
| 7.6 Calidad de servicio (QoS, <i>quality of service</i>)..... | 25 |
| 7.7 Aprovisionamiento de abonados del CMS | 28 |
| 7.8 Vigilancia electrónica..... | 29 |
| 7.9 Seguridad..... | 31 |
| 8 Consideraciones sobre el diseño de red | 36 |
| 8.1 Cuestiones relativas al mantenimiento del tiempo y a las notificaciones | 36 |
| 8.2 Temporización para alinear el tampón de reproducción de sonido con la tasa de codificación | 36 |
| 8.3 Direccionamiento IP | 37 |
| 8.4 Asignación dinámica de direcciones IP..... | 37 |
| 8.5 Asignación de nombres de dominio totalmente cualificados (FQDN) | 37 |

| | Página |
|--|---------------|
| 8.6 Marcado de prioridades de los paquetes del tren de señalización y del tren de medios | 38 |
| 8.7 Soporte fax..... | 39 |
| 8.8 Soporte para módems analógicos | 39 |
| Apéndice I – Glosario de términos | 39 |
| I.1 Definiciones..... | 39 |
| I.2 Abreviaturas y acrónimos..... | 42 |
| BIBLIOGRAFÍA | 45 |

Recomendación UIT-T J.160

Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable

1 Alcance

El proyecto IPCablecom define una familia de Recomendaciones que pueden utilizarse para la construcción de equipos interfuncionales capaces de proveer servicios de voz, vídeo y otros servicios multimedia basados en paquetes por sistemas de cable híbridos fibra/coaxial (HFC, *hybrid fiber/coax*) que utilizan módems de cable, conforme a la familia de Recomendaciones DOCSIS. Se continuará trabajando en la ampliación de esta arquitectura a fin de incluir aplicaciones multimedia.

2 Referencias

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

- Recomendación UIT-T G.711 (1988), *Modulación por impulsos codificados (MIC) de frecuencias vocales*.
- Recomendación UIT-T J.83 (1997), *Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable*.
- Recomendación UIT-T J.112 (1988), *Sistemas de transmisión para servicios interactivos de televisión por cable*, más anexo A (2001), *Difusión de vídeo digital: Canal de interacción para sistemas de distribución de televisión por cable en difusión de vídeo digital*, anexo B (2004), *Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia* y anexo C (2002), *Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia mediante la técnica de modulación de amplitud en cuadratura*.
- Recomendación UIT-T J.161 (2001), *Requisitos de los códecs de audio para la prestación de servicios de audio bidireccionales por redes de televisión por cable que utilizan módems de cable*.
- Recomendación UIT-T J.162 (2005), *Protocolo de señalización de llamada de red para la prestación de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable*.
- Recomendación UIT-T J.163 (2005), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por los redes de televisión por cable que utilizan módems de cable*.
- Recomendación UIT-T J.164 (2005), *Requisitos de los mensajes de evento para el soporte de servicios en tiempo real transmitidos mediante redes de televisión por cable que utilizan módems de cable*.
- Recomendación UIT-T J.166 (2005), *Marco de las bases de información de gestión IPCablecom*.

- Recomendación UIT-T J.167 (2005), *Requisitos del aprovisionamiento de un dispositivo adaptador de terminal de medios para la entrega de servicios en tiempo real por redes de televisión por cable que utilizan módems de cable.*
- Recomendación UIT-T J.170 (2005), *Especificación de seguridad de IPCablecom.*
- Recomendación UIT-T J.171.0 (2005), *Protocolo de control de pasarela de circuitos troncales IPCablecom: Aspectos generales de los perfiles.*
- Recomendación UIT-T J.178 (2005), *Señalización entre servidores de gestión de llamadas IPCablecom.*
- Recomendación UIT-T Q.704 (1996), *Funciones y mensajes de red de señalización.*
- Recomendación UIT-T T.38 (2005), *Procedimientos para la comunicación facsímil en tiempo real entre terminales facsímil del grupo 3 por redes con protocolo Internet.*
- IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*
- IETF RFC 1119 (1989), *Network Time Protocol.*
- IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications.*
- IETF RFC 1890 (1996), *RTP Profile for Audio and Video Conferences with Minimal Control.*
- IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.*
- IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP.*
- IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv.*
- IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*
- IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).*
- IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).*
- IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR).*

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 IPCablecom: Proyecto del UIT-T consistente en una arquitectura y una serie de Recomendaciones que permiten la entrega de servicios en tiempo real por las redes de televisión por cable utilizando módems de cable.

3.2 módem de cable: Un módem de cable es un dispositivo de terminación de capa 2 que termina el extremo cliente de la conexión DOCSIS.

3.3 red IP gestionada: Una red IP gestionada por una sola entidad y que se utiliza para transportar señalización IPCablecom y paquetes de medios.

3.4 red medular IP gestionada: Una red IP gestionada que se utiliza para interconectar dominios IPCablecom.

4 Abreviaturas, acrónimos y convenios

4.1 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos.

| | |
|---------|--|
| ANC | Controlador de anuncios (<i>announcement controller</i>) |
| ANP | Reproductor de anuncios (<i>announcement player</i>) |
| ANS | Servidor de anuncios (<i>announcement server</i>) |
| CM | Módem de cable (<i>cable modem</i>) |
| CMS | Servidor de gestión de llamadas (<i>call management server</i>) |
| CPE | Equipo en las instalaciones del cliente (<i>customer premises equipment</i>) |
| DHCP | Protocolo de configuración dinámico del anfitrión (<i>dynamic host configuration protocol</i>) |
| DNS | Sistema de nombres de dominio (<i>domain name system</i>) |
| DTMF | Multifrecuencia bitono (<i>dual tone multi-frequency</i>) |
| FQDN | Nombre de dominio totalmente cualificado (<i>fully qualified domain name</i>) |
| GC | Controlador de puerta (<i>gate controller</i>) |
| HFC | Híbrido fibra/coaxial (<i>hybrid fibre/coax</i>) |
| HTTP | Protocolo de transferencia hipertexto (<i>hypertext transfer protocol</i>) |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Grupo de tareas especiales de ingeniería en Internet (<i>Internet Engineering Task Force</i>) |
| IP | Protocolo Internet (<i>Internet protocol</i>) |
| IPsec | Seguridad de protocolo Internet (<i>IP security</i>) |
| ISTP | Protocolo de transporte de señalización Internet (<i>Internet signalling transport protocol</i>) |
| MAC | Control de acceso a medios (<i>media access control</i>) |
| MF | Multifrecuencia |
| MG | Pasarela de medios (<i>media gateway</i>) |
| MGC | Controlador de pasarela de medios (<i>media gateway controller</i>) |
| MIB | Base de información de gestión (<i>management information base</i>) |
| MMH | Troceo modular multilineal (<i>multilinear modular hash</i>) |
| MTA | Adaptador de terminal de medios (<i>media terminal adapter</i>) |
| MTP | Parte transferencia de mensajes (<i>message transfer part</i>) |
| NAT | Traductor de dirección de red (<i>network address translator</i>) |
| NCS | Señalización de llamadas basada en la red (<i>network-based call signalling</i>) |
| OSS | Sistema de soporte de operaciones (<i>operations support system</i>) |
| PU-RDSI | Parte usuario de la red digital de servicios integrados |
| QoS | Calidad de servicio (<i>quality of service</i>) |
| RKS | Servidor de mantenimiento de registros (<i>record keeping server</i>) |
| RTP | Protocolo de transferencia en tiempo real (<i>real-time transfer protocol</i>) |

| | |
|------|---|
| RTPC | Red telefónica pública conmutada |
| SA | Dirección de origen (<i>source address</i>) |
| SCCP | Parte control de la conexión de señalización (<i>signalling connection control part</i>) |
| SG | Pasarela de señalización (<i>signalling gateway</i>) |
| SID | Número de identificación de sistema (<i>system identification number</i>) |
| SNMP | Protocolo simple de gestión de red (<i>simple network management protocol</i>) |
| TCAP | Parte aplicación de capacidades de transacción (<i>transaction capabilities application part</i>) |
| TFTP | Protocolo de transferencia de ficheros trivial (<i>trivial file transfer protocol</i>) |
| TGCP | Protocolo de control de pasarela troncal (<i>trunking gateway control protocol</i>) |
| TGS | Servidor que concede tickets (<i>ticket granting server</i>) |
| ToS | Tipo de servicio (<i>type of service</i>) |
| UDP | Protocolo de datagrama de usuario (<i>user datagram protocol</i>) |

4.2 Convenios

Si se implementa esta Recomendación, se entenderá que las palabras "DEBE(N)" y "DEBERÁ(N)" así como "REQUERIDO" indican un aspecto obligatorio de esta Recomendación.

En el siguiente cuadro se resumen las palabras clave utilizadas en esta Recomendación que indican el nivel de importancia de determinados requisitos.

| | |
|-----------------|--|
| "DEBE(N)" | Esta palabra o el adjetivo "REQUERIDO" significa que el elemento es un requisito absoluto de esta Recomendación. |
| "NO DEBE(N)" | Esta expresión significa que el elemento es una prohibición absoluta de esta Recomendación. |
| "DEBERÍA(N)" | Esta palabra o el adjetivo "RECOMENDADO" significa que, en determinadas circunstancias, pueden existir motivos válidos para hacer caso omiso de este elemento, pero que se debería considerar todas las repercusiones y ponderar el caso cuidadosamente antes de optar por un procedimiento diferente. |
| "NO DEBERÍA(N)" | Esta expresión significa que pueden existir motivos válidos en determinadas circunstancias en las que el comportamiento indicado es aceptable o incluso útil, pero que se debería considerar todas las repercusiones y ponderar cuidadosamente el caso antes de aplicar cualquier comportamiento descrito con esta etiqueta. |
| "PUEDE(N)" | Esta palabra o el adjetivo "OPCIONAL" significa que este elemento es verdaderamente opcional. Un vendedor puede elegir incluir el elemento porque, por ejemplo, así lo requiere un determinado mercado o porque mejora el producto, y otro vendedor puede omitir el mismo elemento. |

5 IPCablecom

5.1 Marco arquitectural IPCablecom

A muy alto nivel, la arquitectura IPCablecom contiene tres redes: la "red de acceso HFC DOCSIS", la "red IP gestionada" y la RTPC. El sistema de terminación de módem de cable (CMTS, *cable modem termination system*) proporciona conectividad entre la "red de acceso HFC DOCSIS" y la

"red IP gestionada". Tanto la pasarela de señalización (SG, *signalling gateway*) como la pasarela de medios (MG, *media gateway*) proporcionan conectividad entre la "red IP gestionada" y la RTPC. La arquitectura de referencia IPCablecom está representada en la figura 1.

La red de acceso HFC DOCSIS proporciona transporte de alta velocidad fiable y seguro entre las instalaciones del cliente y la cabecera del cable. Esta red de acceso puede proporcionar todas las capacidades DOCSIS y, en particular, la de calidad de servicio. Entre los componentes de la red de acceso HFC DOCSIS se cuenta con: el módem de cable (CM), el adaptador de terminal multimedia (MTA) y el sistema de terminación de módem de cable (CMTS).

La red IP gestionada desempeña varias funciones. En primer lugar, proporciona interconexión entre los componentes funcionales IPCablecom básicos que se encargan de la señalización, los medios, el aprovisionamiento, y el establecimiento de la calidad de servicio en la red de acceso. Además, la red IP gestionada proporciona conectividad IP de largo alcance entre otras redes IP gestionadas y las redes HFC DOCSIS. La red IP gestionada incluye los componentes funcionales siguientes: servidor de gestión de llamadas (CMS, *call management server*), varios servidores auxiliares del sistema de soporte de operaciones (OSS, *operations support system*), pasarela de señalización (SG), pasarela de medios (MG), y controlador de pasarela de medios (MGC, *media gateway controller*).

Los diferentes componentes de red de la figura 1 se describen detalladamente en la cláusula 6.

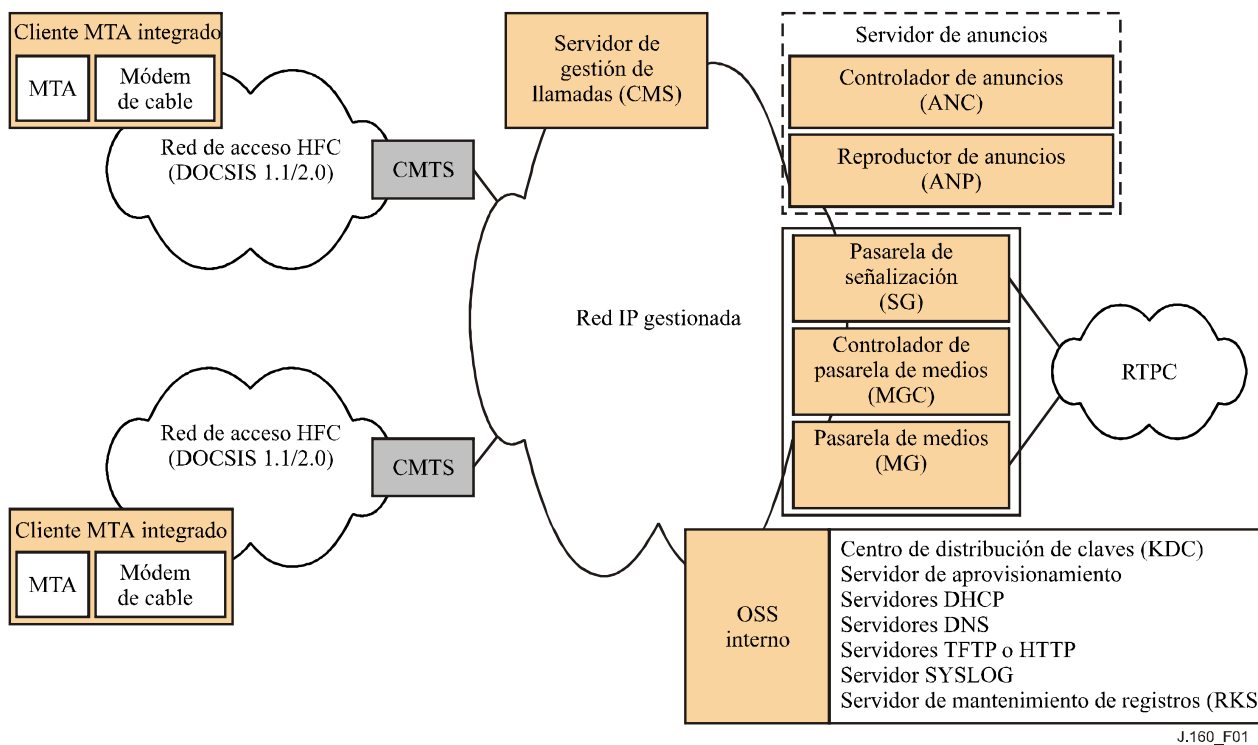


Figura 1/J.160 – Arquitectura de referencia IPCablecom

5.2 Zonas y dominios IPCablecom

Una zona IPCablecom está constituida por el conjunto de MTA de una o más redes de acceso HFC DOCSIS que son gestionadas por un solo CMS funcional, como se muestra en la figura 2. En el interior de una zona, las interfaces entre los componentes funcionales y entre las zonas (por ejemplo CMS ↔ CMS) están definidas en las Recomendaciones de IPCablecom.

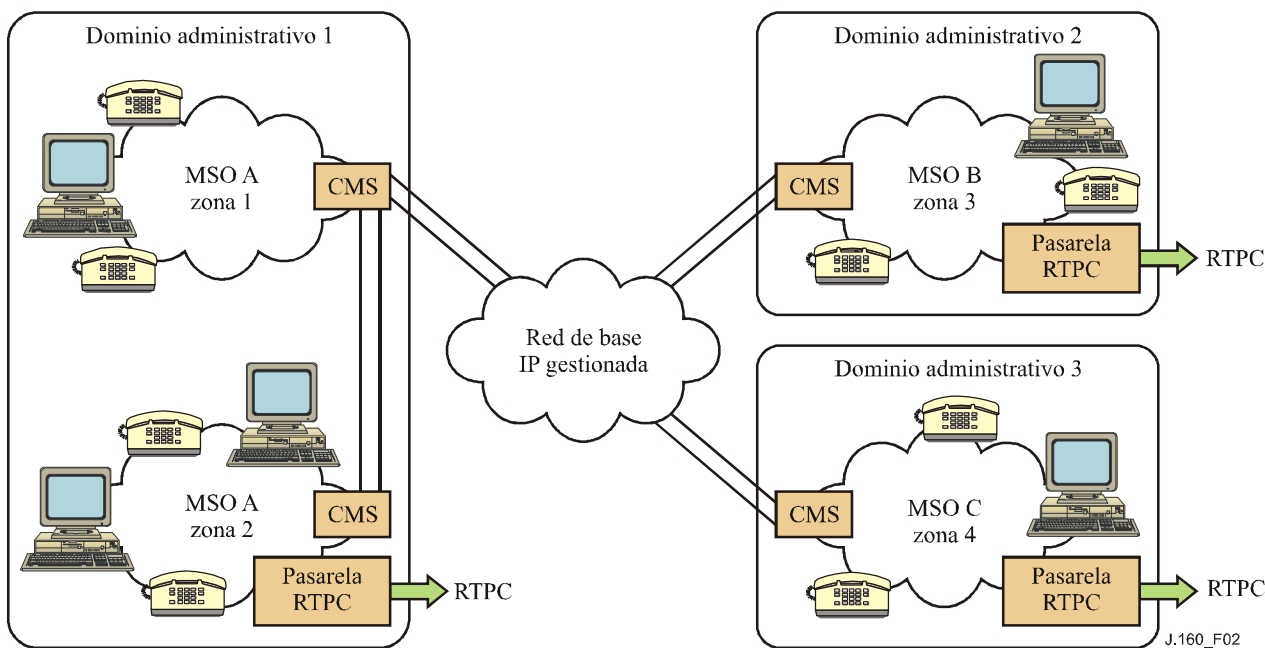


Figura 2/J.160 – Zonas y dominios administrativos

Un dominio IPCablecom está constituido por una o más zonas IPCablecom operadas y gestionadas por una sola entidad administrativa. Un dominio IPCablecom puede denominarse también dominio administrativo.

5.3 Recomendaciones IPCablecom

Cuadro 1/J.160 – Recomendaciones IPCablecom

| | |
|----------------|---|
| J.160 | Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable |
| J.161 | Requisitos de los códecs de audio para la prestación de servicios de audio bidireccionales por redes de televisión por cable que utilizan módems de cable |
| J.162 | Protocolo de señalización de llamada de red para la prestación de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable |
| J.163 | Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable |
| J.164 | Requisitos de los mensajes de evento para el soporte de servicios en tiempo real transmitidos mediante redes de televisión por cable que utilizan módems de cable |
| J.165 | Protocolo de transporte de señalización Internet IPCablecom |
| J.166 | Marco de las bases de información de gestión IPCablecom |
| J.167 | Requisitos del aprovisionamiento de un dispositivo adaptador de terminal de medios para la entrega de servicios en tiempo real por redes de televisión por cable que utilizan módems de cable |
| J.168 | Libre – Incorporado como anexo E/J.166 |
| J.169 | Libre – Incorporado como anexo C/J.166 |
| J.170 | Especificación de la seguridad de IPCablecom |
| J.171.1 | Protocolo de control de pasarela de circuitos troncales IPCablecom: Perfil 1 |
| J.171.2 | Protocolo de control de pasarela de circuitos troncales IPCablecom: Perfil 2 |

Cuadro 1/J.160 – Recomendaciones IPCablecom

| | |
|-------|---|
| J.172 | Mecanismo de evento de gestión IPCablecom |
| J.173 | Soporte del servicio de comunicaciones de línea primaria mediante adaptador de terminal de medios incorporado en IPCablecom |
| J.174 | Calidad de servicio interdominio IPCablecom |
| J.175 | Protocolo de servidor de audio |
| J.176 | Libre – Incorporado como anexo D/J.166 |
| J.177 | Especificación de la prestación de servicios de abonado por el servidor de gestión de llamadas IPCablecom |
| J.178 | Señalización entre servidores de gestión de llamadas IPCablecom |
| J.179 | Soporte de IPCablecom para multimedia |

5.4 Consideraciones de diseño IPCablecom

A fin de posibilitar las comunicaciones multimedia en tiempo real utilizando la estructura de red de cable, en las Recomendaciones IPCablecom se definen protocolos en las siguientes áreas:

- señalización de llamadas;
- calidad de servicio;
- transporte y codificación de trenes de medios;
- aprovisionamiento de dispositivos;
- mensajería de eventos;
- seguridad;
- vigilancia electrónica;
- sistemas de soporte operacional.

La presente cláusula proporciona una visión de conjunto de los objetivos y conceptos de diseño de alto nivel utilizados en la elaboración de las Recomendaciones que definen la arquitectura de referencia IPCablecom. En las Recomendaciones de IPCablecom se encuentran los requisitos detallados de los protocolos de cada una de estas áreas.

5.4.1 Objetivos de arquitectura generales

- Poder disponer de capacidades de calidad de voz de un nivel comparable o superior al de la RTPC desde el punto de vista del usuario final.
- Proporcionar una arquitectura de red que sea escalable y que pueda dar cabida a millones de abonados.
- Lograr que el retardo en un sentido del acceso IP local y del egreso IP (es decir, excluyendo la red de base IP) sea menor que 45 ms.
- Mejorar las normas existentes. IPCablecom procura especificar para la industria unas normas abiertas y aprobadas que hayan sido ampliamente adoptadas en redes de comunicaciones comerciales. Se incluyen, en particular, diversas normas aprobadas por la UIT, el IETF, el IEEE y otras organizaciones normativas en materia de comunicaciones.
- Mejorar y utilizar como base las capacidades de transporte de datos y de calidad de servicio que posibilita la infraestructura J.112.
- Definir una arquitectura que permita a múltiples vendedores desarrollar rápidamente soluciones interoperables de bajo costo para satisfacer los requisitos de fecha de salida al mercado.

- Conseguir que la probabilidad de bloqueo de llamadas sea inferior al 1% durante la hora cargada de un día de alto tráfico (HDBH, *high day busy hour*).
- Conseguir que los cortes de llamada y los defectos de llamada puedan modificarse hasta que constituyan menos del 1 por 10 000 de las llamadas completadas.
- Dar soporte a módems (hasta 56 kbit/s para V.90) y fax (hasta 14,4 kbit/s).
- Conseguir que los deslizamientos de trama debidos a relojes de muestreo no sincronizados o a paquetes perdidos se produzcan menos de 0,25 veces por minuto.

5.4.2 Señalización de llamada

- Definir una arquitectura de señalización en red.
- Proporcionar señalización de llamadas de extremo a extremo para los modelos de llamada siguientes:
 - llamadas originadas en la RTPC y terminadas en la red de cable;
 - llamadas originadas en la red de cable y terminadas en la red de cable;
 - llamadas originadas en la red de cable y terminadas en la RTPC;
 - llamadas que atraviesan zonas (de un mismo dominio) y dominios (entre dominios).
- Proporcionar señalización para dar cabida a características de llamada tales como:
 - llamada en espera;
 - cancelación de llamada en espera;
 - reenvío de llamada (no responde, ocupado, variable);
 - llamada tripartita;
 - indicador de espera para mensajes de correo vocal;
 - entrega del número llamante;
 - entrega del nombre del llamante;
 - entrega de la identidad del llamante en espera;
 - bloqueo de entrega de la identidad del llamante;
 - rechazo de llamadas anónimas;
 - comunicación por intermediario automática;
 - rellamada automática;
 - tono distintivo/llamada en espera;
 - localización de llamadas por el cliente.
- Dar soporte a una señalización compatible con las normas de telefonía IP existentes, para utilizarlo en las redes IPCablecom de los operadores por cable y al conectarse con la RTPC.
- Capacidad de marcación directa de cualquier número de teléfono nacional o internacional (dirección Rec. UIT-T E.164).
- Posibilidad de recibir una llamada desde cualquier teléfono nacional o internacional soportado por la RTPC.
- Posibilidad de que un nuevo abonado conserve su número de teléfono actual mediante portabilidad de número local (LNP, *local number portability*).
- Posibilidad de utilizar el operador que se desee para llamadas de larga distancia. Particularmente, mediante preabono y mediante selección por llamada.
- Posibilidad de restricciones tales como el bloqueo de llamada o el cargo por bloqueo de llamada (por ejemplo, bloqueo de llamadas a determinados prefijos).

5.4.3 Calidad de servicio

- Proporcionar un amplio abanico de mecanismos de política para habilitar y gestionar la QoS de los servicios IPCablecom en la red de acceso.
- Proporcionar mecanismos de control de admisión en los sentidos ascendente y descendente.
- Posibilitar cambios dinámicos de la QoS en el transcurso de las llamadas IPCablecom.
- Reducir al mínimo y evitar una utilización abusiva de la QoS y, en particular, ataques tales como la apropiación indebida de servicio o la denegación de servicio. Hacer que la política de QoS sea decidida y aplicada por elementos de confianza de la red IPCablecom.
- Incorporar un mecanismo prioritario para los servicios de señalización de emergencia o de otro tipo basados en el concepto de prioridad.

5.4.4 Códecs y trenes de medios

- Reducir al mínimo los efectos producidos por el retardo, la pérdida de paquetes y la fluctuación de fase sobre la calidad de la señal vocal en telefonía IP.
- Definir un conjunto mínimo de códecs de audio que deberán ser compatibles con todos los dispositivos de los puntos de extremo IPCablecom (MTA y MG). Los criterios de evaluación de los códecs obligatorios se elegirán como los más eficientes en términos de calidad vocal, utilización de anchura de banda y complejidad de implementación.
- Dar cabida a tecnologías de códec evolutivas en banda estrecha y en banda ancha.
- Especificar mecanismos de cancelación de eco y de detección de actividad vocal.
- Posibilitar la transmisión y detección en multifrecuencia bitono de manera transparente y sin errores mediante transmisión en banda y retransmisión DTMF.
- Poder utilizar dispositivos de terminal para sordos y personas con deficiencias auditivas.
- Proporcionar mecanismos de conmutación de códec cuando se necesiten servicios de fax y módem.
- Dar soporte a la retransmisión fax que permita una transmisión fiable de fax por redes IP.
- Dar soporte al cálculo e información mediante la métrica VoIP para supervisar la calidad vocal.

5.4.5 Aprovisionamiento de dispositivos y OSS

- Posibilitar el aprovisionamiento estático y dinámico de equipos en las instalaciones del cliente (MTA y CM).
- Los cambios de aprovisionamiento comunes no deberían obligar a reiniciar el MTA.
- Posibilitar la asignación y gestión dinámica de direcciones IP para los dispositivos de los abonados.
- Asegurarse de que el aprovisionamiento y configuración en tiempo real del software del MTA no afectan negativamente al servicio prestado al abonado.
- Definir módulos MIB para gestionar el equipo en las instalaciones del cliente (MTA) utilizando el protocolo simple de gestión de red (SNMP) del IETF.

5.4.6 Seguridad

- Posibilitar capacidades vocales para usos domiciliarios que den como mínimo la misma sensación de privacidad que la RTPC.
- Conferir protección frente a posibles ataques al MTA.
- Proteger al operador de cable de diversos tipos de ataques, tales como la denegación de servicio, la interrupción de la red, o la apropiación indebida de servicios.

- Entre las consideraciones de diseño se incluyen la confidencialidad, la autenticación, la integridad y el control de acceso.

5.4.7 Vigilancia electrónica

- Facilitar la posibilidad de vigilancia electrónica con información de datos de llamadas y contenido de llamadas.

6 Componentes funcionales IPCablecom

En esta cláusula se describen los componentes funcionales presentes en una red IPCablecom (véase la figura 3). La descripción de los componentes no tiene por objeto definir o implicar requisitos respecto de la implementación de los productos, sino más bien describir las funciones que cada uno de esos componentes desempeñan en la arquitectura de referencia. Obsérvese que determinadas implementaciones de productos pueden combinar componentes funcionales conforme resulte necesario. No es necesario que en una red IPCablecom estén presentes todos los componentes.

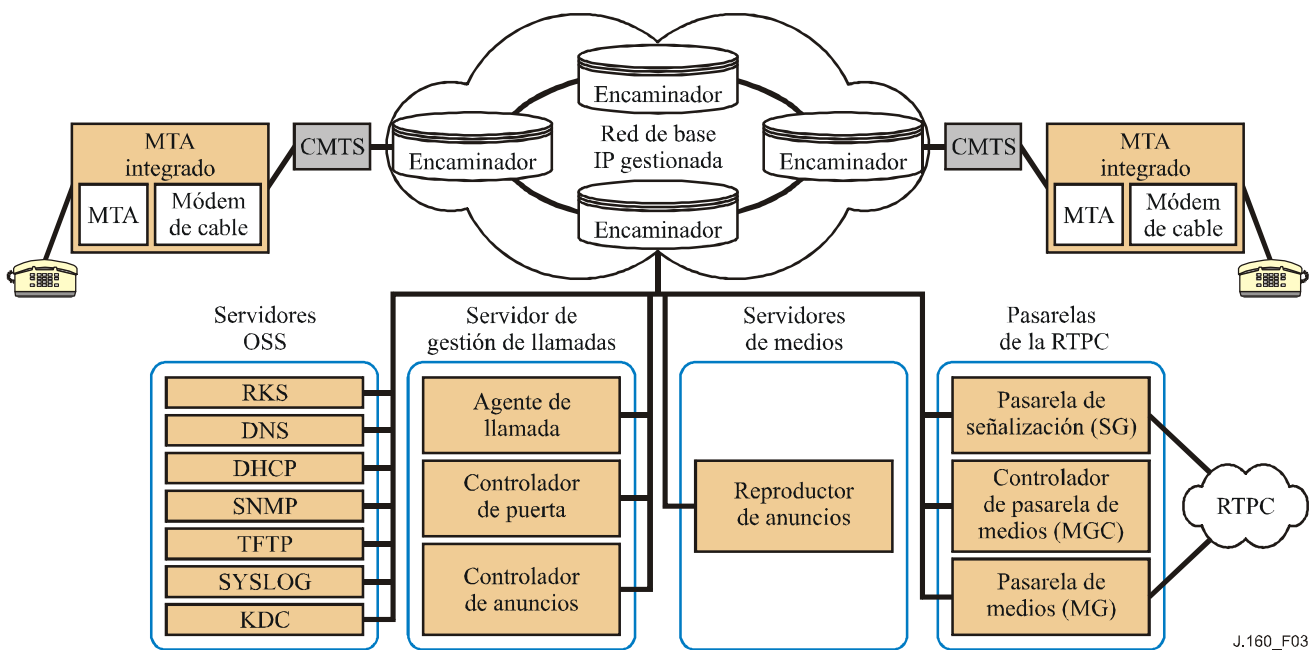


Figura 3/J.160 – Modelo de referencia de componentes IPCablecom

La arquitectura IPCablecom contiene elementos de red de confianza y elementos que no son de confianza. Los elementos de red de confianza suelen estar situados en una red de base gestionada del operador de cable. Los elementos de red que no son de confianza, como el CM o el MTA, suelen estar ubicados en el domicilio del abonado y son externos a las instalaciones del operador de cable.

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

Un MTA es un dispositivo de cliente IPCablecom que contiene en el lado del abonado una interfaz con el CPE del abonado (por ejemplo, un teléfono) y en el lado red una interfaz de señalización para llamar a los elementos de control de la red. Un MTA proporciona, además de códecs, todas las funciones de señalización y encapsulado requeridas para el transporte de medios y la señalización de llamadas.

Los MTA residen en la ubicación del cliente y están conectados a otros elementos de la red IPCablecom mediante la red de acceso HFC (Rec. UIT-T J.112). Se requiere que los MTA den

soporte al protocolo de señalización de llamada basada en la red (NCS, *network call signalling*) (Rec. UIT-T J.162).

Un MTA integrado (E-MTA, *embedded MTA*) es un dispositivo físico que incorpora un módem de cable y un componente MTA IPCablecom. En la figura 4 se muestra un diagrama funcional representativo de un MTA integrado.

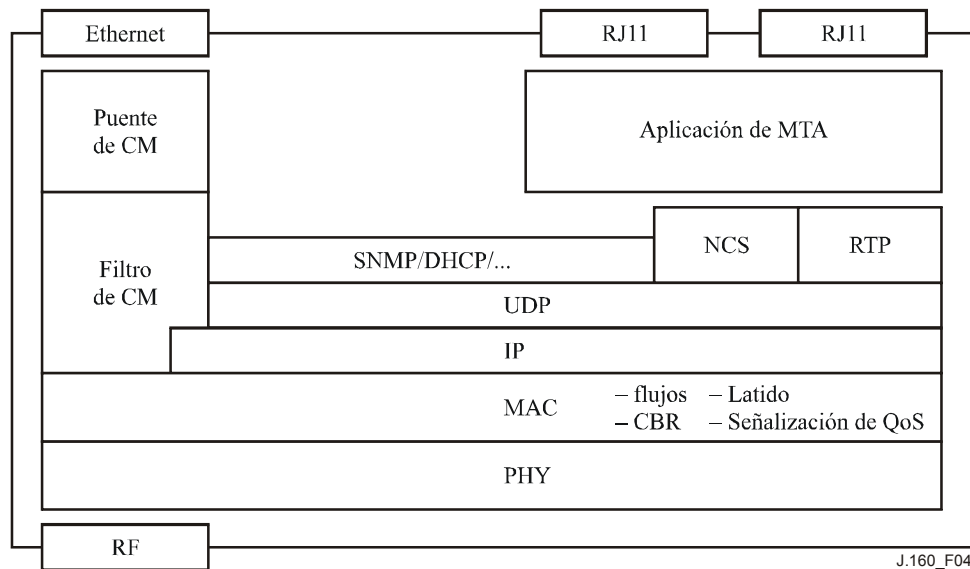


Figura 4/J.160 – Arquitectura funcional conceptual de un MTA integrado

6.1.1 Requisitos funcionales de un MTA

Un MTA desempeña las funcionalidades siguientes:

- Señalización de llamadas NCS con el CMS.
- Señalización de QoS con el CMS y el CMTS.
- Autenticación, confidencialidad e integridad de algunos mensajes entre el MTA y otros elementos de la red IPCablecom.
- Establecimiento de correspondencias entre los trenes de medios y los servicios MAC de la red de acceso DOCSIS.
- Codificación/decodificación de trenes de medios.
- Incorporación de múltiples indicadores de audio en los teléfonos, por ejemplo en forma de tonos de llamada, tonos de llamada en espera, tono de marcación entrecortado, tono de marcación, etc.
- Señalización normalizada de línea analógica RTPC para tonos de audio, transporte de voz, señalización de identificación de llamante, DTMF, e indicadores de mensaje en espera.
- El códec audio G.711 y códec de baja velocidad binaria.
- Una o más interfaces BRI analógicas y/o RDSI.

En otras Recomendaciones IPCablecom se definen funciones adicionales del MTA.

6.1.2 Atributos de MTA

El MTA integrado está caracterizado mediante los siguientes atributos:

- Un MTA integrado tiene dos direcciones MAC, una para el CM y otra para el MTA.
- Un MTA integrado tiene dos direcciones IP, una para el CM y otra para el MTA.

- Un MTA integrado tiene dos nombres de dominio totalmente cualificados (FQDN, *fully qualified domain names*), uno para el CM y otro para el MTA.
- Al menos un número de teléfono por puerto físico configurado.
- Capacidades de dispositivo.
- El CMS asociado al MTA.

6.2 Módem de cable (CM, *cable modem*)

Un CM es un modulador/demodulador situado en las instalaciones del cliente, que proporciona transmisión de datos por la red de cable mediante el protocolo DOCSIS. En IPCablecom, el CM desempeña un papel clave en el manejo del tren de medios, y proporciona servicios tales como la clasificación del tráfico en flujos de servicio, la conformación de velocidad binaria y la puesta en cola priorizada.

6.3 Red de acceso HFC

Los servicios basados en IPCablecom son llevados por la red de acceso híbrida fibra/coaxial (HFC, *hybrid fibre/coax*). La red de acceso es un sistema bidireccional con compartición de medios constituido por el CM, el CMTS y las capas de acceso MAC y PHY DOCSIS.

6.4 Sistema de terminación de módem de cable (CMTS)

El CMTS proporciona conectividad de datos y funcionalidad complementaria a los CM mediante la red de acceso HFC. Proporciona también conectividad a redes de área extensa. El CMTS está situado en el extremo de cabecera o en el núcleo de distribución del sistema de televisión por cable.

El CMTS se encarga de las funciones siguientes:

- Proporcionar al CM la QoS requerida con arreglo a las peticiones DOCSIS, que se comprueban atendiendo a la política.
- Atribuir anchura de banda en sentido ascendente con arreglo a las peticiones del CM y a las políticas de QoS de la red.
- Clasificar cada paquete proveniente de la interfaz del lado red, y asignarlo a un nivel de QoS con arreglo a unas especificaciones de filtro definidas.
- Vigilar el campo TOS en los paquetes recibidos de la red de cable para que se cumplan los valores fijados para dicho campo conforme a la política de cada operador de red.
- Alterar el campo TOS en los encabezamientos IP de sentido descendente, con arreglo a la política del operador de la red.
- Conformar el tráfico, y realizar las tareas de vigilancia que se deriven de la especificación del flujo.
- Reenviar a la red DOCSIS paquetes descendentes utilizando la QoS asignada.
- Reenviar a los dispositivos de la red de base paquetes ascendentes utilizando la QoS asignada.
- Convertir los parámetros de puerta de QoS en parámetros DOCSIS.
- Registrar la utilización de recursos por llamada mediante mensajes de evento IPCablecom.

6.4.1 Puerta del CMTS

El CMTS se encarga de atribuir y programar la anchura de banda en los sentidos ascendente y descendente con arreglo a las peticiones del MTA y las autorizaciones de QoS establecidas por el controlador de pasarela.

El CMTS implementa una puerta de QoS dinámica IPCablecom o una puerta del CMTS entre la red de cable DOCSIS y una red de base IP. La puerta del CMTS es un componente funcional del CMTS

que realiza la clasificación del tráfico y hace cumplir la política de QoS en los trenes de medios conforme indique el controlador de puerta (GC, *gate controller*). La puerta del CMTS es controlada por el controlador de puerta (GC), que es un componente lógico de gestión de QoS del CMS que coordina todas las autorizaciones y el control de la calidad de servicio.

6.5 Servidor de gestión de llamadas (CMS)

El servidor de gestión de llamadas proporciona servicios de control de llamadas y servicios relacionados con la señalización para las pasarelas del MTA, del CMTS y de la RTPC en la red IPCablecom. El CMS es un elemento de red de confianza que reside en la porción IP gestionada de la red IPCablecom.

Un CMS IPCablecom consta de los componentes IPCablecom lógicos siguientes:

- **Agente de llamada (CMS/CA)** – El término "agente de llamada" se utiliza a menudo como sinónimo de CMS, especialmente en el MGCP. En un IPCablecom, el agente de llamada (CA, *call agent*) remite al componente de control del CMS encargado de proporcionar al MTA servicios de señalización mediante el protocolo NCS (Rec. UIT-T J.162). En ese contexto, las responsabilidades de un agente de llamada incluyen, aunque no exclusivamente, las siguientes:
 - implementar aspectos de las llamadas;
 - mantener el estado de progresión de la llamada;
 - utilizar códecs en el dispositivo MTA del abonado;
 - recoger y preprocesar los dígitos marcados;
 - recoger y clasificar las acciones del usuario.
 - controlar la utilización de la métrica de voz por el MTA.
- **Controlador de puerta (CMS/GC)** – El controlador de puerta (GC) es un componente lógico de gestión de QoS, interno al CMS, que coordina todas las autorizaciones y tareas de control de la calidad de servicio. La funcionalidad del controlador de puerta está definida en la Recomendación relativa a la calidad de servicio dinámica.

El CMS puede contener también los componentes lógicos siguientes:

- **Controlador de pasarela de medios** – El MGC es un componente lógico de gestión de señalización que se utiliza para controlar las pasarelas de medios de la RTPC. La función del MGC se define más adelante en esta misma cláusula.

El CMS puede proporcionar también las funciones siguientes:

- gestión de llamada y aspectos mejorados;
- servicios de directorio y traducción de direcciones;
- encaminamiento de llamadas;
- registro de la utilización de los servicios de portabilidad de números locales.

A los efectos de la presente Recomendación, los protocolos que implementan la funcionalidad del CMS se especifican considerando que terminan en el CMS: en la práctica, las implementaciones pueden distribuir la funcionalidad en uno o más servidores situados "detrás" del servidor de gestión de llamadas.

6.6 Pasarela RTPC

IPCablecom permite a los MTA interoperar con la actual RTPC mediante la utilización de pasarelas RTPC.

A fin de que los operadores puedan reducir a un mínimo sus costos y optimizar su interconexión con la RTPC, la pasarela RTPC se descompone en tres componentes funcionales:

- **Controlador de pasarela de medios (MGC)** – El MGC mantiene el estado de la llamada y controla el comportamiento general de la pasarela RTPC.
- **Pasarela de señalización (SG)** – La SG proporciona una función de interconexión de señalización entre la red de señalización SS7 de la RTPC y la red IP.
- **Pasarela de medios (MG)** – La MG termina los trayectos de portador y transcodifica los medios entre la RTPC y la red IP.

6.6.1 Controlador de pasarela de medios (MGC)

El controlador de pasarela de medios (MGC) recibe y sirve de mediador para la información de señalización de llamadas entre la red IPCablecom y la RTPC. Mantiene y controla el estado general de las llamadas cuando éstas requieren una interconexión con la RTPC.

El MGC controla la MG encomendando a ésta crear, modificar y suprimir conexiones que dan soporte al tren de medios en la red IP. El MGC encomienda también a la MG que detecte y genere eventos y señales tales como los tonos de prueba de continuidad de los circuitos troncales de la PU-RDSI. Cada circuito está representado como un punto extremo.

Se indica a continuación una lista de funciones desempeñadas por el controlador de pasarela de medios:

- **Función control de llamadas** – Mantiene y controla el estado general de las llamadas en la pasarela RTPC para la porción de llamada que atraviesa la pasarela RTPC. Esta función se comunica con elementos externos a la RTPC para, con arreglo a las necesidades, efectuar el control de llamadas de la pasarela RTPC, por ejemplo, generando interrogaciones de la TCAP.
- **Señalización IPCablecom** – Termina y genera la señalización de llamadas desde y hacia el lado IPCablecom de la red.
- **Control de MG** – La función control de MG ejerce un control general de los puntos extremos de la pasarela de medios:
 - Detección de eventos encomienda a la MG que detecte eventos (por ejemplo, tonos en banda) en el punto extremo y, posiblemente, en las conexiones.
 - Generación de señal encomienda a la MG que genere tonos y señales en banda en el punto extremo y, posiblemente, en las conexiones.
 - Control de conexión da instrucciones a la MG sobre el manejo básico de las conexiones desde y hacia los puntos extremos de la MG.
 - Control de atributos da instrucciones a la MG sobre los atributos que se han de aplicar a un punto extremo y/o a una conexión: por ejemplo, método de codificación, utilización de cancelación de eco, parámetros de seguridad, etc.
- **Supervisión de recursos externos** – Mantiene la visión desde el MGC de los recursos de la MG que son visibles externamente y de los recursos de la red de paquetes; por ejemplo, disponibilidad de los puntos extremos.
- **Encaminamiento de llamadas** – Toma decisiones sobre el encaminamiento de llamadas.
- **Seguridad** – Se ocupa de que todas las entidades que se comuniquen con el MGC cumplan los requisitos de seguridad.
- **Registro de utilización vía mensajes de evento** – Registra la utilización de recursos por llamada.

6.6.2 Pasarela de medios (MG)

La pasarela de medios proporciona conexiones de portador entre la RTPC y la red IP de tipo IPCablecom. Cada portador está representado como un punto extremo, y el MGC da instrucciones a la MG para que establezca y controle conexiones de medios con otros puntos extremos de la red IPCablecom. El MGC da también instrucciones a la MG para que detecte y genere eventos y señales relativos al estado de llamada conocido por el MGC.

6.6.2.1 Funciones de la pasarela de medios

Se indica a continuación una lista de funciones desempeñadas por la pasarela de medios:

- Termina y controla circuitos físicos en forma de canales portadores provenientes de la RTPC.
- Detecta eventos en los puntos extremos y conexiones conforme lo solicite el MGC.
- Genera señales en los puntos extremos y conexiones (por ejemplo, de pruebas de continuidad) conforme lo ordene el MGC.
- Crea, modifica y suprime conexiones hacia y desde otros puntos extremos conforme lo ordene el MGC.
- Controla y asigna a determinadas conexiones recursos internos para el procesamiento de medios, tras recibir peticiones del controlador de pasarela de medios.
- Realiza transcodificación de medios entre la RTPC y la red IPCablecom. Esta función abarca todos los aspectos de la transcodificación, como los códecs, la cancelación de eco, etc.
- Se encarga de que toda entidad que se comuniquen con la MG cumpla los requisitos de seguridad.
- Determina la utilización de recursos y atributos pertinentes asociados a esos recursos; por ejemplo, el número de bytes de medios enviados y recibidos.
- Informa al MGC de la utilización de los recursos de red.

6.6.3 Pasarela de señalización (SG)

La función pasarela de señalización envía y recibe señalización de la red con conmutación de circuitos en el borde de la red IPCablecom. Para IPCablecom, la función de pasarela de señalización soporta sólo señalización no asociada a las instalaciones, en la forma de SS7.

6.6.3.1 Funciones de la pasarela de señalización SS7

Se indica a continuación una lista de las funciones realizadas por la pasarela de señalización:

- Termina enlaces de señalización SS7 físicos desde la RTPC (enlaces A, F).
- Implementa aspectos de seguridad, con objeto de que la seguridad en la pasarela sea compatible con los requisitos de seguridad de la red IPCablecom y SS7.
- Termina los niveles 1, 2 y 3 de la parte transferencia de mensajes (MTP, *message transfer part*).
- Implementa las funciones necesarias de gestión de red en la MTP para cualquiera de los puntos de señalización SS7.
- Realiza el establecimiento de correspondencia de direcciones en la PU-RDSI para dar soporte a una correspondencia flexible entre los códigos de punto (tanto el código de punto de destino como el código de punto de origen) y/o las combinaciones código de punto/código CIC contenidas en los mensajes SS7 de la PU-RDSI, y el controlador de pasarela de medios (MGC) apropiado (ya sea un nombre de dominio, ya sea una dirección IP). El MGC direccionado se encargará de controlar la pasarela de medios, que termina los circuitos correspondientes.

- Realiza el establecimiento de correspondencia de direcciones en la TCAP entre combinaciones código de punto/título mundial/número de subsistema SCCP contenidas en los mensajes SS7 de la TCAP, y el controlador de pasarela de medios o el servidor de gestión de llamada apropiados.
- Proporciona un mecanismo para que ciertas entidades de confianza ("usuarios TCAP") internas a la red IPCablecom, como los agentes de llamada, interroguen bases de datos externas de la RTPC mediante mensajes TCAP enviados por la red SS7.
- Implementa el protocolo de transporte requerido para transportar la información de señalización entre la pasarela de señalización y el controlador de pasarela de medios.

6.7 Componentes auxiliares del OSS

Los equipos auxiliares del OSS contienen componentes administrativos, de servicio y de gestión de red que sirven de soporte para los procesos comerciales básicos. Tal como se define en el marco UIT de la RGT, las principales áreas funcionales del OSS son la gestión de averías, la gestión de la calidad de funcionamiento, la gestión de la seguridad, la gestión de la contabilidad, y la gestión de la configuración.

IPCablecom define un conjunto limitado de componentes funcionales del OSS y hace de interfaz para dar soporte al aprovisionamiento de dispositivos MTA y a la mensajería de eventos, con objeto de transportar información de facturación.

6.7.1 Servidor de seguridad – Centro de distribución de claves (KDC)

En IPCablecom, el término KDC se utiliza para los servidores de seguridad Kerberos. El protocolo Kerberos se utiliza con la extensión en clave pública PKINIT para la gestión de claves en las interfaces entre el MTA y el servidor de aprovisionamiento del CMS.

Tras la autenticación del MTA utilizando el protocolo PKINIT, el KDC concede tickets Kerberos al MTA. Un ticket contiene información utilizada para configurar la seguridad de la señalización de llamadas entre el MTA y el CMS (si el MTA debe comunicar con el CMS utilizando una interfaz segura) y para la interfaz de gestión entre el MTA y el servidor de aprovisionamiento (si el MTA ha de gestionarse utilizando una interfaz segura). Los tickets se expiden:

- Durante el aprovisionamiento del dispositivo. En caso de que el MTA se reinicie, y un ticket guardado es todavía válido, el MTA no tendrá que ejecutar el intercambio PKINIT para solicitar un nuevo ticket del KDC.
- Cuando expira un ticket. En circunstancias normales los tickets expiran aproximadamente cada semana.

6.7.2 Servidor de protocolo de configuración dinámico del anfitrión (DHCP, *dynamic host configuration protocol*)

El servidor DHCP es un elemento de red auxiliar utilizado durante el proceso de aprovisionamiento del dispositivo MTA para asignar dinámicamente direcciones IP y otros tipos de información sobre la configuración del cliente.

6.7.3 Servidor de sistema de nombre de dominio (DNS, *domain name system*)

El servidor DNS es un elemento de red de oficio interno utilizado para establecer correspondencias entre nombres de dominio y direcciones IP.

6.7.4 Servidor de protocolo de transferencia de ficheros trivial o servidor de protocolo de transferencia hipertexto (TFTP o HTTP, *trivial file transfer protocol or hypertext transfer protocol*)

El servidor TFTP es un elemento de red auxiliar utilizado durante el proceso de aprovisionamiento del dispositivo MTA para telecargar ficheros de configuración al MTA. Un servidor HTTP puede utilizarse en lugar de un servidor TFTP para telecargar ficheros de configuración al MTA.

6.7.5 Servidor SYSLOG (SYSLOG)

El servidor SYSLOG es un elemento opcional de una red auxiliar utilizado para almacenar los mensajes de notificación de eventos que indican que han ocurrido ciertos eventos como errores de dispositivo.

6.7.6 Servidor de mantenimiento de registros (RKS, *record keeping server*)

El RKS es un componente de confianza de un elemento de red que recibe mensajes de evento IPCablecom de otros elementos de red IPCablecom de confianza, como el CMS, el CMTS, o el MGC. El RKS es también, como mínimo, un lugar en el que almacenar durante corto tiempo mensajes de evento IPCablecom. El RKS puede reunir o correlacionar los mensajes de evento para formar conjuntos coherentes o registros de detalles de llamada (CDR, *call detail records*), que se ponen seguidamente a disposición de otros sistemas auxiliares, como los de facturación, o detección de fraudes.

6.8 Servidor de anuncios (ANS)

Un servidor de anuncios es un componente de red que gestiona y reproduce tonos y mensajes informativos en respuesta a eventos acaecidos en la red. Un servidor de anuncios (ANS) es una entidad lógica integrada por un controlador de anuncios (ANC, *announcement controller*) y un reproductor de anuncios (ANP, *announcement player*).

6.8.1 Controlador de anuncios (ANC)

El ANC inicia y gestiona todos los servicios de anuncios proporcionados por el reproductor de anuncios. El ANC solicita al ANP que reproduzca anuncios en función del estado de la llamada, conforme determine el CMS. Cuando el ANP recoge información del usuario final, el ANC se encarga de interpretar esa información, y gestiona la sesión en consonancia. Por consiguiente, el ANC puede también gestionar el estado de la llamada.

6.8.2 Reproductor de anuncios (ANP)

El reproductor de anuncios es un servidor de recursos de medios. Se encarga de recibir e interpretar instrucciones del ANC y de entregar el anuncio o anuncios apropiados al MTA. El ANP se encarga también de aceptar y notificar lo entrado por el usuario (por ejemplo, tonos DTMF). El ANP funciona bajo el control del ANC.

7 Interfaces de protocolo

Se han definido especificaciones de protocolo para la mayoría de las interfaces de los componentes de la arquitectura IPCablecom. En esta cláusula se ofrece una visión de conjunto de cada interfaz de protocolo. Para conocer los requisitos completos de cada protocolo, deberían consultarse las Recomendaciones IPCablecom.

Es posible que algunas de estas interfaces no existan en la implementación de un producto dado de un vendedor. Así, por ejemplo, si se combinan varios componentes IPCablecom funcionales, es posible que algunas de esas interfaces sean internas a ese componente.

7.1 Interfaces de señalización de llamada

La señalización de las llamadas requiere múltiples interfaces en la arquitectura IPCablecom. Estas interfaces se indican en la figura 5. Cada interfaz del diagrama lleva un texto explicativo, y se describe más ampliamente en el cuadro 2 siguiente.

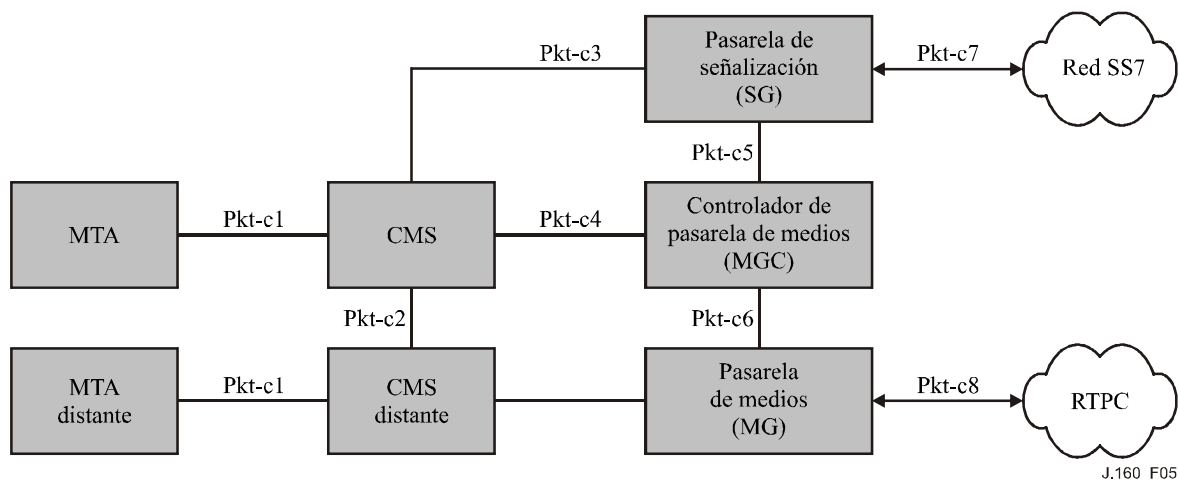


Figura 5/J.160 – Interfaces de señalización de llamada

Cuadro 2/J.160 – Interfaces de señalización de llamada

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|----------|------------------------------------|---|
| Pkt-c1 | MTA ↔ CMS | Intercambio de mensajes de señalización de llamada entre el MTA y el CMS utilizando el protocolo NCS, que es un perfil del MGCP. |
| Pkt-c2 | CMS ↔ CMS | Intercambio de mensajes de señalización de llamada entre distintos CMS. El protocolo para esta interfaz es CMSS (Rec. UIT-T J.178). |
| Pkt-c3 | CMS ↔ SG | Intercambio de mensajes de señalización de llamada entre el CMS y la SG. |
| Pkt-c4 | CMS ↔ MGC | Intercambio de mensajes de señalización de llamada entre el CMS y el MGC. El protocolo para esta interfaz es CMSS. |
| Pkt-c5 | SG ↔ MGC | Intercambio de mensajes de señalización de llamada entre el MGC y la SG. |
| Pkt-c6 | MGC ↔ MG | Interfaz para el control de la pasarela de medios utilizando el protocolo TGCP, que es un perfil de MGCP, similar al NCS. |
| Pkt-c7 | SG ↔ SS7 | La SG termina los enlaces físicos de señalización SS7 desde la RTPC (enlaces A, F). Se da soporte a los protocolos siguientes: <ul style="list-style-type: none"> Interfaz de usuario de la PU-RDSI. Proporciona una interfaz de señalización SS7 entre la PU-RDSI y los operadores de RTPC externos. Interfaz de usuario TCAP: Proporciona un mecanismo para ciertas entidades de confianza ("Usuarios TCAP") de la red IPCablecom (por ejemplo, los agentes de llamadas) con el fin de interrogar bases de datos de RTPC externas mediante mensajes TCAP enviados por la red SS7. |
| Pkt-c8 | MG ↔ RTPC | Esta interfaz define la conectividad del canal portador desde la pasarela de medios hacia la RTPC. |

7.1.1 Marco de señalización de llamadas basada en la red (NCS)

El protocolo de señalización de llamadas basada en la red (NCS, *network-based call signalling*) IPCablecom (Pkt-c1) es una variante ampliada del protocolo de señalización de llamadas MGCP del IETF. La arquitectura NCS sitúa el estado de llamada y la implementación de características en un componente centralizado, el servicio de gestión de llamadas (CMS), y sitúa en el MTA la información relativa al control de dispositivo. El MTA pasa al CMS eventos del dispositivo, y responde a las instrucciones emitidas desde el CMS. El CMS, que podría estar constituido por múltiples sistemas distribuidos geográfica o administrativamente, se encarga de establecer y retirar las llamadas, de proporcionar servicios avanzados (características de llamadas avanzadas), de efectuar la autorización de las llamadas, de generar registros de eventos de facturación, etc.

Un ejemplo de partición de función consistiría en que el CMS encomendara al MTA informar al CMS del momento en que el teléfono es descolgado y de que se ha introducido el número apropiado de dígitos en DTMF. Cuando se produce esta secuencia de eventos, el MTA notifica al CMS. El CMS puede entonces encomendar al MTA que cree una conexión, que reserve recursos de QoS mediante la red de acceso para la conexión de voz pendiente, y que haga sonar un tono paralelo generado localmente. El CMS, a su vez, se comunica con un CMS (o MGC) distante para establecer la comunicación. Cuando el CMS detecta una respuesta del extremo distante, da instrucciones al MTA para interrumpir el tono paralelo, activa la conexión de medios entre el MTA y el MTA del extremo distante, y comienza a enviar y recibir paquetes de trenes de medios.

Centralizando el estado de la llamada y el procesamiento del servicio en el CMS, el proveedor del servicio está en condiciones de gestionar centralmente la fiabilidad del servicio suministrado. Además, el suministrador del servicio adquiere pleno acceso a todo el software y el hardware si aparece un defecto que afecte a los servicios de los abonados. El software puede controlarse centralmente y actualizarse en ciclos rápidos de depuración y resolución para los que no es necesario enviar personal a las instalaciones del cliente. Además, el proveedor del servicio tiene un control directo sobre los servicios introducidos y sobre el aflujo de ingresos asociado a ese tipo de servicios.

7.1.2 Marco de señalización de la RTPC

En el cuadro 2 se resumen las interfaces de señalización de la RTPC (Pkt-c3 a Pkt-c8). Estas interfaces proporcionan acceso a servicios basados en la RTPC y a abonados RTPC desde la red IPCablecom.

El marco de señalización IPCablecom de la RTPC se compone de una pasarela RTPC subdividida en tres componentes funcionales:

- controlador de pasarela de medios (MGC);
- pasarela de medios (MG);
- pasarela de señalización (SG).

El controlador de pasarela de medios y la pasarela de medios son análogos, respectivamente, al CMS y al MTA en el marco del NCS. La pasarela de medios proporciona conectividad de portadores y de señalización en banda con la RTPC. El controlador de pasarela de medios implementa todos los estados de llamada e informaciones sobre ésta, y controla el funcionamiento de la pasarela de medios mediante el protocolo TGCP (J.171) (Pkt-c6). Este control abarca, en particular, la creación, modificación y supresión de conexiones. El TGCP es una variante ampliada del protocolo de señalización de llamada MGCP del IETF. La variante TGCP está en estrecha concordancia con el NCS.

Tanto el CMS como el MGC pueden enviar interrogaciones de encaminamiento (por ejemplo, consultas de números de llamada gratuita, o consultas de LNP) a un punto de control de servicio (SCP, *service control point*) SS7 vía la SG (Pkt-c3 y Pkt-c5). El MGC, a través de la SG,

intercambia también señalización de la PU-RDSI con las entidades SS7 de la RTPC para la gestión y control troncales.

7.1.3 Marco de señalización de CMS a CMS

IPCablecom soporta señalización CMS-CMS y CMS-MCG en un mismo dominio y entre dominios, conforme a lo definido en la Rec. UIT-T J.178, relativa a la señalización del servidor de gestión de llamadas (CMSS). La arquitectura de señalización CMSS se basa en el protocolo de iniciación de sesión (SIP, *session initiation protocol*) del IETF (IETF RFC 3261). La CMSS define un protocolo de señalización de llamada. No trata el encaminamiento en la red.

El CMS contiene un cliente de agente de usuario (UAC, *user agent client*) y servidor de agente de usuario (UAS, *user agent server*) de SIP. El agente de usuario registra el estado de la llamada durante la misma, y supervisa los cambios de estado del MTA que afecten la llamada. La interfaz entre el CMS y el MTA es la NCS. Los mensajes de la CMSS para establecer una nueva llamada, o que modifican los atributos de las partes de una llamada activa son iniciados por CMS. El CMS es a su vez impulsado a hacerlo por señalización procedente del MTA, por ejemplo, al recibir un mensaje NCS informando sobre las cifras marcadas. Un CMS incluye una función controlador de puerta (GC). La parte agente de usuario del CMS participa en la señalización CMSS y la parte controlador de puerta participa en la señalización D-QoS. Juntas controlan la coordinación de la señalización para el establecimiento de llamada y la gestión de recursos.

7.2 Trenes de medios

La norma del IETF sobre el RTP (RFC 1889 – RTP: *A Transport Protocol for Real-Time Applications*) se utiliza para transportar todos los trenes de medios en la red IPCablecom. IPCablecom utiliza el perfil RTP para los trenes de audio y vídeo, conforme se define en IETF RFC 1890 (*RTP Profile for Audio and Video Conferences with Minimal Control*).

En la figura 6 se muestran los trayectos primarios de flujos de medios en la arquitectura de red IPCablecom, que se describen más detalladamente a continuación.

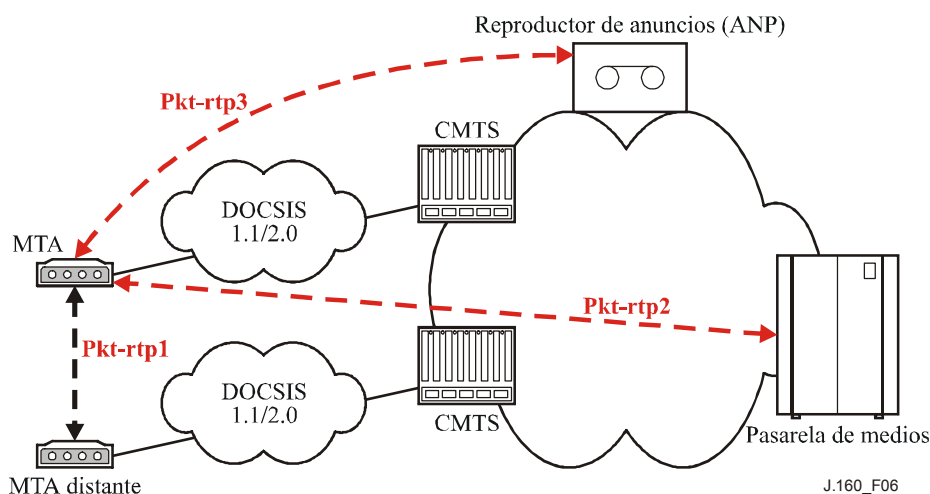


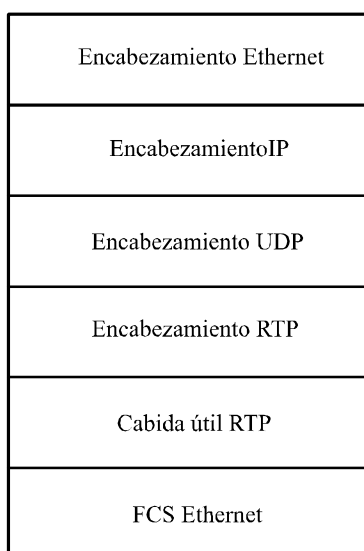
Figura 6/J.160 – Flujos de trenes de medios RTP en una red IPCablecom

Cuadro 3/J.160 – Flujos de trenes de medios RTP

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|-----------------|---|---|
| pkt-rtp1 | MTA ↔ MTA | Flujo de medios entre MTA. Incluye, por ejemplo, voz y fax codificados. |
| pkt-rtp2 | MTA ↔ MG | Flujo de medios entre la MG y el MTA. Incluye, por ejemplo, tonos, anuncios y flujo de medios RTPC. |
| pkt-rtp3 | MTA ↔ ANP | Flujo de medios entre el ANP y el MTA. Incluye, por ejemplo, tonos y anuncios enviados por el reproductor de anuncios al MTA. |

El RTP codifica un solo canal de información multimedia en un solo sentido. Dentro de cada encabezamiento RTP, un "tipo de carga útil (PT, *payload type*)" de 7 bits indica el algoritmo de codificación (por ejemplo G.711) que se utiliza dentro del paquete de carga útil. La mayoría de los algoritmos de audio comunes se asignan a determinados valores del tipo de carga útil comprendidos entre 0 y 95. La gama de 96 a 127 está reservada para tipos de carga útil "dinámicos" del RTP, en los que la vinculación entre el algoritmo de codificación y el tipo de carga útil se establece mediante señalización.

El formato de los paquetes de datos RTP transmitidos mediante IP por Ethernet se describe en la figura 7.



J.160_F07

Figura 7/J.160 – Formato de paquete RTP

En el RTP, la longitud de carga útil, así como la frecuencia con que se transmiten los paquetes, dependerán del algoritmo de codificación definido en el campo tipo de carga útil.

Las sesiones RTP son establecidas de manera dinámica por los puntos de extremo correspondientes, de modo que no es posible hablar de un número de puerto UDP "conocido", utilizado para recibir información RTP. El protocolo de descripción de sesión (SDP, *session description protocol*) fue desarrollado por el IETF con objeto de comunicar la dirección IP y el puerto UDP que utilice una sesión RTP dada. Tanto NCS como TGCP utilizan SDP.

En Ethernet, IP, UDP y RTP, la tara de los encabezamientos de paquete es considerable cuando se compara con un tamaño típico de carga útil RTP, que puede llegar a ser tan pequeño como 10 bytes para datos de voz paquetizados. En las Recomendaciones DOCSIS se hace frente a este

problema mediante una prestación de supresión de encabezamiento de cabida útil, para abreviar los encabezamientos comunes.

La Rec. UIT-T T.38 también se utiliza para transportar medios de facsímil en redes IPCablecom. En la cláusula 8.7 se dan más detalles.

7.2.1 Protocolo de control de transporte en tiempo real (RTCP)

El RTCP se define en el IETF RFC 1889. Se basa en la transmisión periódica de paquetes de control a todos los participantes de la sesión utilizando el mismo mecanismo que se usa para la distribución de los paquetes de datos. RTCP suministra información sobre la calidad de distribución de datos. Ésta es una de las funciones del RTP como protocolo de transporte y está relacionada con las funciones de control de flujo y de congestión de otros protocolos de transporte. IPCablecom soporta la utilización de RTCP en todos sus puntos extremo.

Existen extensiones del RTCP que permiten una mejor evaluación de la calidad de las llamadas de voz y diagnosticar más efectivamente los problemas de la red. Estas extensiones se denominan ampliaciones de informes del RTCP (*RTCP Extended Reports*) (RTCP XR) y se definen en el IETF RFC 3611. RTCP XR contiene muchos conjuntos de métricas, pero IPCablecom soporta únicamente las métricas de voz de RTCP XR en todos los puntos extremos.

7.3 Aprovisionamiento de dispositivo MTA

El aprovisionamiento de dispositivo MTA permite a un MTA registrarse en la red del operador y proporcionar servicios de abonado mediante la red HFC. El aprovisionamiento engloba las funciones de inicialización, autenticación y registro requeridas para el aprovisionamiento de dispositivos MTA. En la Recomendación de aprovisionamiento se incluyen también definiciones de atributo requeridas en el fichero de configuración del MTA. (Véase la figura 8.)

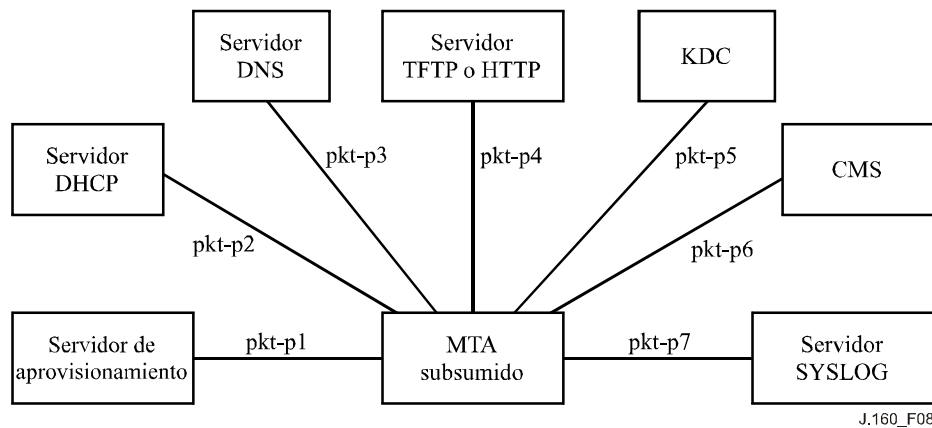


Figura 8/J.160 – Interfaces de aprovisionamiento IPCablecom

En el cuadro 4 se describen las interfaces de aprovisionamiento representadas en la figura 8.

Cuadro 4/J.160 – Interfaces de aprovisionamiento de dispositivo

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|-----------------|---|--|
| Pkt-p1 | Servidor MTA ↔ PROV | Interfaz para el intercambio de capacidad de dispositivo y de información sobre el dispositivo y punto extremo MTA entre el MTA y el servidor de aprovisionamiento utilizando el protocolo SNMP. El MTA envía asimismo notificación de que el aprovisionamiento está completado, así como de la situación pasa/falla mediante el protocolo SNMP. |
| Pkt-p2 | Servidor MTA ↔ DHCP | Interfaz DHCP entre el MTA y el servidor DHCP utilizada para asignar una dirección IP al MTA y suministrar información adicional de bajo nivel utilizada por el MTA cuando éste se incorpora a la red. |
| Pkt-p3 | Servidor MTA ↔ DNS | Interfaz DNS entre el MTA y el servidor DNS utilizada para obtener la dirección IP de un servidor IPCablecom a partir de su nombre de dominio plenamente expresado. |
| Pkt-p4 | Servidor MTA ↔ HTTP o TFTP | El fichero de configuración del MTA es telecargado al MTA desde el servidor TFTP o desde el servidor HTTP. |
| Pkt-p5 | MTA ↔ KDC | El MTA obtiene un tique Kerberos del centro de distribución de claves mediante el protocolo Kerberos. |
| Pkt-p6 | MTA ↔ CMS | El MTA establece una asociación de seguridad IPsec con el CMS mediante el protocolo Kerberos. |
| Pkt-p7 | MTA ↔ SYSLOG | Interfaz utilizada por el MTA para enviar notificaciones de eventos de red a un servidor SYSLOG y que incluye información relacionada con el estado del aprovisionamiento de dispositivo. |

7.4 Interfaces de capa de gestión de elemento SNMP

IPCablecom necesita el protocolo SNMP para establecer una interfaz entre el MTA y los sistemas de gestión de elemento, para el aprovisionamiento del dispositivo MTA. Se da soporte a las primitivas "atrapar" e "informar" de SNMPv3 para el manejo de mensajes, así como a "establecer" y "obtener" para el aprovisionamiento. En IPCablecom, la MIB de NCS contiene información de señalización de llamada de red para el aprovisionamiento, tanto por dispositivos como por puntos extremo. La MIB del MTA contiene datos para el aprovisionamiento de dispositivos y para dar soporte a funciones aprovisionadas, como la anotación cronológica de eventos. En la Recomendación relativa al marco de las MIB IPCablecom (Rec. UIT-T J.166) se encontrará información más detallada sobre las MIB.

7.5 Interfaces de mensajes de evento

7.5.1 Marco de mensajes de evento

Un mensaje de evento es un registro de datos que contiene información sobre la utilización de la red y las actividades en ésta. Un solo mensaje de evento puede contener un conjunto completo de datos sobre utilización, o puede contener sólo una parte de la información total sobre utilización. Cuando es correlacionada por el servidor de mantenimiento de registros (RKS, *record keeping server*), la información contenida en múltiples mensajes de evento proporciona un registro completo del servicio suministrado a una llamada. Este registro completo del servicio recibe frecuentemente el nombre de registro de detalles de las llamadas (CDR, *call detail record*). Pueden enviarse mensajes de evento o registro de detalles de las llamadas a una o más aplicaciones auxiliares como, por ejemplo, a un sistema de facturación, a un sistema de detección de fraudes, o a un procesador de servicios prepagados.

En la Recomendación (Rec. UIT-T J.164) sobre mensajes de evento IPCablecom se define la estructura del registro de datos de mensajes de evento y se define RADIUS como el protocolo de transporte. El formato del registro de datos de mensajes de evento ha sido diseñado para ser flexible y ampliable, a fin de llevar información sobre la utilización de la red en una gran diversidad de servicios. En la figura 9 se muestra una arquitectura representativa de mensajes de evento.

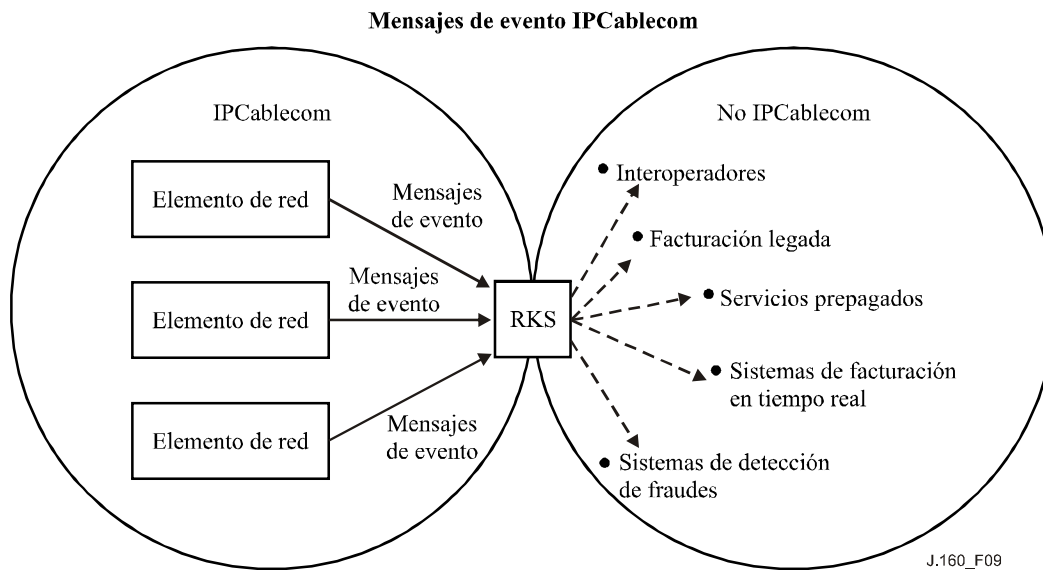
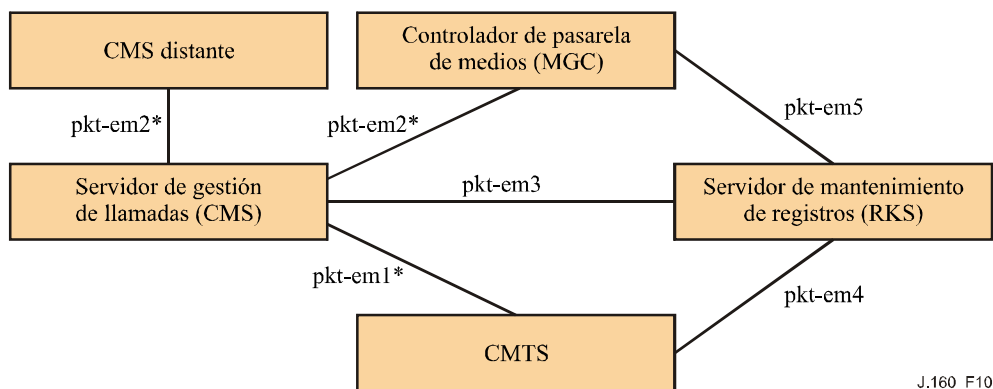


Figura 9/J.160 – Arquitectura representativa de mensajes de evento

En el cuadro 5 se describen las interfaces de mensajes de evento representadas en la figura 10.

Cuadro 5/J.160 – Interfaces de mensajes de evento

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|-----------------|---|---|
| Pkt-em1 | CMS ↔ CMTS | Mensaje establecer-puerta DQoS que lleva el identificador de correlación de facturación y otros datos requeridos para que el CMTS envíe mensajes de evento a un RKS. |
| Pkt-em2 | CMS ↔ MGC CMS ↔ CMS | El protocolo para esta interfaz es CMSS. Se utiliza para transportar el identificador de correlación de facturación y otra información requerida para los datos de facturación. |
| Pkt-em3 | CMS ↔ RKS | Protocolo RADIUS que lleva mensajes de evento IPCablecom. |
| Pkt-em4 | CMTS ↔ RKS | Protocolo RADIUS que lleva mensajes de evento IPCablecom. |
| Pkt-em5 | MGC ↔ RKS | Protocolo RADIUS que lleva mensajes de evento IPCablecom. |



J.160_F10

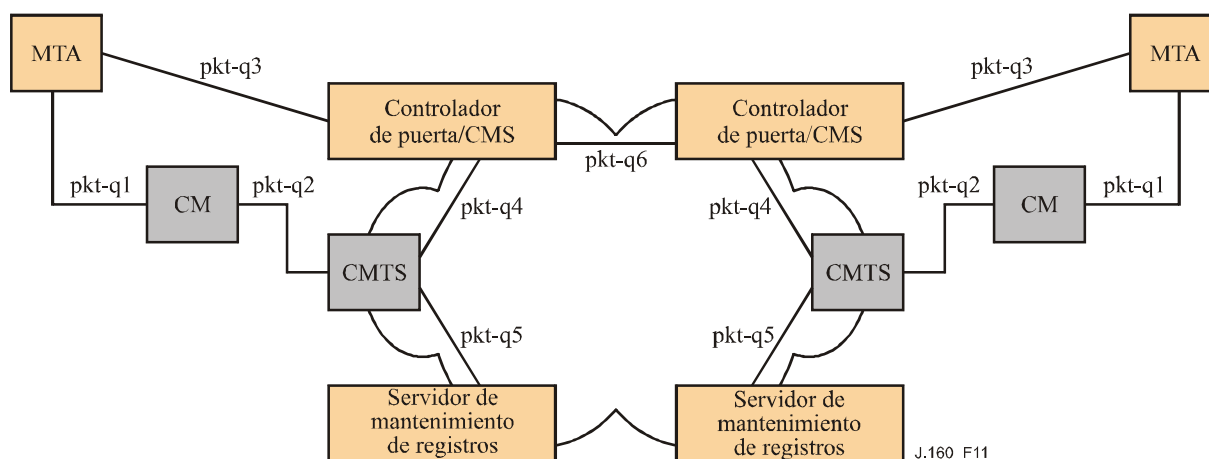
NOTA – * Indica que se utiliza la interfaz de señalización existente para transportar los datos utilizados por otras interfaces EM.

Figura 10/J.160 – Interfaces de mensajes de evento

7.6 Calidad de servicio (QoS, *quality of service*)

7.6.1 Marco de QoS

En la figura 11 se representa el marco de QoS IPCablecom:



J.160_F11

Figura 11/J.160 – Interfaces de señalización de QoS IPCablecom

En el cuadro 6 se identifica sucintamente cada una de las interfaces, así como la manera en que se utilizan en la Recomendación de QoS dinámica (DQoS, *dynamic QoS*, Rec. UIT-T J.163).

Cuadro 6/J.160 – Interfaces de QoS para los MTA autónomos e integrados

| Interfaz | Componentes funcionales IPCablecom | Descripción de DQoS |
|----------|------------------------------------|--|
| Pkt-q1 | MTA ↔ CM | E-MTA subsumido, interfaz de servicio de control MAC |
| Pkt-q2 | CM ↔ CMTS | J.112, iniciado por el CM |
| Pkt-q3 | MTA ↔ CMS | NCS |
| Pkt-q4 | GC ↔ CMTS | Gestión de puerta |

Cuadro 6/J.160 – Interfaces de QoS para los MTA autónomos e integrados

| Interfaz | Componentes funcionales IPCablecom | Descripción de DQoS |
|----------|------------------------------------|---------------------------|
| Pkt-q5 | CMTS ↔ RKS | Facturación |
| Pkt-q6 | CMS ↔ CMS | Establecimiento de sesión |

La función de cada interfaz de QoS se describe más ampliamente en el cuadro 7.

Cuadro 7/J.160 – Interfaces de QoS

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|----------|------------------------------------|--|
| Pkt-q1 | MTA ↔ CM | <p>Esta interfaz se descompone en tres subinterfaces:</p> <p><i>Control:</i> utilizada para gestionar los flujos de servicio DOCSIS, junto con los correspondientes parámetros de tráfico y reglas de clasificación de QoS.</p> <p><i>Sincronización:</i> utilizada para sincronizar paquetes y para planificar la minimización del retardo y de la fluctuación de fase.</p> <p><i>Transporte:</i> utilizada para procesar paquetes del tren de medios y para realizar un procesamiento adecuado de QoS por paquetes.</p> <p>La interfaz MTA/CM se define conceptualmente en la Rec. UIT-T J.112.</p> |
| Pkt-q2 | CM ↔ CMTS | <p>Es la interfaz de QoS DOCSIS (control, planificación y transporte). Conviene observar que, en lo relativo a la arquitectura, las funciones de control pueden ser iniciadas únicamente por el CM. El CMTS es el árbitro final respecto de la aplicación de políticas, y el que concede la admisión a la red de acceso DOCSIS. En IPCablecom se utilizan las capacidades siguientes del MAC DOCSIS:</p> <ul style="list-style-type: none"> • Multiplicidad de flujos de servicio, cada uno de ellos con su propia clase de tráfico ascendente, con una o varias conexiones de voz por flujo de servicio DOCSIS. • Clasificación priorizada de los trenes de tráfico en función de los flujos de servicio. • Servicio garantizado de planificación de velocidad binaria mínima/constante. • Planificación de velocidad binaria constante con servicio de detección de actividad de tráfico (disminución de velocidad, aumento de velocidad, detención y reiniciación de la planificación). • Supresión de encabezamientos de paquete DOCSIS para aumentar la densidad de llamadas. • Clasificación DOCSIS de flujos de voz en flujo de servicio. • Sincronización DOCSIS del CÓDEC con el reloj CMTS y del intervalo de concesión. • Activación en dos fases de los recursos de QoS. • Marcado de paquetes TOS en la capa de red. • Garantías respecto del retardo y la fluctuación de fase. • Señalización de subcapa interna entre el MTA IPCablecom y el CM (MTA integrado). <p>Esta interfaz se define más detalladamente en la Rec. UIT-T J.112.</p> |

Cuadro 7/J.160 – Interfaces de QoS

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|-----------------|---|---|
| Pkt-q3 | MTA ↔ CMS | Interfaz de señalización entre el MTA y el CMS. A través de esta interfaz se señalizan numerosos parámetros, como tren de medios, direcciones IP, números de puerto y la selección de códec y paquetización. |
| Pkt-q4 | CMS ↔ CMTS | Esta interfaz se utiliza para gestionar las puertas dinámicas para las sesiones de trenes de medios. Esta interfaz permite a la red IPCablecom solicitar y autorizar QoS. |
| Pkt-q5 | CMTS ↔ RKS | Esta interfaz es utilizada por el CMTS para informar las modificaciones de recursos de QoS utilizados por una llamada. Esta interfaz se define en la Recomendación relativa a los mensajes de evento. |
| Pkt-q6 | CMS ↔ CMS | Esta interfaz se utiliza para establecer sesiones dentro de un dominio y entre dominios. Incluye funcionalidad para asegurar que se dispone de recursos de QoS en ambos extremos de la conexión antes que se permita concluir la llamada. |

7.6.2 Calidad de servicio dinámica

La QoS dinámica (DQoS) IPCablecom utiliza la información de señalización de llamadas en el momento en que se efectúa la llamada para autorizar dinámicamente recursos con destino a dicha llamada. La QoS dinámica permite evitar diversos tipos de ataques de apropiación indebida de servicio integrando los mensajes de QoS con otros protocolos y elementos de red. Los elementos de red necesarios para controlar la QoS dinámica se indican en la figura 11.

En el CMTS, la entidad lógica que define la clasificación del tráfico y la política de QoS en los trenes de medios se denomina puerta. El elemento controlador de puerta del CMS gestiona puertas para los trenes de medios IPCablecom. En la señalización entre el GC y el CMTS se incluye la información esencial siguiente:

Envolvente de QoS máxima permitida – La envolvente de QoS máxima permitida define los recursos de QoS máximos (por ejemplo, "2 concesiones de 160 bytes por cada 10 ms") que se permite que el MTA solicite para un flujo dado de portador de trenes de medios. Si el MTA solicita un valor superior a los parámetros contenidos en la envolvente, la petición será denegada.

Identidad de los puntos de extremo del tren de medios – El GC/CMS autoriza a las partes que intervienen en un flujo de portadora de trenes de medios. Utilizando esa información, el CMTS puede vigilar el tren de datos para asegurarse de que su destino y origen son las partes autorizadas a tal efecto.

Destino de la información de facturación – El GC/CMS informa al CMTS de la identidad de los servidores de mantenimiento de registros primarios y secundarios y provee una identificación de facturación única que posibilita la correlación de registros en los diversos elementos de red.

El papel que cada uno de los componentes de IPCablecom desempeña en la implementación de DQoS es el siguiente:

Servidor de gestión de llamadas/controlador de puerta – El CMS/GC se encarga de la autorización de QoS. La autorización de QoS puede depender del tipo de llamada, del tipo de usuario, o de otros parámetros definidos mediante políticas. El CMS/GC también utiliza CMSS para asegurar que los recursos de QoS estén disponibles en ambos extremos de la llamada en caso de una llamada en el mismo dominio o entre dominios.

CMTS – Utilizando información suministrada por el CMS/GC, el CMTS realiza el control de admisión de las peticiones de QoS y posteriormente vigila el tren de datos admitido para asegurarse de que el origen y el destino del tren de datos corresponda a las partes que fueron autorizadas como puntos extremos de este tren. El CMTS interactúa con la porción CM del MTA y con el RKS. Las responsabilidades del CMTS con respecto a cada uno de esos elementos son:

- **Del CMTS al servidor de mantenimiento de registros** – El CMTS actualiza el servidor de mantenimiento de registros (RKS) cada vez que hay un cambio en la QoS entre el CMTS y el MTA para una determinada llamada.
- **Del CMTS al MTA** – El MTA efectúa peticiones dinámicas para la creación y modificación de los parámetros de tráfico de QoS asociados con los flujos de servicio dinámicos DOCSIS que transportan el tráfico de portador. Cuando el CMTS recibe una petición, comprueba si las características solicitadas están dentro de la envolvente de QoS autorizada y si los puntos de extremo del tren de medios están autorizados a transportar este tráfico. Si las comprobaciones son exitosas, el CMTS crea o modifica adecuadamente el flujo de servicio dinámico.

Servidor de mantenimiento de registros (RKS) – El RKS recibe cada evento (en la forma de un mensaje de evento) enviado por el CMTS. El RKS normalmente posee una interfaz con uno o varios sistemas auxiliares y adecua el formato y retransmite la información recibida del CMTS hacia estos otros sistemas.

MTA – El MTA es la entidad a la cual la red de acceso proporciona el acuerdo de nivel de servicio. El MTA debe velar por el uso adecuado del enlace de QoS (y el CMTS por la introducción de ese uso adecuado, ya que el MTA no es un dispositivo confiable). Si el MTA intenta exceder la envolvente autorizada en el acuerdo de nivel de servicio, el CMTS asegura que el MTA no recibirá la QoS en exceso que solicitó.

7.7 Aproveccionamiento de abonados del CMS

La Recomendación relativa al aprovisionamiento de abonados del CMS proporciona un medio para la activación del servicio automatizado definiendo una interfaz entre el servidor de aprovisionamiento (o entre un componente auxiliar autorizado) y el CMS. El marco para el aprovisionamiento de abonados del CMS se representa en la figura 12.

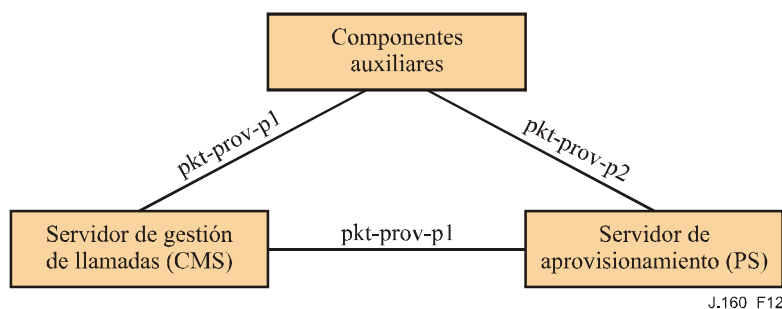


Figura 12/J.160 – Interfaces de aprovisionamiento de abonados

La función de cada interfaz de aprovisionamiento de abonado del CMS se detalla en el cuadro 8.

Cuadro 8/J.160 – Interfaces de aprovisionamiento de abonados del CMS

| Interfaz | Componentes funcionales | Descripción |
|-----------------|--------------------------------------|--|
| pkt-prov-p1 | PS-CMS Componentes auxiliares-CMS | Se trata de la interfaz de aprovisionamiento de los abonados del CMS. La información de abonado puede ser suministrada al CMS por el PS o por un componente auxiliar autorizado. |
| pkt-prov-p2 | Componentes auxiliares-PS | Estas interfaces permiten a los componentes auxiliares que intercambien información con el servidor de aprovisionamiento. Esta interfaz no se define en IPCablecom. |

El aprovisionamiento de abonado está compuesto por:

- **Soporte del registro/facturación del cliente** – Establecimiento de un registro de clientes que contiene la información necesaria para suministrar el servicio, facturar y percibir pagos del cliente. La creación/facturación de un registro de cliente se considera parte de la aplicación OSS auxiliar y actualmente cae fuera del ámbito de IPCablecom.
- **Establecimiento/configuración del equipo** – Puede incluir la instalación y/o conexión física de equipo así como las actualizaciones de software y/o bases de datos necesarias para suministrar efectivamente el servicio al cliente. Con respecto a la interfaz de aprovisionamiento del abonado del CMS, el establecimiento del equipo afecta al CMS. El aprovisionamiento del CMS en sí puede descomponerse en dos áreas principales:
 - **Aprovisionamiento del servicio telefónico tradicional (POTS) básico (BPP)** – El BPP provee al CMS el conjunto mínimo de datos necesarios para el encaminamiento del servicio telefónico básico (POTS) por la red IPCablecom. Ese conjunto mínimo de datos está compuesto por un número telefónico al que se hace corresponder con el FQDN de su MTA asociado y por un identificador de punto extremo NCS. Estos datos se utilizarán para establecer tablas de conversión que permitan al CMS encaminar llamadas al dispositivo/puerto adecuado mediante un número de teléfono concreto. Es necesario el aprovisionamiento del BPP para cada cliente antes que éste pueda recibir llamadas en una red IPCablecom.
 - **Aprovisionamiento de características de llamada (CFP, *call feature provisioning*)** – Además del BPP, se efectúa el CFP para suministrar características de llamada a un cliente. El CFP es más complicado que el BPP ya que los parámetros transmitidos pueden variar con cada característica y también depender de las diferentes implementaciones de los fabricantes.

7.8 Vigilancia electrónica

El marco de vigilancia electrónica de IPCablecom permite la vigilancia electrónica autorizada legalmente (LAES, *lawfully authorized electronic surveillance*) en redes IPCablecom. IPCablecom soporta el suministro de datos de llamada y de contenido de llamadas a los organismos encargados de aplicar la ley (LEA, *law enforcement agencies*). Los datos de llamadas y los contenidos de llamadas se suministran desde diversos componentes de la red a una función de entrega (DF, *delivery function*). La DF se encarga de recolectar los datos de llamada y de los contenidos de llamada para luego entregarlos al LEA adecuado. El LEA utiliza una función de recopilación que se encarga de recibir los datos de llamada y los contenidos de llamada de la DF.

IPCablecom sólo define los mecanismos para efectuar la vigilancia electrónica. No define cómo se administra una orden de vigilancia electrónica (es decir, cómo es aceptada por el operador de IPCablecom y provisionada en la red).

El marco de vigilancia electrónica de IPCablecom se representa en la figura 13.

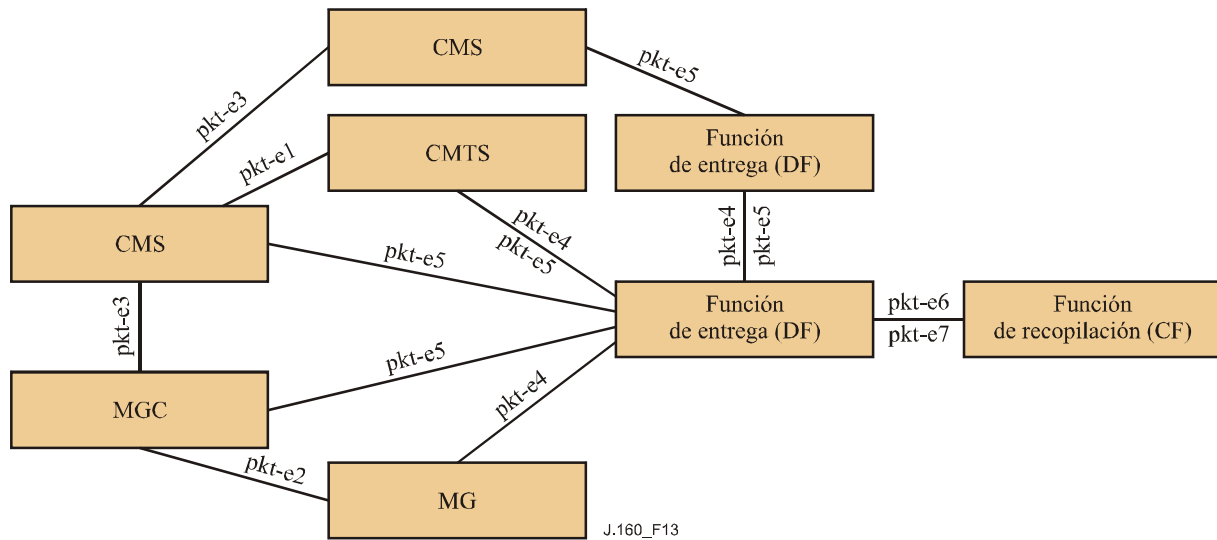


Figura 13/J.160 – Interfaces de vigilancia electrónica

La función de cada interfaz de vigilancia electrónica se describe en el cuadro 9.

Cuadro 9/J.160 – Interfaces de vigilancia electrónica

| Interfaz | Componentes funcionales de IPCablecom | Descripción |
|----------|--|--|
| pkt-e1 | CMS ↔ CMTS | Ésta es la interfaz DQoS del COPS, que permite a un CMS habilitar la vigilancia de datos de llamada y de contenido de llamada. |
| pkt-e2 | MGC ↔ MG | Esta interfaz es TGCP, que permite a un MGC ordenar a la MG para que efectúe la vigilancia electrónica. |
| pkt-e3 | CMS ↔ CMS CMS ↔ MGC | Esta interfaz es el CMSS, que soporta la posibilidad de comunicar las necesidades de vigilancia electrónica en el caso de ciertos escenarios de llamadas en el mismo dominio y entre dominios (por ejemplo, si el sujeto reenvía una llamada). |
| pkt-e4 | CMTS ↔ DF MG ↔ DF DF ↔ DF | Esta interfaz se basa en la mensajería de eventos IPCablecom y se utiliza para suministrar datos de llamada de componentes de IPCablecom a la DF, o de una DF a otra. |
| pkt-e5 | CMTS ↔ DF MGC ↔ DF DF ↔ DF CMS ↔ DF | Esta interfaz se utiliza para suministrar contenidos de llamada en la forma de paquetes RTP encapsulados de componentes de IPCablecom a la DF, o de una DF a otra. |
| pkt-e6 | DF ↔ CF | Esta interfaz se utiliza para suministrar datos de llamada a la CF. |
| pkt-e7 | DF ↔ CF | Esta interfaz se utiliza para suministrar contenidos de llamada a la CF. |

7.9 Seguridad

7.9.1 Panorámica

Cada una de las interfaces de protocolo de IPCablecom está expuesta a amenazas que pueden entrañar peligro tanto para el abonado como para el proveedor del servicio. La arquitectura IPCablecom trata de contrarrestar esas amenazas especificando, para cada interfaz de protocolo definida, los mecanismos de seguridad subyacentes (como, por ejemplo, IPsec) que proporcionan a la interfaz de protocolo los servicios de seguridad que necesita.

En la mayoría de las interfaces, IPCablecom exige que se utilicen el o los mecanismos de seguridad definidos; en algunas interfaces la arquitectura permite que los operadores utilicen enlaces no seguros, aunque actuando así el operador expondrá a los abonados y a sí mismo a ataques que se contrarrestarían cuando los enlaces están asegurados por los mecanismos definidos en la Recomendación relativa a seguridad de IPCablecom (Rec. UIT-T J.170).

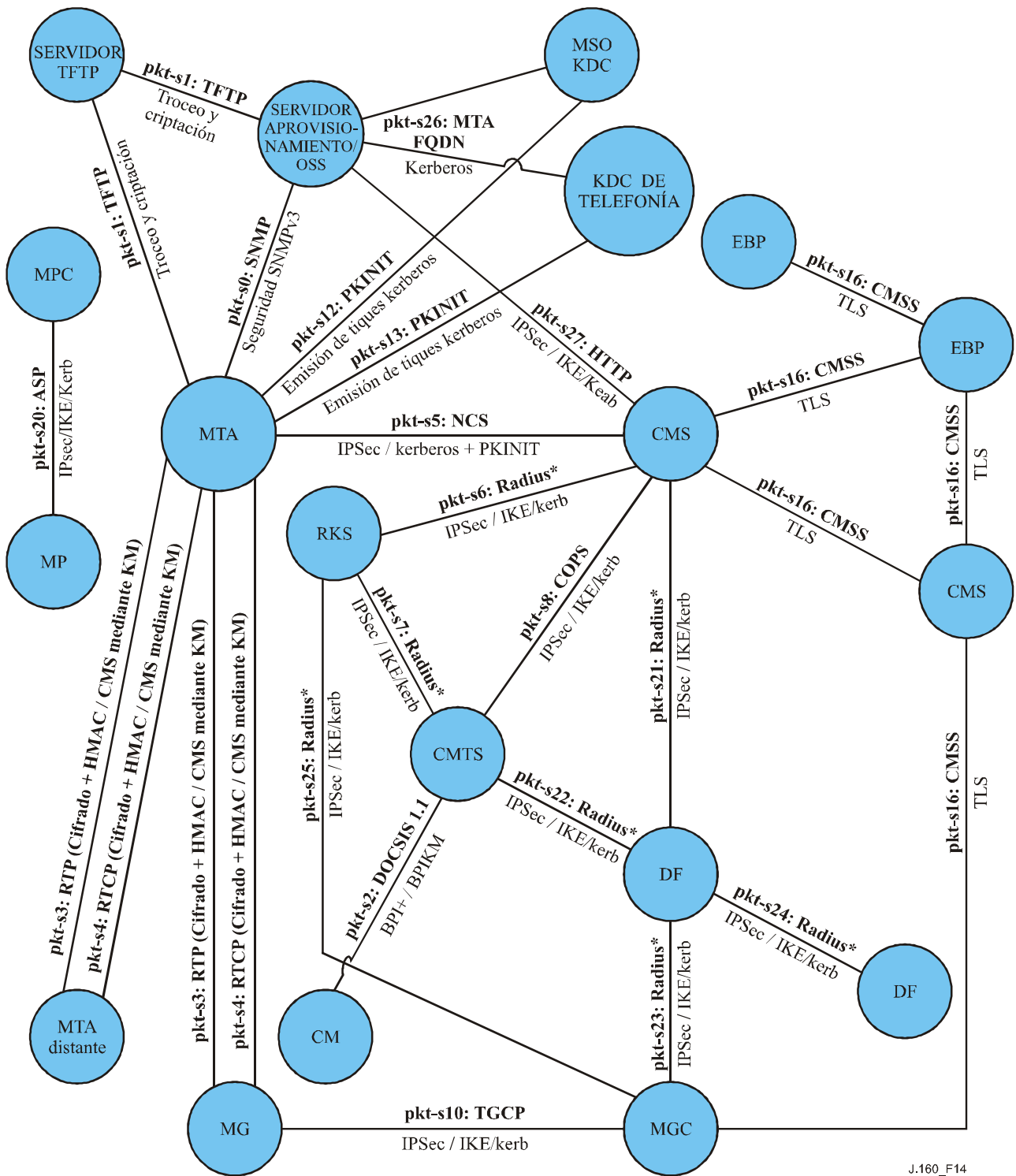
Los servicios de seguridad disponibles mediante la capa de servicio básica de IPCablecom son los de autenticación, control de acceso, integridad y confidencialidad. Una interfaz de protocolo IPCablecom puede utilizar cero, uno o más de esos servicios para atender a sus necesidades de seguridad particulares.

La seguridad IPCablecom subviene a las necesidades de seguridad de cada interfaz de protocolo constituyente:

- identificando el modelo de amenaza específico para cada interfaz de protocolo constituyente;
- identificando los servicios de seguridad (autenticación, autorización, confidencialidad, integridad, y no repudio) necesarios para hacer frente a las amenazas identificadas;
- especificando el mecanismo de seguridad que proporciona los servicios de seguridad requeridos.

Entre los mecanismos de seguridad se incluyen el protocolo de seguridad (por ejemplo, IPsec, seguridad de capa RTP o seguridad SNMPv3) y el protocolo de gestión de claves que le da soporte (por ejemplo, IKE o PKINIT/Kerberos).

En la figura 14 se ofrece un resumen de todas las interfaces de seguridad IPCablecom.



J.160_F14

Figura 14/J.160 – Interfaces de seguridad IPCablecom

En la figura 14, los textos que etiquetan las interfaces reflejan la estructura siguiente:

<etiqueta>: <protocolo> { <protocolo de seguridad> / <protocolo de gestión de claves> }

Cuando el protocolo de gestión de claves no está indicado, es porque no es necesario para esa interfaz. Las interfaces de IPCablecom en las que no se requiere seguridad no se han representado en la figura 14.

En el cuadro 10 se describe cada una de las interfaces representadas en la figura 14.

Cuadro 10/J.160 – Interfaces de seguridad

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|-----------------|---|---|
| Pkt-s0 | MTA ↔ PS/OSS | Inmediatamente después de la secuencia DHCP en el flujo de aprovisionamiento seguro, el MTA efectúa, con el servidor de aprovisionamiento, la gestión de clave basada en Kerberos para establecer las claves de SNMPv3. El MTA omite el SNMPv3 basado en Kerberos y utiliza SNMPv2c en los flujos básico e híbrido. |
| Pkt-s1 | MTA ↔ TFTP o PS/OSS | Telecarga de ficheros de configuración del MTA. Cuando el servidor de aprovisionamiento en flujo de aprovisionamiento seguro envía una instrucción SNMP Set al MTA, incluye el nombre de la configuración y el troceo del fichero. Más adelante, cuando el MTA telecarga el fichero, autentica el fichero de configuración utilizando el valor de troceo. El fichero de configuración puede ser opcionalmente criptado. Puede utilizarse HTTP en vez de TFTP. |
| Pkt-s2 | CM ↔ CMTS | Esta interfaz debería asegurarse con BPI+ utilizando gestión de claves BPI. En el enlace HFC se provee privacidad BPI+. |
| Pkt-s3 | MTA ↔ MTA MTA ↔ MG | RTP: Paquetes de medios de extremo a extremo entre dos MTA, o entre un MTA y una MG. Los paquetes RTP son criptados directamente con el cifrado escogido. Opcionalmente podría proporcionarse integridad de mensajes mediante un MAC MMH. Las claves se generan aleatoriamente, y son intercambiadas por los dos puntos extremos dentro de los mensajes de señalización a través del CMS u otro servidor de aplicación. |
| Pkt-s4 | MTA ↔ MTA MTA ↔ MG | Protocolo de control RTCP para el RTP. Integridad de mensajes y criptación por cifrado seleccionado. Las claves RTCP se calculan utilizando el mismo secreto negociado durante la gestión de claves RTP. No se necesitan ni se utilizan mensajes de gestión de claves adicionales. |
| Pkt-s5 | MTA ↔ CMS | Integridad de mensajes y privacidad mediante IPsec. La gestión de claves se realiza mediante Kerberos, con la extensión PKINIT (autenticación inicial de clave pública). |
| Pkt-s6 | RKS ↔ CMS | RADIUS: Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE o Kerberos. |
| Pkt-s7 | CMTS ↔ RKS | Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE- o Kerberos. |
| Pkt-s8 | CMS ↔ CMTS | Protocolo COPS entre el GC y el CMTS, utilizado para telecargar autorización de QoS al CMTS. Integridad de mensajes y privacidad proporcionadas mediante IPsec. La gestión de claves es IKE- o Kerberos. |
| Pkt-s10 | MGC ↔ MG | TGCP: Interfaz de IPCablecom con la pasarela de medios RTPC. Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE- o Kerberos. |

Cuadro 10/J.160 – Interfaces de seguridad

| Interfaz | Componentes funcionales IPCablecom | Descripción |
|-----------------|---|---|
| Pkt-s12 | MTA ↔ MSO KDC | PKINIT: Se envía un mensaje AS-REQ al KDC utilizando criptografía de claves públicas para la autenticación. El KDC verifica el certificado y emite un tique de servicio o un tique de concesión de tique (TGT, <i>ticket granting ticket</i>), dependiendo del contenido de la petición AS. La respuesta AS devuelta por el KDC contiene una cadena de certificado y una signatura digital que son utilizados por el MTA para autenticar este mensaje. En caso de que el KDC devuelva un TGT, el MTA envía una petición TGS al KDC a la que el KDC contesta con una respuesta TGS que contiene un tique de servicio. Los mensajes petición/respuesta del TGS se autentican utilizando una clave de sesión simétrica contenida en el TGT. |
| pkt-s13 | MTA ↔ KDC de telefonía | PKINIT: Véase pkt-s12. Esta interfaz se muestra separadamente debido a que se utiliza un KDC distinto para suministrar servicios de autenticación al servicio de telefonía. |
| pkt-s16 | CMS ↔ CMS CMS ↔ MGC CMS ↔ EBP EBP ↔ EBP | SIP: Se utiliza TLS para la integridad de mensajes y la privacidad. Se utilizan certificados para la autenticación mutua durante la toma de contacto TLS. |
| pkt-s20 | MPC ↔ MP | ASP: Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE o Kerberos. |
| pkt-s21 | DF ↔ CMS | RADIUS: Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE o Kerberos. |
| pkt-s22 | DF ↔ CMTS | RADIUS: Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE o Kerberos. |
| pkt-s23 | DF ↔ MGC | RADIUS: Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE o Kerberos. |
| pkt-s24 | DF ↔ DF | RADIUS: Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE+. |
| pkt-s25 | RKS ↔ MGC | RADIUS: Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE o Kerberos. |
| pkt-s26 | OSS/servidor de aprovisionamiento – KDC del MSO OSS/servidor de aprovisionamiento – KDC de telefonía | El KDC utiliza Kerberos para hallar la correspondencia de la dirección MAC del MTA con su FQDN a fin de autenticar el MTA antes de emitir un tique. |
| Pkt-s27 | CMS ↔ PS/OSS | HTTP. Se utiliza IPsec para la integridad de mensajes y la privacidad. La gestión de claves es IKE o Kerberos. |

7.9.2 Seguridad del aprovisionamiento de dispositivo

IPCablecom permite el aprovisionamiento de dispositivos en modo no seguro o en modo seguro. IPCablecom también permite la gestión SNMPv2 no segura después de que se haya aprovisionado el MTA de forma segura. Dado que esta sección de esta Recomendación se especializa en seguridad, suponemos que la red está funcionando en modo seguro.

La arquitectura de seguridad IPCablecom divide el aprovisionamiento de dispositivos en tres actividades diferenciadas: incorporación del abonado, aprovisionamiento de dispositivo y autorización de dispositivo.

7.9.2.1 Incorporación del abonado

El proceso de incorporación de un abonado establece una cuenta permanente de facturación de abonado que identifica de modo único al MTA ante el CMS mediante la dirección MAC del MTA. La cuenta de facturación se utiliza también para identificar los servicios suscritos por el abonado en relación con el MTA.

La incorporación del abonado puede producirse en banda o fuera de banda. En la práctica, la especificación del proceso de incorporación del abonado queda fuera del alcance de IPCablecom, y puede ser diferente para cada proveedor de servicio.

7.9.2.2 Aprovisionamiento del dispositivo

El dispositivo MTA se autentica a sí mismo ante el KDC utilizando la extensión PKINIT a Kerberos. Tras comprobar las credenciales de autenticación y garantizar que el sistema de aprovisionamiento auxiliar reconoce el MTA, el KDC emite un tique para el servidor de aprovisionamiento. El MTA utiliza el tique para intercambiar claves SNMPv3 de forma segura con el servidor de aprovisionamiento. Una vez se ha establecido una sesión SNMPv3 segura, el MTA pide su fichero de configuración (que es autenticado y puede ser criptado) de un servidor TFTP o HTTP.

7.9.2.3 Aprovisionamiento dinámico

Para aprovisionar y gestionar dinámicamente capacidades de comunicación de voz y otros aspectos del MTA, se utilizará seguridad SNMPv3.

7.9.2.4 Autorización del dispositivo

La autorización del dispositivo se produce cuando un dispositivo del MTA aprovisionado se autentica ante el servidor de gestión de llamada y establece una asociación de seguridad con dicho servidor antes de entrar plenamente en servicio. La autorización del dispositivo permite proteger la señalización de llamada posterior conforme a la asociación de seguridad establecida.

El dispositivo MTA se autentica a sí mismo al KDC utilizando la extensión PKINIT a Kerberos. Tras comprobar las credenciales de autenticación y asegurar que el MTA es conocido para el sistema de aprovisionamiento auxiliar, el KDC emite un tique para el CMS. El MTA utiliza el tique para establecer un conducto lógico al CMS de forma segura. En el conducto lógico IPsec se puede utilizar criptación nula, en cuyo caso los mensajes de señalización NSC viajan sin criptar a través de esta interfaz.

7.9.2.5 Seguridad de señalización

Todo el tráfico de señalización, incluida la señalización de QoS, la señalización de llamada y la señalización con la interfaz de pasarela RTPC, viaja a través de conductos lógicos IPsec. La gestión de la asociación de seguridad IPsec se produce mediante alguna combinación de Kerberos e IKE. Se utiliza Kerberos con las extensiones PKINIT para intercambiar claves entre clientes MTA y su servidor CMS; IKE, u opcionalmente se utilizará Kerberos para gestionar todas las demás asociaciones de seguridad de señalización IPsec.

7.9.2.6 Seguridad del tren de medios

Durante el establecimiento de la comunicación los MTA negocian un algoritmo de criptación determinado para el flujo de portador. Como mínimo se requiere que los dispositivos soporten criptación nula y criptación AES. La criptación se aplica al contenido del paquete RTP, pero no a su encabezamiento.

Cada paquete RTP puede contener un código de autenticación de mensajes (MAC) opcional basado en el algoritmo MMH. La computación MAC incluye el encabezamiento sin criptar del paquete y la cabida útil criptada (o no criptada).

Las claves para la criptación y cálculo MAC se obtienen del secreto de extremo a extremo, intercambiado entre el MTA enviante y el MTA receptor en el proceso de señalización de la llamada durante el establecimiento de la comunicación. Así, los intercambios de claves para la seguridad del tren de medios están también protegidos por el nivel de seguridad que ofrece el transporte IPsec que asegura la señalización de la llamada.

7.9.2.7 OSS y seguridad del sistema de facturación

Los agentes SNMP de los MTA IPCablecom utilizan SNMPv3 cuando funcionan en modo seguro. El modelo de seguridad de usuario de SNMPv3 (RFC 3414) proporciona servicios de autenticación y privacidad para el tráfico SNMP. Para controlar el acceso a los objetos MIB puede utilizarse el control de acceso de SNMPv3 basado en la inspección (RFC 3415).

El protocolo de gestión de claves IKE o Kerberos se utiliza para establecer claves de criptación y autenticación entre el servidor de mantenimiento de registros (RKS) y cada uno de los elementos de red IPCablecom que genera mensajes de evento. Se requiere que los dispositivos conformes con la Recomendación sobre seguridad de PacketCable implementen IKE con claves previamente compartidas; también pueden implementar IKE con certificados o Kerberos, lo que permitirá que los fabricantes utilicen mecanismos de intercambio de claves completamente automáticos. Los mensajes de evento son enviados desde el CMS y el CMTS al RKS mediante el protocolo de transporte RADIUS, que, a su vez, se dota de seguridad mediante IPsec.

8 Consideraciones sobre el diseño de red

8.1 Cuestiones relativas al mantenimiento del tiempo y a las notificaciones

A fin de mantener la calidad del servicio, se recomienda decididamente que todos los relojes del equipo de la red se mantengan a no más de 200 milisegundos del tiempo universal coordinado (UTC, *universal time coordinated*). Se requiere que los dispositivos que envían mensajes de eventos se mantengan sincronizados utilizando el protocolo de señales horarias de red (NTP, *network time protocol*) (conforme a la RFC 1119).

Se recomienda que las redes IPCablecom mantengan un servidor NTP cuya exactitud no exceda de un intervalo especificado respecto del tiempo universal coordinado (UTC).

8.2 Temporización para alinear el tampón de reproducción de sonido con la tasa de codificación

El equipo de generación de paquetes y el equipo de manejo de paquetes suelen operar con relojes no controlados. La naturaleza plesiócrona de estos relojes puede entrañar problemas a la hora de ofrecer servicios isócronos. La diferencia entre las velocidades de reloj de estas entidades plesiócronas suele manifestarse en una sobreutilización o infrautilización de los tampones de reproducción.

A fin de reducir al mínimo la aparición de esas situaciones, todos los CMTS deberían acoplar sus velocidades de transmisión hacia adelante a un reloj obtenido de una fuente que refleje un reloj Stratum-3. Los MTA deberían utilizar la velocidad de transmisión hacia adelante para obtener el reloj mediante el que se determinará el periodo de paquetización. Los MTA deberían utilizar también ese reloj para determinar la velocidad de reproducción desde el tampón de recepción.

8.3 Direccionamiento IP

Un MTA es una entidad multifuncional, una de cuyas funciones es necesaria para la administración del CM, mientras que la otra es la función del propio MTA.

Todos los MTA IPCablecom tienen que tener dos direcciones IP – una para el CM, y otra para el MTA. Todos los MTA integrados IPCablecom tienen que tener dos direcciones MAC – una para el CM, y otra para el MTA. IPCablecom soporta únicamente direcciones IPv4.

Los requisitos siguientes pueden satisfacerse utilizando la configuración de dirección IP dual:

- El operador IPCablecom puede asignar una dirección IP privada para la función anfitrión del CM, en aquellos casos en que ningún otro ejemplar de la red IPCablecom disponga de NAT.
- Con dos direcciones IP por MTA, el operador de IPCablecom puede encaminar los paquetes del servicio vocal por una red medular de voz, y todos los demás paquetes (datos) por una red medular de datos. En este caso, la red medular de encaminamiento deberá estar configurada de manera que se sigan trayectos diferentes para cada una de las dos direcciones IP de destino.
- El operador IPCablecom puede simplificar las funciones de administración y gestión del lado red utilizando direcciones IP diferentes. Por ejemplo, pueden instalarse filtros de políticas que bloqueen o que permitan el paso de tráfico del componente MTA del dispositivo. Además, los proveedores de servicio de red pueden proporcionar servicios de cribado de direcciones fuente, y pueden obtenerse estadísticas y diagnósticos sobre el tráfico de la red en base a la dirección IP del MTA.

Las direcciones IP duales suscitan consideraciones especiales que afectan a:

- la implementación de la pila de protocolos IP del MTA,
- la implementación del OSS IPCablecom, y de protocolos de aprovisionamiento de dispositivo,
- la implementación de los encaminamientos en la red.

8.4 Asignación dinámica de direcciones IP

Existe un requisito operacional para asignar dinámicamente direcciones IP a los MTA, tanto para el aprovisionamiento y gestión de dispositivos como para las diversas operaciones de protocolos. El modelo de señalización de llamada especificado en la Recomendación relativa a NCS (Rec. UIT-T J.162) se basa en la posibilidad de que un servidor de gestión de llamadas establezca una correspondencia entre un servicio de un abonado y un identificador de punto extremo y un nombre de dominio totalmente cualificado (FQDN) del MTA. Las operaciones de procesamiento de llamada resultarían afectadas si la dirección asignada al MTA cambiara en el transcurso de una llamada activa (lo que puede suceder si expira el alquiler del DHCP durante una llamada activa). DHCP no permite que se modifique una dirección IP tras las renovaciones; un cambio sólo puede administrarse obligando al MTA a una reinicialización (sea explícitamente o denegando una renovación). Se recomienda que se mantenga la continuidad de la dirección IP del MTA utilizando renovaciones DHCP. Operaciones tales como "renumeración de direcciones IP" deberían tener en cuenta estas repercusiones.

8.5 Asignación de nombres de dominio totalmente cualificados (FQDN)

Se supone que los sistemas auxiliares del OSS generarán FQDN para todos los dispositivos IPCablecom, y que transmitirá esos datos a los dispositivos IPCablecom y otros elementos de red apropiados. Estas interfaces no están definidas en IPCablecom (fase 1).

8.6 Marcado de prioridades de los paquetes del tren de señalización y del tren de medios

Tanto el tren de medios como el tren de señalización de los servicios basados en IPCablecom requieren la existencia de métodos que permitan marcar y transportar adecuadamente paquetes con un nivel de calidad de servicio suficientemente alto, tanto en la red de acceso DOCSIS como en la red medular IP gestionada.

El principal mecanismo para proporcionar una calidad de servicio de retardo bajo los trenes de medios en la red de acceso es el servicio de clasificación de flujo DOCSIS. Este servicio clasifica los paquetes en flujos específicos con arreglo a diferentes campos de los paquetes, como las direcciones de origen y destino IP y el número de puerto UDP. Flujo arriba, esos paquetes clasificados son transportados mediante un servicio apropiado a una velocidad binaria constante (para los códecs actualmente soportados), conforme planifique dinámicamente el CMTS. Flujo abajo, los paquetes son transportados mediante un mecanismo apropiado de puesta en cola de espera y planificación de alta prioridad. Los mecanismos de señalización de DQoS (entre el CMS y el CMTS) y DOCSIS (entre el CMTS y el CM) se utilizan para establecer dinámicamente las reglas de clasificación del flujo del tren de medios y los parámetros del tráfico QoS del flujo de servicio.

Además de clasificar el flujo, es también útil para establecer unas marcas de prioridad apropiadas en los paquetes del tren de medios. Esas marcas de prioridad pueden utilizarse en los sistemas de puesta en cola de espera del CMTS o del CM, y también en las redes medulares de QoS gestionadas Diffserv a fin de dispensar un trato QoS de alta prioridad a esos paquetes. IPCablecom no define cómo se aplican las políticas de QoS en la red medular gestionada, pero proporciona los mecanismos de protocolo que permiten crear clases especiales de servicios.

Los paquetes de señalización podrían beneficiarse también del establecimiento de prioridades en los servicios de QoS. En particular, cuando una red de acceso alcanza su plena capacidad de carga, podría ser importante reenviar paquetes de señalización con una prioridad superior para evitar un retardo excesivo de la señalización. Si se desea establecer prioridades en la señalización, entonces el método que se utilice para proporcionar QoS con prioridades estará basado en dos mecanismos. En primer lugar, se marcarán todos los paquetes de señalización con una marca de alta prioridad y, en segundo lugar, se proporcionará un clasificador DOCSIS que clasifique ese tipo de paquetes para transportarlos en un flujo de servicio de prioridad superior. La función del clasificador puede ser tan simple como asignar al SID de alta prioridad todos los paquetes ascendentes que tengan esa prioridad, o puede ser más compleja y consistir en identificar también la dirección IP del MTA o los MTA que originan la señalización. El flujo de servicio de prioridad superior puede provisionarse estadísticamente o puede ser creado dinámicamente por el administrador del CMTS. Hay que señalar que, si el administrador está preocupado por una posible apropiación indebida de servicio en el flujo de servicio de alta prioridad, podrá configurar el flujo de servicio con alta prioridad (retardo bajo) pero con poca anchura de banda.

La arquitectura de IPCablecom permite que se utilice el marco de servicios diferenciados (IETF RFC 3260) para diferenciar los medios y la señalización de IPCablecom de los paquetes de datos a alta velocidad. La marcación de paquetes de los flujos de medios (RTP y RTCP) y del flujo de señalización (NCS, TGCP) es efectuada por el MTA/MG y/o el CMS/MGC. La marcación de paquetes puede efectuarse en la capa IP utilizando el punto de código Diffserv (DSCP, *diffserv code point*). Obsérvese que IETF RFC 2474 intenta red denominar el octeto TOS del encabezamiento IPv4 y el octeto de clase de tráfico del encabezamiento IPv6 como campo de servicios diferenciados (DS, *differentiated services*). El campo DS tiene un punto de código Diffserv de seis bits y dos bits "actualmente no utilizados". IETF RFC 2474 fue actualizada por IETF RFC 3168, que definió los dos bits "no utilizados" como bits de "notificación de congestión explícita (ECN, *explicit congestion notification*). Se recomienda encarecidamente que se utilice el campo DSCP en vez del byte de TOS IPv4.

La configuración de los valores DSCP de los flujos de medios y de señalización se efectúan mediante los módulos MIB de IPCablecom para el MTA. Debe señalarse que los parámetros SDP

señalizados en la NCS pueden contener valores que dejarían sin efecto, conexión a conexión, el valor configurado de la marcación de prioridad del flujo de medios.

8.7 Soporte fax

IPCablecom da soporte a la transmisión fax en tiempo real. En IPCablecom, la mejor manera de prestar servicio fax es utilizando la Rec. UIT-T T.38 para la retransmisión fax por redes IP (es decir, terminación local de fax y la traducción del tren fax en un tren de datos de retransmisión fax IP). Si se establece una comunicación mediante un códec de audio, se encomienda al MTA que busque tonos fax. Si se detectan tonos fax, se notifica al CMS y se encomienda al MTA que conmute el tren portador a T.38. IPCablecom también soporta transferencia de fax, en la que los tonos fax pasan a través de la red IP como un tren de audio codificado G.711. En la transferencia de fax también se soporta cancelación de eco.

Se necesita poder pasar de fax a llamada vocal. En el caso de retransmisión de fax, también es posible regresar de fax a llamada vocal.

8.8 Soporte para módems analógicos

Los módems analógicos reciben soporte de manera análoga al paso de fax, es decir, se pide a un MTA que detecte tonos módem y, cuando los tonos han sido detectados, el CMS encomienda al MTA que conmute para pasar al códec G.711 si éste no está ya en uso. Para el paso de módem también se soporta la cancelación de eco.

Se soporta el cambio desde un códec de baja anchura de banda a G.711 para así soportar la señalización de módem análogo desde una llamada vocal. También se soporta volver a un códec de bajo ancho de banda una vez que concluya la señalización del módem.

No es necesaria la terminación local de los módems, ni la traducción del tren de bits del módem a un tren de datos que retransmita flujo del módem mediante IP.

Apéndice I

Glosario de términos

El presente apéndice contiene la lista completa de términos, definiciones, acrónimos y abreviaturas utilizados en el conjunto de las Recomendaciones IPCablecom.

I.1 Definiciones

I.1.1 control de acceso: Limitación del flujo de información proveniente de los recursos de un sistema de modo que se dirija sólo a personas, programas, procesos u otros recursos de sistema autorizados en una red.

I.1.2 activo: Un flujo J.112 se denomina "activo" cuando le está permitido reenviar paquetes de datos. Un flujo J.112 deberá ser admitido antes de poder estar activo.

I.1.3 autenticación: Proceso de verificación de la identidad que una entidad declara a otra.

I.1.4 autenticidad: Posibilidad de cerciorarse de que la información proporcionada no ha experimentado modificaciones o falsificaciones, sino que ha sido realmente producida por la entidad que declara haber proporcionado la información.

- I.1.5 autorización:** Concesión de acceso a un servicio o dispositivo, siempre que se tenga permiso para dicho acceso.
- I.1.6 módem de cable:** Un módem de cable es un dispositivo de terminación de capa 2 que termina el extremo cliente de la conexión J.112.
- I.1.7 llamada:** Una llamada es un ejemplar de capacidades de comunicación de voz iniciada por el usuario. En telefonía tradicional, una llamada suele entenderse como el establecimiento de conectividad directamente entre dos puntos: la parte de origen y la parte de terminación. En el contexto IPCablecom, como ya se ha indicado, la comunicación entre las partes se realiza "sin conexiones" en el sentido tradicional.
- I.1.8 cifrado:** Algoritmo que convierte datos de texto claro en texto cifrado, y viceversa.
- I.1.9 conjunto de cifrado:** Conjunto que debe contener tanto un algoritmo de criptación como un algoritmo de autenticación de mensajes (por ejemplo, de tipo MAC o HMAC). En general, puede contener también un algoritmo de gestión de claves, aunque no es ése el caso en el contexto de IPCablecom.
- I.1.10 confidencialidad:** Medio de cerciorarse de que no se revela información a nadie más que a las partes escogidas. Para proteger la confidencialidad, la información es criptada. Se conoce también como "privacidad".
- I.1.11 descendente:** Sentido que va desde el extremo de cabecera hacia la ubicación del abonado.
- I.1.12 criptación:** Método utilizado para convertir información de texto claro en texto cifrado.
- I.1.13 punto de extremo:** Terminal, pasarela o MCU.
- I.1.14 mensaje de evento:** Un mensaje de evento es un conjunto de datos representativo de un evento en la arquitectura IPCablecom que puede ser indicativo de haberse utilizado una o más capacidades IPCablecom facturables. Aunque, por sí mismo, un mensaje de evento puede no ser indicativo de actividades facturables de un cliente, un mensaje de evento correlacionado con otros mensajes de evento sienta las bases de un registro detallado de utilización, que sí es facturable.
- I.1.15 atributo de mensaje de evento:** Un atributo de mensaje de evento es un elemento de datos predefinido descrito mediante una definición de atributo y un tipo de atributo.
- I.1.16 pasarela:** Dispositivos que sirven de enlace entre el mundo de la comunicación vocal IP IPCablecom y la RTPC. Algunos ejemplos son: la pasarela de medios, que proporciona las interfaces de circuito portador con la RTPC y transcodifica el tren de medios, y la pasarela de señalización, que envía y recibe señalización de red conmutada al borde de la red IPCablecom.
- I.1.17 encabezamiento:** Información de control de protocolo ubicada al comienzo de una unidad de datos de protocolo.
- I.1.18 integridad:** Medio de conseguir que la información no experimente modificaciones, excepto por parte de quienes estén autorizados a hacerlo.
- I.1.19 IPCablecom:** Proyecto del UIT-T consistente en una arquitectura y una serie de Recomendaciones que permiten la entrega de servicios en tiempo real por las redes de televisión por cable utilizando módems de cable.
- I.1.20 transacción IPCablecom:** Una transacción IPCablecom es un conjunto de eventos que se producen en la red IPCablecom cuando se entrega un servicio a un abonado. Los mensajes de evento de una misma transacción se identifican mediante un identificador de correlación de facturación único. Para algunos servicios, puede requerirse más de una transacción a fin de proporcionar información necesaria para censar la utilización total del servicio. Para conocer los recursos utilizados en cada servicio pueden ser necesarios múltiples mensajes de evento. Una transacción puede persistir en el tiempo.

- I.1.21 flujo J.112:** Flujo unidireccional o bidireccional de paquetes de datos sujeto a señalización de capa MAC y a asignación de QoS de conformidad con la Rec. UIT-T J.112.
- I.1.22 Kerberos:** Protocolo de autenticación de red mediante claves secretas que utiliza cierto número de algoritmos criptográficos escogidos para criptar y una base de datos de claves centralizada para la autenticación.
- I.1.23 clave:** Valor matemático introducido en el algoritmo criptográfico seleccionado.
- I.1.24 intercambio de claves:** Trueque de claves públicas entre entidades para criptar la comunicación entre las entidades.
- I.1.25 gestión de claves:** Proceso de distribución de claves simétricas compartidas necesarias para utilizar un protocolo de seguridad.
- I.1.26 base de información de gestión (MIB, *management information base*):** Especificación de información de manera que permita un acceso normalizado mediante un protocolo de gestión de red.
- I.1.27 no repudio:** Posibilidad de impedir que un enviante niegue posteriormente que ha enviado un mensaje o realizado una acción.
- I.1.28 privacidad:** Medio de asegurarse de que no se revela información a nadie más que a las partes deseadas. Para proteger la confidencialidad, la información suele criptarse. Se conoce también como confidencialidad.
- I.1.29 clave privada:** Clave utilizada en criptografía de clave pública, que pertenece a una entidad y debe mantenerse secreta.
- I.1.30 mandatario:** Facilidad que proporciona indirectamente algún servicio o que actúa como representante en la entrega de información, eximiendo de ese modo a un anfitrión de dar soporte a ese servicio.
- I.1.31 clave pública:** Clave utilizada en criptografía de clave pública, que pertenece a una entidad y es distribuida públicamente. Otras entidades utilizan esta clave para criptar datos y enviarlos al propietario de la clave.
- I.1.32 certificado de clave pública:** Vinculación entre una clave pública de una entidad y uno o más atributos relativos a su identidad; se conoce también como certificado digital.
- I.1.33 criptografía de clave pública:** Procedimiento que utiliza dos claves, una pública y una privada, para la criptación y descriptación; conocido también como algoritmo asimétrico. La clave pública de un usuario está públicamente a disposición de otros para que éstos envíen un mensaje al propietario de la clave. La clave privada de un usuario se mantiene secreta, y es la única clave que puede descriptar los mensajes que se envían criptados mediante la clave pública del usuario.
- I.1.34 clave privada raíz:** Clave firmada privada de la más alta autoridad de certificación. Suele utilizarse para firmar certificados de clave pública destinados a autoridades de certificación u otras entidades de nivel inferior.
- I.1.35 clave pública raíz:** Clave pública de la más alta autoridad de certificación, que suele utilizarse para verificar firmas digitales generadas por aquella con la clave privada raíz correspondiente.
- I.1.36 servicio:** Un servicio es una característica o lote de características de comunicaciones que puede seleccionar un abonado. Un servicio se identifica por un conjunto de una o más "llamadas" o transacciones que entregan al abonado la funcionalidad deseada. Ejemplos de servicio son: una comunicación vocal entre dos abonados IPCablecom locales, una llamada tripartita, una película de pago por visión, o una sesión de navegación web. Un servicio puede ser instantáneo o duradero.

I.1.37 pasarela de señalización (SG, *signalling gateway*): Una SG es un agente de señalización que recibe/envía señalización nativa RCC en el borde de la red IP. En particular, la función SG mediante SS7 traduce variantes PU-RDSI y TCAP de una pasarela Internet SS7 a una versión común de PU-RDSI y de TCAP.

I.1.38 certificado X.509: Especificación de un certificado de clave pública desarrollada como parte del directorio de normas de la Rec. UIT-T X.500.

I.2 Abreviaturas y acrónimos

| | |
|------|--|
| AH | Encabezamiento de autenticación (<i>authentication header</i>) |
| AMA | Contabilidad de mensaje automatizada (<i>automated message accounting</i>) |
| AN | Nodo de acceso (<i>access node</i>) |
| ANC | Controlador de anuncios (<i>announcement controller</i>) |
| ANP | Reproductor de anuncios (<i>announcement player</i>) |
| ANS | Servidor de anuncios (<i>announcement server</i>) |
| API | Interfaz de programación de aplicación (<i>application programming interface</i>) |
| BPI+ | Interfaz de privacidad de referencia plus (<i>baseline privacy interface plus</i>) |
| CA | Agente de llamada (<i>call agent</i>) |
| CBC | Modo concatenación de bloques cifrados (<i>cipher block chaining mode</i>) |
| CDR | Registro de detalles de las llamadas (<i>call detail record</i>) |
| CIC | Código de identificación de circuito |
| CID | Identificador de circuito (<i>circuit ID</i>) |
| CM | Módem de cable (<i>cable modem</i>) |
| CMS | Servicio de gestión de llamadas (<i>call management server</i>) |
| CMS | Sintaxis de mensaje criptográfico (<i>cryptographic message syntax</i>) |
| CMTS | Sistema de terminación de módem de cable (<i>cable modem termination system</i>) |
| COPS | Servicio de política común abierta (<i>common open policy service</i>) |
| CPE | Equipo en las instalaciones del cliente (<i>customer premises equipment</i>) |
| DCS | Señalización de llamada distribuida (<i>distributed call signalling</i>) |
| DHCP | Protocolo de configuración dinámico del anfitrión (<i>dynamic host configuration protocol</i>) |
| DNS | Sistema de nombres de dominio (<i>domain name system</i>) |
| DPC | Código de punto de destino (<i>destination point code</i>) |
| DQoS | Calidad de servicio dinámica (<i>dynamic quality of service</i>) |
| DTMF | Multifrecuencia bitono (<i>dual tone multi-frequency</i>) |
| ESP | Seguridad de encapsulado IPsec (<i>IPsec encapsulation security</i>) |
| FID | Identificador de flujo (<i>flow identifier</i>) |
| FQDN | Nombre de dominio totalmente cualificado (<i>fully qualified domain name</i>) |
| GC | Controlador de puerta (<i>gate controller</i>) |
| HFC | Híbrido fibra/coaxial (cable) (<i>hybrid fibre/coaxial (cable)</i>) |

| | |
|---------|--|
| HMAC | Código de autenticación de mensaje troceado (<i>hashed message authentication code</i>) |
| HTTP | Protocolo de transferencia hipertexto (<i>hypertext transfer protocol</i>) |
| IANA | Autoridad de asignación de números Internet (<i>Internet assigned numbers authority</i>) |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Grupo de tareas especiales de ingeniería en Internet (<i>Internet engineering task force</i>) |
| IKE | Intercambio de claves Internet (<i>Internet key exchange</i>) |
| IKE– | IKE con claves precompartidas de autenticación (<i>IKE with pre-shared keys for authentication</i>) |
| IKE+ | Notación definida para referirse al uso de IKE, que requiere certificados digitales para la autenticación (<i>a notation defined to refer to the use of IKE, which requires digital certificates for authentication</i>) |
| INA | Adaptador de red interactivo (<i>interactive network adapter</i>) |
| IP | Protocolo Internet (<i>Internet protocol</i>) |
| IPsec | Seguridad del protocolo Internet (<i>IP security</i>) |
| ISTP | Protocolo de transporte de señalización Internet (<i>Internet signalling transport protocol</i>) |
| LNP | Portabilidad de números locales (<i>local number portability</i>) |
| MAC | Código de autenticación de mensaje (<i>message authentication code</i>) |
| MAC | Control de acceso a medios (<i>media access control</i>) |
| MD5 | Message Digest 5 |
| MF | Multifrecuencia |
| MG | Pasarela de medios (<i>media gateway</i>) |
| MGC | Controlador de pasarela de medios (<i>media gateway controller</i>) |
| MGCI | Interfaz de controlador de pasarela de medios (<i>media gateway controller interface</i>) |
| MGCP | Protocolo de control de pasarela de medios (<i>media gateway control protocol</i>) |
| MIB | Base de información de gestión (<i>management information base</i>) |
| MMH | Troceo modular multilineal (<i>multilinear modular hash</i>) |
| MTA | Adaptador de terminal de medios (<i>media terminal adapter</i>) |
| MTP | Parte transferencia de mensajes (<i>message transfer part</i>) |
| MWD | Periodo de espera máximo (<i>maximum waiting delay</i>) |
| NCS | Señalización de llamada de red (<i>network call signalling</i>) |
| NTP | Protocolo de señales horarias de red (<i>network time protocol</i>) |
| OSS | Sistema de soporte de operaciones (<i>operations support system</i>) |
| PHS | Supresión de encabezamiento de cabida útil (<i>payload header suppression</i>) |
| PKI | Infraestructura de claves públicas (<i>public key infrastructure</i>) |
| PKINIT | Autenticación inicial de criptografía de clave pública (<i>public key cryptography initial authentication</i>) |
| PU-RDSI | Parte usuario de la red digital de servicios integrados |
| QoS | Calidad de servicio (<i>quality of service</i>) |

| | |
|--------|--|
| RADIUS | Servicio de usuario para acceso a distancia por marcación directa de extensión (<i>remote access dial-in user service</i>) |
| RAP | Protocolo de asignación de recursos (<i>resource allocation protocol</i>) |
| RC4 | Cifra de longitud de clave variable ofrecida en el conjunto de cifrado, que se utiliza para criptar el tráfico de medios en IPCablecom |
| RFC | Petición de comentarios (<i>request for comments</i>) |
| RFI | Interfaz de radiofrecuencia (<i>radio frequency interface</i>) |
| RKS | Servidor de mantenimiento de registros (<i>record keeping server</i>) |
| RSVP | Protocolo de reserva de recursos (<i>resource reservation protocol</i>) |
| RTCP | Protocolo de control en tiempo real (<i>real-time control protocol</i>) |
| RTO | Temporizador de retransmisión (<i>retransmission timeout</i>) |
| RTP | Protocolo de transferencia en tiempo real (<i>real-time transfer protocol</i>) |
| RTPC | Red telefónica pública conmutada |
| SA | Asociación de seguridad (<i>security association</i>) |
| SA | Dirección de origen (<i>source address</i>) |
| SCCP | Parte control de la conexión de señalización (<i>signalling connection control part</i>) |
| SCP | Punto de control de servicio (<i>service control point</i>) |
| SCTP | Protocolo de transmisión de control de trenes (<i>stream control transmission protocol</i>) |
| SDP | Protocolo de descripción de sesión (<i>session description protocol</i>) |
| SG | Pasarela de señalización (<i>signalling gateway</i>) |
| SHA-1 | Algoritmo de troceo seguro 1 (<i>secure hash algorithm 1</i>) |
| SID | Número de identificación de sistema (<i>system identification number</i>) |
| SIP | Protocolo de iniciación de sesión (<i>session initiation protocol</i>) |
| SIP+ | Protocolo de iniciación de sesión plus (<i>session initiation protocol plus</i>) |
| SNMP | Protocolo simple de gestión de red (<i>simple network management protocol</i>) |
| SPI | Índice de parámetros de seguridad (<i>security parameters index</i>) |
| SS7 | Sistema de señalización N.º 7 (<i>signalling system No. 7</i>) |
| SSP | Punto de conmutación de señal (<i>signal switching point</i>) |
| TCAP | Parte aplicación de capacidades de transacción (<i>transaction capabilities application part</i>) |
| TCP | Protocolo de control de transmisión (<i>transmission control protocol</i>) |
| TGS | Servidor que concede tique (<i>ticket granting server</i>) |
| TLV | Tipo-longitud-valor (<i>type-length-value</i>) |
| ToS | Tipo de servicio (<i>type of service</i>) |
| UDP | Protocolo de datagrama de usuario (<i>user datagram protocol</i>) |
| VAD | Detección de actividad vocal (<i>voice activity detection</i>) |
| VoIP | Voz sobre el protocolo Internet (<i>voice over IP</i>) |

BIBLIOGRAFÍA

- IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.
- IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.
- IETF RFC 2274 (1998), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.
- IETF RFC 2575 (1999), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*. (Obsoletes RFC 2275).

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 multimedios |
| Serie I | Red digital de servicios integrados |
| Serie J | Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios |
| 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 |