Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.179

(11/2005)

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

IPCablecom

Soporte de IPCablecom para multimedia

Recomendación UIT-T J.179

Recomendación UIT-T J.179

Soporte de IPCablecom para multimedia

Resumen

Esta Recomendación contribuye al despliegue de servicios multimedia generales proporcionando una definición técnica de varias interfaces de señalización basadas en IP que soportan las capacidades medulares QoS y de gestión de políticas, inherentes a los módems de cable de la tecnología CableModem. Los servicios multimedia se definen como servicios basados en IP (por ejemplo, juegos en línea, videoconferencia, medios de flujo continuo, etc.) que requieren recursos de red basados en QoS (en contraste con servicios tales como la consulta rápida de la web, el correo electrónico, la mensajería instantánea y la compartición de ficheros que se proporcionan normalmente utilizando flujos de mejor esfuerzo). Si bien la telefonía o los servicios basados en la voz no están excluidos de manera específica de esta definición, el conjunto de Recomendaciones IPCablecom-T proporcionan una cobertura específica de este tipo de entrega de servicios y, por consiguiente, esas Recomendaciones deberán ser consultadas según proceda.

Orígenes

La Recomendación UIT-T J.179 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.

ÍNDICE

Página

Recomendación UIT-T J.179

Soporte de IPCablecom para multimedia

1 Alcance

Esta Recomendación se refiere al despliegue de servicios multimedia generales proporcionando una definición técnica de varias interfaces de señalización basadas en IP que soportan las capacidades medulares de QoS y gestión de políticas inherentes a los módems de cable de la tecnología CableModem. Los servicios multimedia se definen como servicios basados en IP (por ejemplo, juegos en línea, videoconferencia, medios de flujo continuo, etc.) que requieren recursos de red basados en QoS (en contraste con servicios tales como la consulta rápida de la web, el correo electrónico, la mensajería instantánea y la compartición de ficheros que se proporcionan normalmente utilizando flujos de mejor esfuerzo). Si bien la telefonía o los servicios basados en la voz no están excluidos de manera específica de esta definición, el conjunto de Recomendaciones IPCablecom-T proporcionan una cobertura específica de este tipo de entrega de servicios y, por consiguiente, esas Recomendaciones deberán ser consultadas según proceda.

2 Referencias

2.1 Referencias normativas

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.

[1] Recomendación UIT-T J.112/anexo B (2004), *Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia*.

[2] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*

[3] IETF RFC 2210 (1997), *The Use of RSVP with IETF Integrated Services*.

[4] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service.*

[5] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service*.

[6] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

[7] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol.*

[8] IETF RFC 2866 (2000), *RADIUS Accounting*.

[9] Recomendación UIT-T J.163 (2005), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable*.

[10] 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*.

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

[12] Recomendación UIT-T J.125 (2004), *Privacidad del enlace para la implementación de módems de cable*.

2.2 Referencias informativas

[13] IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: An Overview*.

[14] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[15] IETF RFC 2216 (1997), *Network Element Service Specification Template*.

[16] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

[17] IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS Compliant RF Interfaces*.

[18] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*.

[19] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)*.

[20] IETF RFC 3175 (2001), *Aggregation of RSVP for IPv4 and IPv6 Reservations*.

[21] CableLabs (http://www.cablemodem.com/specifications).

[22] IETF RFC 2751 (2000), *Signaled Preemption Priority Policy Element*.

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 cliente de tipo 1: El cliente de tipo 1 representa puntos de extremo "herederos" (por ejemplo, aplicaciones de PC, consolas de juegos) que carecen de información específica relativa a QoS o capacidades de señalización. Este cliente no sabe nada sobre mensajería de CableModem, IPCable2Home o IPCablecom y, por tanto, no cabe imponerle requisitos relativos a la misma. Clientes de tipo 1 pueden ser desde dispositivos sencillos de presentación analógica audio y vídeo hasta periféricos en red y electrónica de consumidor complejos, tales como unidades de adaptación multimedia o consolas de juegos. Estos clientes se comunican con un gestor de aplicación para pedirle servicio y no piden recursos QoS directamente de la red de acceso del operador de cable. La presente Recomendación se refiere sólo a clientes de tipo 1.

3.2 cliente de tipo 2: El cliente de tipo 2 es similar a un MTA de telefonía IPCablecom-T en el sentido de que soporta la señalización de QoS basada en la Recomendación sobre DQoS de IPCablecom. Este cliente está al corriente de la QoS de multimedia IPCablecom y se comunica con un gestor de aplicación para pedirle servicio y obtener un testigo para recursos de red de acceso. El cliente presenta a continuación ese testigo, cuando pide recursos QoS de la red de acceso (pkt-mm-1, pkt-mm-6). El soporte de esta Recomendación para los clientes de tipo 2 queda en estudio.

3.3 cliente de tipo 3: El cliente de tipo 3 pide QoS en base al RSVP sin la interacción del gestor de aplicación. Este cliente está al corriente del RSVP basado en las normas IETF y utiliza dicho protocolo para pedir recursos QoS de la red de acceso directamente del CMTS. El soporte de de esta Recomendación para los clientes de tipo 3 queda en estudio.

3.4 DOCSIS: Norma que denota una tecnología de módem de cable específica, la tecnología CableModem, desarrollada por Cable Television Laboratories, Inc. ("CableLabs") cuyas especificaciones se encuentran en: http://www.cablemodem.com/specifications/. La versión internacional se define en el anexo B/J.112.

3.5 IPCablecom-T: Serie de Recomendaciones de la UIT sobre IPCablecom relativas al servicio telefónico.

4 Abreviaturas, siglas o acrónimos y convenios

4.1 Abreviaturas, siglas o acrónimos

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

AM Gestor de aplicación (*application manager)* (un sistema que hace interfaz con el servidor o los servidores de política para pedir servicio basado en QoS en nombre de un usuario extremo o un sistema de gestión de red)

BCID ID de correlación de facturación (*billing correlation ID*) (definido en la Recomendación relativa a la mensajería de eventos de IPCablecom)

CM Módem de cable (*cable modem*)

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

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

COPS Servicio de política común abierta (*common open policy service*) (definido en RFC 2748)

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

DSx Mecanismo de señalización de QoS del anexo B/J.112 que proporciona la (mensajería) semántica de añadir, cambiar y suprimir servicio dinámico

FQDN Nombre de dominio totalmente cualificado (*fully qualified domain name*)

HFC Híbrido fibra/coaxial (*hybrid fibre/coax*)

IETF Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)

IP Protocolo Internet (*Internet protocol*)

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

MG Pasarela de medios (*media gateway*)

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

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

NAT Traducción de dirección de red (*network address translation*)

PDP Punto de decisión de la política (*policy decision point*) (definido en RFC 2753)

PEP Punto de imposición de la política (*policy enforcement point*) (definido en RFC 2753)

PS Servidor de política (*policy server*)

QoS Calidad de servicio (*quality of service*)

RADIUS Servicio de usuario para acceso a distancia por marcación directa de extensión (*remote authentication dial-in user service*) (definido en RFC 2138 y RFC 2139)

RAP Protocolo de asignación de recursos (*resource allocation protocol*) (Grupo de Trabajo del IETF – Responsable de la definición y mantenimiento del protocolo de COPS)

RCD Dominio de control de recurso (*resource control domain*)

RFC Petición de comentarios (*request for comments*) (documentos de carácter técnico aprobados por el IETF que están disponibles en http://www.ietf.org/rfc.html)

RFI Interfaz de radiofrecuencia (*radio frequency interface*) (especificación que define las interfaces de capa MAC y física entre elementos de red CMTS y CM)

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

RPV Red privada virtual

RSVP Protocolo de reserva de recurso (*resource reservation protocol*) (definido en RFC 2205)

RSVP+ Perfil de IPCablecom y ampliación de RSVP (definido en la Recomendación sobre DQoS de IPCablecom)

RTPC Red telefónica pública conmutada

SCD Dominio de control de sesión (*session control domain*)

S-MTA MTA autónomo (*standalone MTA*) (nodo único que contiene un MTA y un MAC no DOCSIS (por ejemplo, Ethernet))

TCP Protocolo de control de transmisión (*transmission control protocol*)

TLV Valor de longitud de tipo (*type-length-value*) (técnica utilizada en el formateo de elementos de protocolo)

UDP Protocolo de datagrama de usuario (*user datagram protocol*) (protocolo sin conexión construido sobre el protocolo Internet (IP))

UGS Servicio de concesión no solicitada (*unsolicited grant service*) (tipo de periodicidad de QoS del anexo B/J.112 utilizado para servicios a velocidad binaria constante (por ejemplo, códecs de voz))

UGS/AD Servicio de concesión no solicitada con detección de actividad (*unsolicited grant service with activity detection*)

VoIP Voz sobre el protocolo Internet (*voice over IP*)

4.2 Convenios

A lo largo de esta Recomendación, las palabras utilizadas para señalar la importancia de requisitos particulares se escriben con letras mayúsculas. Dichas palabras son:

"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 del elemento de que se trate, pero que deberían tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de optar por una vía diferente.

"NO DEBERÍA(N)" Esta expresión significa que pueden existir motivos válidos en determinadas circunstancias en las que el comportamiento indicado sea aceptable o incluso de utilidad, pero que deberían tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de implementar cualquier comportamiento descrito con esta etiqueta.

"PUEDE(N)" Esta palabra, o el adjetivo "FACULTATIVO", significa que el elemento es verdaderamente facultativo. Un vendedor puede optar por incluir el elemento porque así se exige en un determinado mercado o porque mejora el producto, por ejemplo; otro vendedor puede omitir el mismo elemento.

5 Visión general técnica

Esta cláusula consta de material básico que para algunos lectores puede ser el contexto adecuado de las Recomendaciones relativas a interfaces de protocolos que se exponen en detalle más adelante. El propósito de la presente cláusula es dar una visión general de alto nivel de la arquitectura de multimedia IPCablecom y las tecnologías fundamentales en las que se basa. Para más detalles sobre la arquitectura de multimedia, véase el apéndice I.

5.1 Antecedentes de QoS

Como se indica a lo largo de la presente Recomendación, una de las características fundamentales del marco de servicios multimedia IPCablecom consiste en que proporciona acceso de capa IP a capacidades QoS complejas definidas en el anexo B/J.112 y en IPCablecom-T. En esta subcláusula se da una breve visión de conjunto de esas capacidades a modo de antecedente preparatorio del análisis pormenorizado de la política de QoS y la gestión de recursos que sigue.

5.1.1 Resumen sobre QoS del anexo B/J.112

El anexo B/J.112 Recomendación sobre RFI [1] define un conjunto de facilidades de QoS basado en un constructivo fundamental de la gestión de recursos de red al que se denomina flujo de servicio. Un flujo de servicio se define como "un servicio de transporte de la capa de control de acceso a medios (MAC, *media access control*) que:

1) proporciona transporte unidireccional de paquetes desde la entidad de servicio de capa superior hasta la RF; y

2) configura, dirige y prioriza el tráfico de acuerdo con los parámetros de tráfico de QoS definidos para el flujo".

Además de esta abstracción primaria que facilita la reserva y calendarización de recurso de red de acceso compartido flujo por flujo, se define un cierto número de constructivos de soporte tangibles que se utilizan para gestionar esos recursos. Dos de esos constructivos son:

– Las codificaciones de flujo de servicio: Parámetros codificados según su tipo/longitud/valor (TLV) que se utilizan para definir parámetros de QoS asociados a un flujo de servicio.

– El clasificador: Parámetros de IP, Ethernet e IEEE802.1p/q codificados según su tipo/longitud/valor que se utilizan para definir y limitar el alcance de un flujo en función de los puntos de extremo de origen y terminación.

Si bien el anexo B/J.112 soporta modelos de QoS provisionados (es decir, flujos de servicio duraderos y estáticos que se establecen durante el proceso de registro del CM) y modelos de QoS dinámicos (es decir, flujos de servicio transitorios que se añaden, modifican y suprimen según se necesite), el marco de multimedia IPCablecom se refiere sobre todo a la variedad dinámica ya que esta permite una gestión de recursos de red óptima mediante la multiplexación estadística según demanden los requisitos del servicio.

La gestión del flujo de servicio se lleva a cabo mediante mensajes de añadir/cambiar/suprimir servicio dinámico (DSA/DSC/DSD, *add/change/delete*) DOCSIS de capa MAC, que pueden ser iniciados por el CM o el CMTS. Las transacciones DSA y DSC adoptan la forma de un intercambio de tres vías en el que una petición (REQ) va seguida por una respuesta (RSP) de la que a continuación se acusa recibo (ACK). Los mensajes DSD son intercambios sencillos de dos vías. En cada mensaje de respuesta DSx se proporciona un atributo específico conocido como código de confirmación que indica la situación de éxito o fracaso de una transacción.

Un punto importante a tener en cuenta al analizar las capacidades QoS a las que se refiere el anexo B/J.112 es que los flujos de servicio ascendentes y descendentes reciben un tratamiento básicamente distinto en el CMTS. Esto se debe a que los canales RF en sentido ascendente son medios de acceso compartido que compiten entre sí y adoptan la forma topológica de una relación de muchos a uno entre múltiples CM y un único CMTS. Por el contrario, el canal RF en sentido

descendente se comporta de forma mucho más parecida a un encaminador IP tradicional en el que los paquetes llegan (bien desde la red de acceso o bien por circuitos troncales básicos), se ponen en cola de espera y se reenvían a uno o más destinos. En consecuencia, se aplican mecanismos de QoS distintos dependiendo de si un determinado flujo de servicio unidireccional está orientado en sentido ascendente o en sentido descendente.

Los flujos de servicio ascendentes se pueden definir con uno de los cinco tipos de calendarización de flujo de servicio siguientes:

– Mejor esfuerzo: Estrategia normalizada de gestión de recursos basada en la competencia en la que se conceden oportunidades de transmisión en base al principio de prioridad en el tiempo, aunque bajo la coordinación del calendarizador CMTS. Este tipo de calendarización puede ser complementado con características de QoS en las que, por ejemplo, se aplican límites de velocidad máxima a un flujo de servicio particular.
– Interrogación secuencial no en tiempo real: Estrategia de gestión de recursos basada en la reserva en la que un determinado CM es interrogado secuencialmente en un intervalo fijo para determinar si se han puesto datos en cola de espera para su transmisión en un flujo de servicio particular y si, en caso afirmativo, el calendarizador proporciona una oportunidad o concesión de transmisión a ese flujo de servicio.
– Interrogación secuencial en tiempo real: Análogo al tipo de calendarización con interrogación secuencial no en tiempo real, con la salvedad de que el intervalo de interrogación secuencial fijo es normalmente muy corto (<500 ms). Los tipos de calendarización con interrogación secuencial son los más adecuados para el tráfico a velocidad binaria variable que tiene requisitos de latencia y caudal inflexibles.
– Concesión no solicitada: Estrategia de gestión de recursos basada en la reserva en la que se proporciona una concesión de tamaño fijo a un flujo de servicio particular a intervalos (casi) fijos sin interrogación secuencial o interacción adicional. Este tipo de calendarización es el más adecuado para el tráfico a velocidad binaria constante y elimina gran parte de la tara del protocolo asociada a los tipos de interrogación secuencial.
– Concesión no solicitada con detección de actividad: Estrategia de gestión de recursos basada en la reserva que representa un híbrido de los tipos de calendarización con interrogación secuencial y con concesión no solicitada en la que se proporcionan concesiones fijas a intervalos (casi) fijos mientras se pongan datos en cola de espera para su transmisión. Durante los periodos de inactividad, este tipo de calendarización revierte a un modo de interrogación secuencial para conservar la anchura de banda no utilizada.

Debido a la naturaleza singular y a las características especializadas de esos tipos de calendarización, se asocian a cada uno de ellos parámetros de QoS específicos. Dichos parámetros se exponen en detalle en la siguiente cláusula.

Los flujos de servicio descendentes se definen utilizando el mismo conjunto de parámetros de QoS asociado al tipo de calendarización de mejor esfuerzo en sentido ascendente.

Con independencia de la orientación del flujo o del tipo de calendarización particular solicitado, todos los flujos de servicio dinámicos proceden a través de tres estados lógicos, que se exponen a continuación de forma resumida. Si bien ciertos escenarios de señalización optimizados permiten una operación conocida como operación de compromiso "monofásico", la petición pasa por las tres fases del proceso lógico de acuerdo con el servicio proporcionado por el CMTS.

– Autorizado: Se autentican las peticiones y se aplican las reglas de política de red con el resultado de una capacidad máxima de autorización que constituye la frontera de las peticiones de reserva subsiguientes.

– Admitido (o reservado): Se construye un flujo de servicio inactivo y el calendarizador reserva recursos de tal manera que las peticiones de activación subsiguientes tienen el éxito garantizado; los recursos reservados pueden ser utilizados por el tráfico de mejor esfuerzo (del mismo CM o de CM diferentes) hasta que se comprometan.

– Activo (o comprometido): El flujo de servicio es activado junto con los clasificadores correspondientes; los paquetes de QoS mejorada pueden ahora atravesar el flujo.

NOTA – En sentido literal, DOCSIS no define "estados", sino más bien "atributos" de flujos de servicio que son sustituidos por completo con cada transacción DSC. Los estados que aquí se describen son un constructivo lógico utilizado en un modelo conceptual que describe el proceso de gestión de recursos que tiene lugar en el CMTS. Además, al definir los atributos de un flujo de servicio, la Recomendación sobre RFI DOCSIS procede a normalizar en base a los términos "admitido" y "activo", en tanto que IPCablecom adopta los términos "reservado" y "comprometido", equivalentes respectivamente a los anteriores, para caracterizar los estados de la puerta.

Aunque DOCSIS no define un procedimiento de autorización específico para aplicarlo a mensajes DSx, proporciona soporte de protocolo mediante una facilidad conocida como bloque de autorización para esquemas de autorización específicos del servicio. Cualesquiera credenciales o testigos de autorización que sean presentados por medio del bloque de autorización son reenviados a un módulo de autorización apropiado antes del procesamiento de la petición DSx en el CMTS. IPCablecom hace un uso extensivo de este mecanismo de autorización como se describe más adelante.

5.1.2 Resumen sobre QoS de IPCablecom-T

Mientras que el anexo B/J.112 sobre RFI define los mecanismos de QoS fundamentales que forman el núcleo del modelo de DQoS de IPCablecom, la Recomendación relativa a DQoS de IPCablecom [9] aumenta esas capacidades con un marco de gestión de políticas basado en el COPS. Al igual que el flujo de servicio representa la abstracción principal en el modelo de DQoS del anexo B/J.112, la puerta desempeña un cometido, de importancia comparable, en el esquema de DQoS de IPCablecom. Una puerta define una capacidad máxima de autorización de recurso que consta de parámetros de QoS a nivel de IP así como de clasificadores que definen el alcance de los flujos de servicio que pueden establecerse con respecto a la puerta. De acuerdo con los mecanismos de autorización del anexo B/J.112 descritos más arriba, sólo se concederán las peticiones DSx que se atengan a la relación general siguiente parámetro por parámetro:

Capacidad máxima autorizada ≥ Capacidad máxima reservada ≥ Capacidad máxima comprometida

En base a este modelo de gestión de políticas, IPCablecom-T define un esquema de preautorización en el que los recursos de red son autorizados con anterioridad a los mensajes DSx que piden el establecimiento del flujo de servicio correspondiente. En consecuencia, la interfaz de COPS utilizada para instalar y gestionar puertas se corresponde más estrechamente con el modelo de COPS-PR definido en RFC 3084 [19] que con el esquema de COPS normalizado definido en RFC 2748 [7]. Además, para instalar y gestionar estas puertas, la Recomendación sobre DQoS de IPCablecom define el conjunto de los objetos específicos del cliente de COPS que constituyen las primitivas de una interfaz de señalización de control por puerta entre el CMS y el CMTS.

De manera específica, el CMS puede descomponerse lógicamente en un agente de llamada responsable del mantenimiento del estado de la llamada telefónica y un controlador de puerta que recibe peticiones de autorización del agente de llamada (mediante una interfaz interna) e instala decisiones de tipo político en forma de puertas en el CMTS. En el modelo multimedia IPCablecom, esta descomposición se formaliza mediante dos elementos de red distintos, el servidor de política (análogo al controlador de puerta de IPCablecom-T) y el gestor de aplicación (que define una funcionalidad específica del servicio similar a la del agente de llamada en el modelo IPCablecom-T).

Lo que sigue es una ilustración de este modelo de preautorización y empleo de la interfaz de control por puerta en el CMTS, en donde un flujo de llamadas típico de IPCablecom-T por red de zona única (es decir, utilizando un solo CMS) procede como se indica (algunos de estos pasos se producirían normalmente en paralelo):

- $E\text{-}MTA_o$ arranca, se provisiona y se registra en el CMS.
- CMS envía una petición a $E\text{-}MTA_o$ para notificar un evento de descuelgue y los dígitos marcados.
- $E\text{-}MTA_t$ arranca, se provisiona y se registra en el CMS.
- CMS envía una petición a $E\text{-}MTA_t$ para notificar un evento de descuelgue y los dígitos marcados.
- $E\text{-}MTA_o$ se descuelga, se lo notifica al CMS y entrega los dígitos marcados.
- CMS envía una petición a $E\text{-}MTA_o$ para crear una conexión lógica nueva y recupera SDP_o.
- CMS envía una petición a $E\text{-}MTA_t$ para crear una conexión lógica nueva y recupera SDP_t.
- CMS instala una puerta en el $CMTS_o$ y recupera el testigo ID de puerta ($GateID_o$) correspondiente.
- CMS instala una puerta en el $CMTS_t$ y recupera el testigo ID de puerta ($GateID_t$) correspondiente.
- CMS envía una petición (con ID de puerta ($GateID_o$)) a $E\text{-}MTA_o$ para reservar recursos y emite un tono de llamada.
- $E\text{-}MTA_o$ envía una DSA-REQ al $CMTS_o$ para establecer flujos de servicio y reservar recursos.
- CMS envía una petición (con ID de puerta ($GateID_t$)) a $E\text{-}MTA_t$ para reservar recursos y dar tono de alerta.
- $E\text{-}MTA_t$ envía un DSA-REQ al $CMTS_t$ para establecer flujos de servicio y reservar recursos.
- $E\text{-}MTA_t$ se descuelga y se lo notifica al CMS.
- CMS envía una petición a $E\text{-}MTA_o$ para parar la emisión del tono de llamada, compromete recursos y pasa a través del trayecto de medios.
- $E\text{-}MTA_o$ envía una DSC-REQ al $CMTS_o$ para comprometer recursos.
- CMS envía una petición a $E\text{-}MTA_t$ para comprometer recursos y pasar a través del trayecto de medios.
- $E\text{-}MTA_t$ envía una DSC-REQ al $CMTS_t$ para comprometer recursos.
- La llamada procede.

En contraste con el modelo IPCablecom en el que el dispositivo de cliente (es decir, E-MTA) inicia los procedimientos de reserva de recurso y activación, el modelo de gestión de recursos multimedia IPCablecom permite la realización de estos pasos mediante apoderado, en nombre del punto de extremo, a través de una interfaz de control por puerta mejorada.

Aquí concluye el breve análisis de los principios de QoS del anexo B/J.112 e IPCablecom. Para más detalles sobre cualquiera de estos temas, bastante complejos, consúltense las correspondientes fuentes primarias [1] y [9]. La cláusula siguiente contiene una visión de conjunto resumida de la arquitectura de multimedia IPCablecom que incluye cada uno de los principales elementos de red y cada una de las interfaces asociadas, como una preparación consiguiente de la Recomendación sobre el protocolo técnico que viene a continuación.

5.2 Arquitectura

El apéndice I describe un marco arquitectural y un modelo de referencia para multimedia IPCablecom. En esta Recomendación se aplica el modelo contenido en el marco arquitectural y se añaden los requisitos normativos que permiten obtener una solución escalable e interoperable, adecuada al despliegue de servicios multimedia IPCablecom.

5.2.1 Tipos de cliente

El informe técnico sobre multimedia IPCablecom define tres clases de tipos de cliente:

- El cliente de tipo 1, que representa puntos de extremo "herederos" existentes (por ejemplo, aplicaciones de PC, consolas de juegos) que carecen de información específica relativa a QoS o capacidades de señalización. Este cliente no sabe nada sobre mensajería de CableModem, IPCable2Home o IPCablecom y, por tanto, no cabe imponerle requisitos relativos a la misma. El cliente de tipo 1 se comunica con un gestor de aplicación para pedirle servicio y no pide (no puede pedir) recursos QoS directamente de la red de acceso del operador de cable.
- El cliente de tipo 2 es similar a un MTA de telefonía IPCablecom-T en el sentido de que soporta la señalización de QoS basada en la Recomendación sobre DQoS de IPCablecom.
- El cliente de tipo 3 pide directamente tratamiento QoS de la red de acceso sin la interacción de un gestor de aplicación. Este cliente está al corriente del RSVP basado en las normas IETF y utiliza dicho protocolo para pedir recursos QoS de la red de acceso de manera directa del CMTS.

La versión actual de la presente Recomendación sólo se refiere al cliente de tipo 1. En consecuencia, esta versión de la Recomendación soporta únicamente el escenario 1, es decir, el escenario basado en "QoS proporcionada mediante apoderado (*proxy*) con empuje (*push*) de la política" descrito en el apéndice I. En ese escenario, el gestor de aplicación se encarga de pedir recursos QoS en nombre del cliente y un servidor de política empuja la petición en sentido descendente hacia el CMTS, que es el dispositivo que se ocupa realmente del establecimiento y la gestión de los flujos de servicio DOCSIS requeridos por la aplicación.

5.2.2 Dispositivos de multimedia IPCablecom

Además del cliente (que normalmente reside en las instalaciones de un abonado), los multimedia IPCablecom requieren varios elementos de red ubicados en, o accesibles a y fiduciarios de, la red del operador de cable. En el proceso de descripción de estos elementos de red a lo largo de la presente Recomendación se utilizan la terminología y los conceptos normalizados del IETF. Para un tratamiento más profundo de la arquitectura global multimedia IPCablecom, incluyendo el análisis de los requisitos y objetivos subyacentes, véase el apéndice I.

Puesto que tanto el COPS [7] como el COPS-PR [19] utilizan los conceptos de punto de imposición de la política (PEP, *policy enforcement point*) y punto de decisión de la política (PDP, *policy decision point*) en escenarios de interacción notablemente diferentes y dado que los multimedia IPCablecom añaden nuevos matices a estos conceptos (sobre todo en la definición del servidor de política), resulta a veces confuso pensar solamente en términos de los PEP y los PDP para entender las responsabilidades de los diversos componentes de la arquitectura de multimedia IPCablecom. A fin de atenuar esa confusión, partes de la presente Recomendación emplean la noción de dominio de control de servicio y de dominio de control de recurso para distinguir el tipo de política que está siendo definida y aplicada.

El dominio de control de recurso (RCD, *resource control domain*) se puede definir como una agrupación lógica de elementos que proporcionan conectividad y gestión de la política a nivel de recursos de red a lo largo de los trayectos de reenvío de paquetes hacia y desde un ordenador anfitrión de extremo. El RCD consta de las entidades CMTS y servidor de política cuyas responsabilidades incluyen la gestión de recursos a lo largo de los trayectos de reenvío de paquetes.

El dominio de control de servicio (SCD, *service control domain*) se define como una agrupación lógica de elementos que ofrecen aplicaciones y contenido a los abonados al servicio. El gestor de aplicación reside en el SCD. Se señala que puede haber uno o más SCD relacionados con un solo RCD. A la inversa, cada RCD puede interactuar con uno o más SCD.

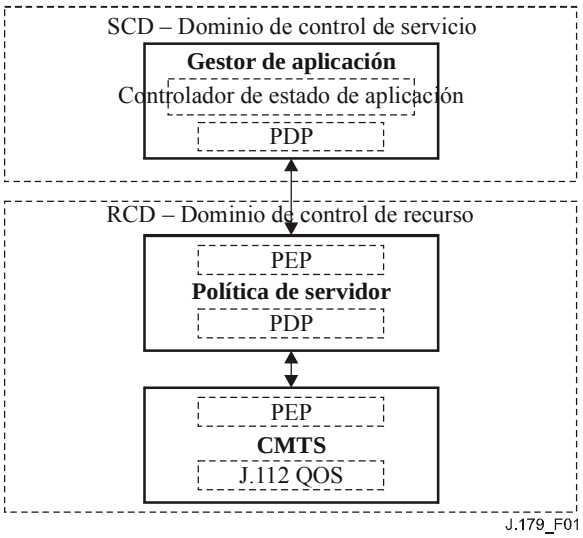


Figura 1/J.179 – Dominios de control de servicio y recurso

En la arquitectura de multimedia IPCablecom, la función principal que realiza el gestor de aplicación es la de mantener el estado, a nivel de sesión, de una aplicación y poner en vigor cualesquiera políticas de dominio de control de servicio (SCD) con respecto a las peticiones de sesión procedentes de los clientes. Si las peticiones de sesión del cliente pasan las verificaciones de política del SCD del gestor de aplicación, el gestor de aplicación convierte la petición de sesión en una petición de recurso y la transfiere al servidor de política para la verificación de política de dominio de control de recurso (RCD). Si la petición de recurso no pasa la verificación de política del RCD, el servidor de política rechaza la petición de recurso y el gestor de aplicación rechaza consecuentemente la petición de sesión del cliente. Si, no obstante, la petición de recurso pasa las verificaciones del RCD del servidor de política, el servidor de política reenvía la petición al CMTS para el control de admisión a nivel de red.

Básicamente, las funciones de los diversos componentes de multimedia IPCablecom son como sigue:

- El gestor de aplicación es responsable del estado a nivel de aplicación o sesión y de la aplicación de la política del SCD.
- El servidor de política es responsable de la aplicación de la política del RCD y de la gestión de las relaciones entre los gestores de aplicación y los CMTS.
- El CMTS es responsable de la realización del control de admisión y de la gestión de los recursos de red mediante los flujos de servicio DOCSIS.

Quizá convenga aclarar aquí la utilización de las expresiones "control de admisión" y "autorización de política". A los efectos de la presente Recomendación, por control de admisión se entiende por lo general el proceso de gestión de un fondo común finito de recursos a nivel de red (por ejemplo, anchura de banda de red de acceso, miniintervalos de tiempo DOCSIS del calendarizador o recursos de CMTS que soportan puertas y temporizadores, etc.) y de admisión de peticiones dirigidas a ese fondo común. Por motivos de calidad de funcionamiento, el control de admisión se lleva a cabo normalmente de forma directa en los elementos de red que gestionan el trayecto de reenvío de paquetes (tal como el CMTS), si bien algunas implementaciones complejas de servidor de política

pueden optar por mantener el estado asociado a los recursos de red, complementando de esa manera el proceso de control de admisión y contribuyendo al mismo.

Por el contrario, la expresión autorización de política se emplea para describir políticas de utilización combinada de nivel superior (por ejemplo, el número de autorizaciones concurrentes para un determinado abonado o servicio) que constituyen la estrategia de gestión de red de un operador de cable. La autorización de política se define y se pone en vigor casi siempre en el servidor de política.

En el resto de la presente cláusula se describen con más detalle cada uno de estos componentes arquitecturales y las interfaces asociadas a los mismos.

5.2.2.1 Gestor de aplicación (AM)

Como se ha indicado en el resumen precedente, el gestor de aplicación es una entidad de red que define políticas del SCD, coordina las peticiones, iniciadas por el abonado, de sesiones de aplicación con acceso a los recursos necesarios para cumplimentar esas peticiones y mantiene el estado a nivel de aplicación.

El AM puede residir en la red del operador de cable o puede residir fuera de ese dominio e interactuar con la red del operador de cable vía una relación fiduciaria particular (definida normalmente por, y puesta en vigor en base a, un acuerdo de nivel de servicio). De manera similar, el AM puede estar bajo el control directo del operador o puede ser controlado por un tercero. Cualquier gestor de aplicación dado puede comunicar con uno o más servidores de política por la red del operador; del mismo modo, uno o más gestores de aplicación pueden comunicar con cualquier servidor de política dado por la red del operador (en tanto en cuanto exista una relación fiduciaria apropiada).

En la mayoría de los escenarios de despliegue de servicios previstos, el gestor de aplicación comunicará con un cliente por medio de un protocolo de señalización que queda fuera del alcance de la presente Recomendación. Utilizando este protocolo no especificado, el AM autentica y autoriza peticiones de cliente teniendo en cuenta las políticas del dominio de control de servicio. En el caso de las peticiones de cliente que pasan esas verificaciones, el AM determina los parámetros de QoS que, en concreto, se necesitan para la entrega del servicio al cliente en base al conocimiento que tiene del servicio solicitado. A continuación envía la petición de recursos al servidor de política apropiado, que puede denegarla, en función de cual sea la política de la red o el RCD, o puede pasarla al CMTS a efectos de control de admisión y puesta en vigor.

5.2.2.2 Servidor de política (PS)

Según el análisis de RFC 2753 [18], el marco de gestión de políticas que subyace en los multimedia IPCablecom se basa en la labor desarrollada por el grupo de trabajo sobre el protocolo de asignación de recursos (RAP, *resource allocation protocol*) del IETF. El servidor de política está situado entre el gestor de aplicación y el CMTS, por lo que desempeña de manera simultánea un cometido dual de "apoderado" para las peticiones de sesión iniciadas por el AM y de "centinela" para definir y aplicar la política del dominio de control de recurso.

Como se describe en [18] y de conformidad con el modelo de DQoS de IPCablecom, el servidor de política sirve de punto de decisión de la política (PDP) en relación con el CMTS en el sentido de que el servidor de política implementa los procedimientos de autorización y gestión de recursos definidos por el operador de cable. A la inversa, el servidor de política asume el papel de punto de imposición de la política (PEP) en relación con el gestor de aplicación ya que administra mediante apoderado los mensajes de control por puerta hacia y desde el elemento CMTS.

Para visitar de nuevo el escenario de interacción, el gestor de aplicación envía peticiones de política al servidor de política. El servidor de política actúa a modo de "centinela" observador de esas peticiones y aplica un conjunto de reglas de política provisionadas previamente por el operador de cable. Una vez pasadas las verificaciones, el servidor de política actúa como un "apoderado"

respecto al gestor de aplicación y el CMTS, reenviando la petición de política y devolviendo cualquier respuesta relacionada con la misma. Cada transacción de petición de política debe ser procesada de manera individual.

Las decisiones de tipo político pueden basarse en un cierto número de factores, tales como:

- Los parámetros asociados a la petición y el estado de los recursos disponibles.
- La identidad del cliente de que se trate y la información de perfil asociada.
- Los parámetros de la aplicación.
- Consideraciones relativas a la seguridad.
- La hora del día.

Entre las funciones principales del servidor de política figuran las siguientes:

- Un mecanismo de petición de decisión de la política, invocado por los gestores de aplicación.
- Un mecanismo de "control" de la petición de decisión de la política, con el que se aplican las reglas de política instaladas.
- Un mecanismo de entrega de decisiones de la política, utilizado para instalar las decisiones de tipo político en el CMTS.
- Un mecanismo que permita la administración de los mensajes de gestión de QoS al CMTS mediante apoderado en nombre del gestor de aplicación.
- Una interfaz de registro de eventos con un servidor mantenedor de registros que se utiliza para registrar cronológicamente las peticiones de política, que puede a su vez estar correlacionado con registros de utilización de recursos de red.

Puesto que el servidor de política funciona como un apoderado entre los elementos AM y CMTS (con interfaces complementarias de cliente y servidor), algunos operadores de cable pueden optar por el despliegue de capas múltiples de servidores de política y denegar determinadas decisiones de tipo político entre estos servidores para satisfacer requisitos asociados a la escalabilidad y la tolerancia frente a averías.

5.2.2.2.1 Servidores de política basados en estados y servidores de política no basados en estados

Hay dos clases fundamentales de servidores de política – los que se basan en estados y los que no se basan en estados. La denominación de servidor de política no basado en estados no es del todo exacta ya que el servidor se basa en los estados en la medida en que lo necesite para establecer la correspondencia entre las peticiones del gestor de aplicación y el CMTS apropiado y mantiene el estado de la sesión de COPS, mientras que un servidor de política no basado en estados en sentido estricto no mantiene ningún estado en ninguna de las sesiones de medios. Los servidores de política basados en estados se presentan en diversas formas – algunos participan en el control de admisión y de ese modo supervisan los atributos de QoS de las sesiones de medios activas, otros dejan el control de QoS y de admisión al CMTS pero supervisan las peticiones de servicio en base al tiempo o en base al volumen procedentes del gestor de aplicación y otros servidores de política se hallan en algún punto intermedio entre esos extremos.

La razón por la que hay una diversidad de tipos de servidor de política es que existen múltiples entornos que los operadores tratan de soportar. Es posible, por ejemplo, que algunos operadores deseen soportar multimedia IPCablecom en los mismo CMTS que utilizan para la telefonía IPCablecom y quizá deseen disponer de un único CMS/servidor de política que tenga una visión más amplia de los recursos de red que se utilizan. Por otro lado, algunos operadores quizá deseen actuar en un entorno de sólo multimedia IPCablecom o deseen utilizar mecanismos más simples excitados por el CMTS a efectos de la partición de los recursos de multimedia IPCablecom y los de

telefonía. Estas configuraciones más sencillas tienen unos requisitos menos rigurosos en cuanto al punto hasta el cual un servidor de política mantiene el estado.

Los requisitos de estado del servidor de política pueden regirse también por el nivel de confianza entre el servidor de política y el gestor de aplicación; un servidor de política basado en estados puede vigilar el comportamiento del control de sesión del gestor de aplicación más fácilmente que un servidor de política no basado en estados. Por ello, un servidor de política basado en estados puede ser lo más apropiado en el caso de operadores que soporten gestores de aplicación como tercera parte. Otros operadores pueden basarse en aspectos económicos para establecer sus relaciones fiduciarias con gestores de aplicación o pueden controlar a los propios gestores de aplicación. En tales casos, lo más conveniente puede ser un servidor de política no basado en estados.

Dado que es imposible clasificar todos los distintos componentes de una sesión de medios y el estado de QoS de una red que mantiene un servidor de política, el protocolo se ha concebido de modo que sea independiente de esa dificultad. Un servidor de política basado en estados analiza minuciosamente la información sobre la sesión de medios de multimedia IPCablecom a partir de las peticiones del gestor de aplicación para las que actúa como apoderado; cualquier otra información que requiera se obtiene por mecanismos que quedan fuera del alcance de la presente Recomendación. El CMTS y el gestor de aplicación no hacen ninguna distinción respecto al tipo de servidor de política al que están conectados y el protocolo se diseña de manera que el tipo de servidor de política sea transparente para el punto de extremo. El tipo de servidor de política sólo le importa al operador.

Es posible que algunos tipos de servidores de política traten de colaborar en el control de admisión y tengan una visión más amplia de la red y sus recursos, por lo que quizá se planteen cuestiones adicionales a propósito de la sincronización de estados al diseñar una red que contiene más de uno de esos tipos de servidores de política. Corresponde al operador garantizar que los esfuerzos de estos servidores de política no resultan perjudicados por una red que incluya otros servidores de política autónomos.

5.2.2.2.2 Modificación de peticiones y respuestas por los servidores de política

Aunque nominalmente forma parte del dominio de control de recursos, el servidor de política puede ser un intermediario entre los dominios de control de servicio y de control de recurso, además de implementar los procedimientos de autorización y de gestión de recursos definidos por el operador. En cualquiera de estas capacidades puede modificar la petición entrante antes de reenviarla al CMTS.

Al actuar como intermediario entre los dominios SCD y RCD, el servidor de política puede traducir los campos de los formatos o escalas utilizados en el SCD a los formatos o escalas utilizados en el RCD. Por ejemplo, el servidor de política puede modificar la "prioridad" de una petición procedente de un gestor de aplicación (lo que es especialmente importante cuando el AM se halla fuera de la red MSO) de modo que este campo prioridad utilice una escala adecuada en todo el dominio RCD del operador. En su condición de intermediario, el servidor de política puede aplicar traducción bidireccional, en otras palabras, debería traducir las peticiones del AM al CMTS y "destraducir" las respuestas del CMTS al AM. Esta capacidad puede ser soportada por servidores de política basados en estados recordando la petición original, y también por servidores de política no basados en estados, si la función es invertible.

La modificación de ciertos objetos, concretamente los objetos clasificador y perfil de tráfico, puede causar problemas operacionales en el AM de origen. Por lo tanto, estos objetos NO DEBEN ser modificados por el servidor de política. Fuera de estas excepciones, todos los demás objetos pueden ser modificados y cambiados de política a discreción del servidor de política con arreglo a las reglas de política provisionadas.

5.2.2.3 Sistema de terminación de módem de cable (CMTS)

Es importante tener en cuenta, al describir el cometido del elemento de red CMTS, la relación entre las funcionalidades de CableModem, IPCablecom-T y multimedia IPCablecom. Si bien cada una de estas series de Recomendaciones se refiere a un conjunto específico de requisitos funcionales, se ha definido, también cada una de ellas, de manera que puedan construirse implementaciones correspondientes de forma modular; el control por puerta, ya sea de multimedia IPCablecom-T o de IPCablecom, puede organizarse en forma de capa dispuesta sobre una base constituida por el CMTS conforme al anexo B/J.112, con la posibilidad de agregar funcionalidades complementarias adicionales según sugiera la actividad comercial. Conviene destacar, además, el hecho de que tanto las variantes de telefonía como las de multimedia tienen una considerable semejanza arquitectural, lo que representa un activo importante de la arquitectura IPCablecom y hace posible la reutilización en los modelos de gestión de puerta subyacentes.

El CMTS de multimedia IPCablecom es una versión generalizada del CMTS de IPCablecom-T que se ha definido para entregar servicios de telefonía en redes de IPCablecom-T. Al CMTS corresponde cumplimentar las peticiones de QoS recibidas de uno o más servidores de política. Esta función la lleva a cabo instalando puertas, que son similares a las definidas en [9]; las puertas permiten que el módem de cable del abonado pida recursos de red del CMTS mediante la creación de flujos DOCSIS dinámicos con niveles garantizados de QoS. El CMTS envía además mensajes de evento detallando la utilización real de los recursos QoS al servidor mantenedor de registros.

5.2.2.4 Servidor de mantenimiento de registros (RKS)

El servidor de mantenimiento de registros de multimedia IPCablecom realiza una función similar a la del RKS en IPCablecom-T [10]. Recibe mensajes de evento correspondientes a decisiones de tipo político procedentes del servidor de política y mensajes de evento relativos a la utilización de recursos QoS procedentes del CMTS.

En la arquitectura de multimedia IPCablecom, el servidor de mantenimiento de registros no recibe mensajes directamente del gestor de aplicación. Sin embargo, el gestor de aplicación puede incorporar datos opacos en mensajes que envía al servidor de política y esos datos se pueden incluir a continuación en mensajes de evento que son enviados subsiguientemente al RKS.

5.2.3 Interfaces de multimedia IPCablecom

Los multimedia IPCablecom se basan en la serie de Recomendaciones sobre IPCablecom-T. Cuando una interfaz de multimedia IPCablecom tiene un corolario en IPCablecom-T, los multimedia IPCablecom utilizan el mismo protocolo o una ampliación del mismo.

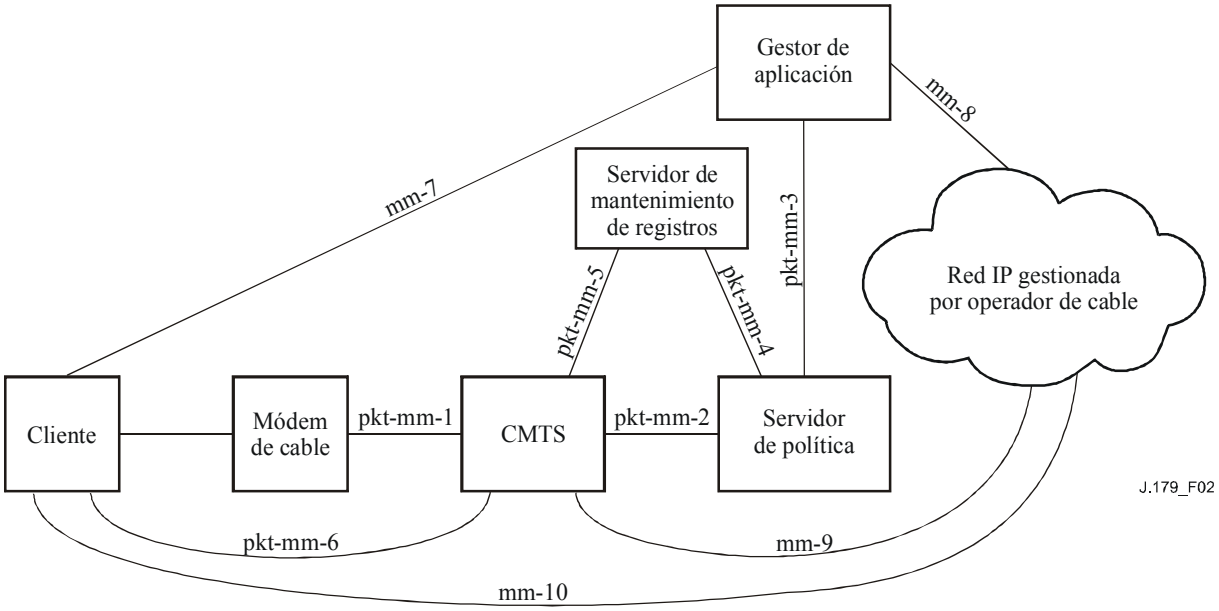


Figura 2/J.179 – Marco arquitectural de multimedia IPCablecom

Cuadro 1/J.179 – Interfaces de multimedia IPCablecom

Interfaz	Descripción	Notas
pkt-mm-1	CMTS – CM	El módem de cable (CM, *cable modem*) puede pedir QoS del CMTS vía señalización DSx del anexo B/ J.112. De manera alternativa, el CMTS puede indicar al CM que establezca, elimine o cambie un flujo de servicio DOCSIS para cumplimentar una petición de QoS, de nuevo vía señalización DSx.
pkt-mm-2	PS – CMTS	Esta interfaz es fundamental para el marco de gestión de políticas. Controla las decisiones de tipo político que pueden ser: a) empujadas por el servidor de política (PS, *policy server*) hacia el CMTS o b) extraídas del PS por el CMTS. La interfaz permite también efectuar peticiones de QoS mediante apoderado en nombre de un cliente. En algunos escenarios, esta interfaz puede ser utilizada además para informar al PS cuando los recursos QoS se han quedado inactivos.
pkt-mm-3	AM – PS	El gestor de aplicación (AM, *application manager*) puede pedir que el PS instale una decisión de tipo político en el CMTS en nombre del cliente. Esta interfaz puede se utilizada además para informar al AM de los cambios en el estado de los recursos QoS.
pkt-mm-4	PS – RKS	El PS envía mensajes de evento al servidor de mantenimiento de registros (RKS, *record keeping server*) para el seguimiento de las decisiones de tipo político relacionadas con la QoS.
pkt-mm-5	CMTS – RKS	El CMTS envía al RKS mensajes de evento para el seguimiento de las peticiones y la utilización de la QoS (por ejemplo, adiciones de flujos de servicio, cambios, supresiones y medidas de volumen).

Cuadro 1/J.179 – Interfaces de multimedia IPCablecom

Interfaz	Descripción	Notas
pkt-mm-6	Cliente – CMTS	El cliente puede utilizar esta interfaz para pedir y gestionar directamente recursos de red de QoS. Si se autorizan, estos recursos son proporcionados por el CMTS.
mm-7	Cliente – AM	Esta interfaz puede ser utilizada por el cliente para interactuar con el AM y pedir y gestionar indirectamente recursos QoS. Esta interfaz queda fuera del alcance de esta versión de la presente Recomendación.
mm-8	AM – Par	El AM puede utilizar esta interfaz para interactuar con alguna otra entidad que forme parte de la aplicación en cuestión. Esta interfaz queda fuera del alcance de esta versión de la presente Recomendación.
mm-9	CMTS – red IP gestionada por operador de cable	Esta interfaz del CMTS puede ser utilizada para el soporte de peticiones de QoS de extremo a extremo más allá de la red de acceso. Esta interfaz queda fuera del alcance de esta versión de la presente Recomendación.
mm-10	Cliente – Par	El cliente puede utilizar esta interfaz para interactuar con alguna otra entidad que forme parte de la aplicación en cuestión. Esta interfaz queda fuera del alcance de esta versión de la presente Recomendación.

5.2.3.1 Interfaz entre cliente y gestor de aplicación (mm-7)

En la presente Recomendación no se considera la interfaz entre el cliente y el gestor de aplicación. Normalmente, el gestor de aplicación autenticará al cliente y se asegurará de que éste tiene derecho al servicio multimedia, mediante algún procedimiento que queda fuera del alcance de la presente Recomendación. El cliente puede, por ejemplo, iniciar una sesión para conectarse a una página web y pedir el servicio dando un nombre de usuario y una contraseña. Cualquiera que sea la forma en que esto se consiga, el gestor de aplicación podrá identificar inequívocamente el módem o los módems de cable a los que habrá de proporcionarse el servicio, ya que para poder proporcionar QoS hay que facilitar esta información al operador de red.

5.2.3.2 Interfaz entre gestor de aplicación y servidor de política (pkt-mm-3)

Esta interfaz corresponde a la interfaz de IPCablecom-T entre un agente de llamada y un controlador de puerta. En IPCablecom-T, la interfaz está oculta y no es verificable y, por tanto, no hay requisitos de protocolo preexistentes a propósito de esta interfaz.

Los multimedia IPCablecom requieren la utilización de COPS [7] en esta interfaz. Para simplificar la arquitectura y hacer posible la existencia de múltiples niveles de elementos servidor de política entre el gestor de aplicación y el CMTS, esta interfaz reproduce, en la medida de lo posible, la interfaz entre el servidor de política y el CMTS. Aunque el gestor de aplicación es el que solicita la autorización de un recurso al servidor de política, de hecho emite esa petición en un mensaje Decisión COPS, en vez de un mensaje Petición COPS. De esta manera, la interfaz entre el gestor de aplicación y el servidor de política puede parecer idéntica a la interfaz entre el servidor de política y el CMTS. El gestor de aplicación es el PDP con respecto al servidor de política y el servidor de política es el PEP con respecto al gestor de aplicación.

Cuando un gestor de aplicación está conforme con prestar un servicio a un cliente, envía un mensaje Decisión COPS que contiene (por lo menos) la información siguiente en forma de objetos COPS:

- La identidad del gestor de aplicación que hace la petición.
- La identidad del cliente o los clientes a los que se ha de prestar el servicio.
- La o las FlowSpec de RSVP que especifican las capacidades máximas de tráfico para la sesión.

En su respuesta, el servidor de política incluye un testigo de autorización, el ID de puerta, que le proporciona el CMTS.

5.2.3.3 Interfaz entre servidor de política y CMTS (pkt-mm-2)

Esta interfaz es básicamente idéntica a la interfaz equivalente (entre CMTS y controlador de puerta) en IPCablecom-T. Al igual que en IPCablecom-T, el COPS se utiliza para transferir información de política entre el servidor de política y el CMTS. El CMTS actúa como un PEP de COPS y el servidor de política actúa como un PDP de COPS. Siguiendo el modelo IPCablecom-T, el servidor de política inicia la comunicación de una sesión de multimedia enviando un mensaje Gate-Set de DQoS (que es un mensaje Decisión COPS no solicitado) al CMTS.

Este mensaje contiene (por lo menos):

- ID de gestor de aplicación.
- ID de abonado.
- GateSpec.
- FlowSpec o FlowSpecs.
- Clasificador.

El CMTS responde, como en DQoS, con un mensaje Gate-Set-Ack o un mensaje Gate-Set-Err (ambos son mensajes Informe COPS).

Si el CMTS responde positivamente (es decir, con un mensaje Gate-Set-Ack), incluye un ID de puerta. Como en IPCablecom-T, el ID de puerta actúa a modo de testigo de la autorización. A diferencia de lo que ocurre en IPCablecom-T, el testigo no se pasa finalmente al cliente (puesto que los puntos de extremo cliente de tipo 1 no tienen conocimiento de IPCablecom); más bien es retenido por el servidor de política (si se basa en estados) y por el gestor de aplicación, permitiéndoles así enviar instrucciones relativas a la sesión al CMTS, bien directamente en el caso del servidor de política o bien indirectamente vía el servidor de política en el caso del gestor de aplicación.

5.2.3.4 Interfaz entre servidor de mantenimiento de registros y servidor de política (pkt-mm-4) e interfaz entre servidor de mantenimiento de registros y CMTS (pkt-mm-5)

Las interfaces entre el servidor de mantenimiento de registros y el servidor de política y entre el servidor de mantenimiento de registros y el CMTS son idénticas a las interfaces equivalentes (del CMS y el CMTS, respectivamente) en IPCablecom-T (véase [10]). Estas interfaces se utilizan para llevar mensajes de evento IPCablecom, que emplean el formateo RADIUS. En los multimedia IPCablecom, los mensajes de evento llevan información minuciosa correspondiente al servicio entregado, incluida la hora exacta en que se crean y se eliminan los flujos de servicio y (facultativamente) el volumen de tráfico que ha pasado por el flujo de servicio mientras estaba vigente.

5.2.4 Información de estado

En esta subcláusula se da una visión general de la situación del estado en un sistema multimedia IPCablecom. Además de mantener una información minuciosa sobre el estado, los dispositivos envían información relativa a las transiciones de estados al servidor de mantenimiento de registros a efectos tales como los de facturación, detección de fraudes, reconstrucción de sesiones, etc.

5.2.4.1 Estado de la aplicación

El gestor de aplicación se encarga en todo momento de mantener un conocimiento detallado del estado de la sesión de medios de la aplicación. Los pormenores de cómo realiza esto quedan fuera del alcance de la presente Recomendación, pero es importante tener en cuenta que no se requieren

ni están previstos otros dispositivos que no sean el gestor de aplicación para mantener cualquier conocimiento sobre el estado de la aplicación.

El gestor de aplicación puede, no obstante, informar sobre el estado de la sesión facilitando mediante apoderado dicha información, vía el servidor de política, al servidor de mantenimiento de registros. Además, alguna información de estado de carácter básico (por ejemplo, el hecho de que se hayan pedido recursos) es enviada automáticamente desde el servidor de política al servidor de mantenimiento de registros.

5.2.4.2 Estado de los recursos QoS

El CMTS está naturalmente al corriente de la situación pormenorizada de los flujos que gestiona. El servidor de política (si se trata de un servidor de política basado en estados) puede mantener también una cierta noción del estado de los recursos QoS en un solo CMTS; además, puede cotejar la información de varios CMTS para conocer (únicamente él) el estado de QoS de todo el sistema. Algo que puede ser importante si, por ejemplo, un operador ha establecido una política según la cual no se permite a una aplicación particular consumir más allá de un porcentaje especificado de los recursos totales del sistema. En una red que sólo tenga servidores de política no basados en estados, los CMTS son los únicos dispositivos que mantienen información sobre el estado de la QoS. Puesto que los servidores de política no basados en estados no mantienen ID de puerta (identificadores de puerta), no pueden ni siquiera interrogar a un CMTS para obtener información sobre una determinada sesión de multimedia.

Siempre que un recurso QoS transita de un estado a otro y siempre que un recurso QoS es suprimido, se envía el mensaje de evento correspondiente del CMTS al servidor de mantenimiento de registros.

6 Descripción de la interfaz de autorización

En esta cláusula se describe la interfaz entre el gestor de aplicación y el servidor de política y la interfaz entre el servidor o los servidores de política y el CMTS.

La interfaz entre el gestor de aplicación y el servidor de política es, en su función de traslación, simétrica a la interfaz entre el servidor de política y el CMTS. Las interfaces se utilizan para pasar información de autorización, reserva y activación al CMTS y para proporcionar información de estado desde el CMTS al servidor de política y desde el servidor de política al gestor de aplicación.

El gestor de aplicación es el PDP del dominio de control de servicio. El servidor de política es el PEP con respecto al gestor de aplicación y aplica políticas del dominio de control de recurso. El servidor de política es un PEP con respecto al CMTS y el CMTS es el PEP con respecto al servidor de política y se halla en el trayecto efectivo de reenvío de paquetes.

En esta cláusula se describe la utilización del protocolo de COPS para transportar mensajes de QoS de IPCablecom entre el gestor de aplicación y el servidor de política y entre el servidor de política y el CMTS.

6.1 Puertas: El marco de control de la QoS

Una puerta de multimedia IPCablecom es la representación lógica de una decisión de la política que ha sido instalada en el CMTS. La puerta se utiliza para controlar el acceso de un flujo IP único a los servicios con QoS mejorada proporcionados por una red de cable del anexo B/J.112. Las puertas son unidireccionales; una sola puerta controla el acceso a un flujo en sentido ascendente o en sentido descendente, pero no en ambos sentidos. En el caso de una sesión IP bidireccional, se necesitan dos puertas, una para el sentido ascendente y otra para el descendente, identificadas cada una de ellas mediante un ID de puerta exclusivo. Es importante tener en cuenta que lo anterior constituye una diferencia fundamental con respecto a IPCablecom-T, en donde un solo ID de puerta puede hacer referencia tanto a la puerta del sentido ascendente como a la del descendente.

En los multimedia IPCablecom, cada puerta tiene un ID de puerta distinto. La puerta define las capacidades máximas de autorización, reserva y compromiso que han de ser utilizadas por el CMTS para realizar las operaciones de autorización, reserva y compromiso.

En todos los escenarios, el CMTS DEBE efectuar verificaciones de control de admisión de las capacidades máximas para asegurarse de que la capacidad máxima comprometida es menor o igual que la reservada y la capacidad máxima reservada es menor o igual que la autorizada (para los requisitos de control de admisión DOCSIS específicos, véase [1]).

En el modelo 'QoS proporcionada mediante apoderado con empuje de la política' (escenario 1), la información de una puerta es utilizada por el CMTS para crear el flujo de servicio del anexo B/J.112 directamente, después de que el CMTS efectúe las verificaciones necesarias de control de admisión de las capacidades. En los otros dos modelo indicados en el apéndice I, 'QoS pedida por el cliente con empuje de la política' (escenario 2) y 'QoS pedida por el cliente con extracción de la política' (escenario 3), el CMTS utiliza la información de la puerta para efectuar el control de admisión de los recursos pedidos por el cliente; el CMTS no inicia la creación de los flujos. El gestor de aplicación es responsable del envío de los mensajes de puerta al servidor de política y el servidor de política es responsable de la aplicación de las reglas de política y del envío a continuación los mensajes de control por puerta al CMTS.

Una puerta consta de los siguientes elementos, que se describen más adelante en la presente cláusula:

- ID de puerta.
- AMID.
- ID de abonado.
- GateSpec.
- Clasificador.
- Perfil de tráfico.
- Información de generación de evento (facultativo).
- Límite de utilización basado en tiempo (facultativo).
- Límite de utilización basado en volumen (facultativo).
- Datos opacos (facultativo).

El ID de puerta es el asa de la puerta. El ID de puerta es asignado por el CMTS y es utilizado por el gestor de aplicación, el servidor de política y el cliente para hacer referencia a la puerta.

AMID es el asa que identifica al gestor de aplicación.

El ID de abonado identifica de manera exclusiva al cliente para el que se fija la política.

GateSpec describe los parámetros de autorización específicos que definen una puerta (es decir, límites de QoS, temporizadores, etc.).

El clasificador describe el flujo o los flujos IP cuya correspondencia se establecerá con el flujo de servicio DOCSIS.

El perfil de tráfico describe los atributos de QoS del flujo de servicio utilizado en soporte del flujo IP.

La información de generación de evento contiene información utilizada por el CMTS a efectos contables y de notificación de la utilización.

El límite de utilización basado en volumen define un valor máximo del volumen que no podrá ser rebasado por el flujo que pase por la puerta.

El límite de utilización basado en tiempo define un valor máximo del tiempo que no podrá ser rebasado por el flujo que pase por la puerta.

El elemento datos opacos representa un objeto de carácter general que permanece opaco a los elementos CMTS y PS, pero que puede contener datos de importancia para el AM. Este objeto facultativo, si lo proporciona el AM, está retenido en el CMTS y se devuelve en todas las respuestas asociadas (véase 6.4.2.11).

Estos elementos se comunican al servidor de política y al CMTS vía objetos COPS y se describen con más detalle más adelante en la presente cláusula. Durante la instalación de la puerta, se comunica al CMTS la información anterior. Una vez completada la instalación, se puede crear un flujo de servicio DOCSIS. Tras la creación del flujo de servicio DOCSIS, la puerta tiene asociado un elemento adicional, el flujo de servicio DOCSIS. Hay una correspondencia estricta de uno a uno entre un flujo de servicio DOCSIS y una puerta.

Una puerta transita a través de múltiples estados. En los escenarios 2 y 3, en donde la entidad cliente se encarga de reservar y activar a continuación los flujos de servicio DOCSIS, la puerta multimedia se comporta de manera muy similar a la de una puerta de DQoS de IPCablecom-T. Cuando el servidor de política instala la puerta en el CMTS, se dice que la puerta está en un estado 'autorizado'. Permanece en ese estado hasta que es suprimida de manera explícita por el servidor de política (o, con menos probabilidad, es suprimida por cualquier motivo por el propio CMTS) o hasta que llega una petición de flujo dinámico procedente del cliente.

Cuando el cliente pide que se añada un flujo de servicio dinámico, presenta el ID de puerta como testigo de autorización. El CMTS utiliza el ID de puerta para efectuar el control de admisión en el flujo dinámico DOCSIS cotejándolo con la capacidad máxima autorizada definida por la puerta. En el escenario 1, el servidor de política indica al CMTS que transite entre los estados en nombre del gestor de aplicación y el CMTS es la entidad responsable de iniciar y eliminar los flujos de servicio DOCSIS. Este comportamiento se describe en la cláusula relativa a la transición de estados de la presente Recomendación. Cuando al CMTS se le indica que elimine un flujo de servicio DOCSIS, la puerta asociada a dicho CMTS permanece en esa situación hasta que es suprimida de manera explicita por el PS/AM o hasta que concluye su temporización y sus recursos son recuperados por el CMTS (véase 6.5.8). Sin embargo, cuando el PS/AM suprima una puerta, el CMTS suprimirá el flujo de servicio DOCSIS asociado.

6.1.1 Identificador de puerta (GateID)

Un identificador de puerta (ID de puerta) es un identificador atribuido locamente por el CMTS en donde reside la puerta. El ID de puerta DEBE estar asociado a una sola puerta. Mientras que el modelo de control por puerta de DQoS de IPCablecom-T asumía por lo general la existencia de un par de puertas unidireccionales (una en sentido ascendente y otra en sentido descendente) por cada ID de puerta que soportará una sesión de voz típica de dos vías, la relación puerta/ID de puerta es aquí de uno a uno de manera explícita, con lo que resulta más fácil soportará una amplia gama de servicios multimedia.

Cuando el gestor de aplicación envía una petición Gate-Set, dicha petición induce al servidor de política a enviar un mensaje Gate-Set al CMTS. Cuando el CMTS responde con un acuse de recibo que contiene el ID de puerta, el servidor de política envía esa respuesta, incluido el ID de puerta, de vuelta al gestor de aplicación. Se señala que, ante la posibilidad de que exista una relación de muchos a muchos entre un PS y el CMTS, no se puede garantizar que el ID de puerta asignado por un CMTS sea único en toda la red, por lo que los PS pueden utilizar el AMID del AM junto con el ID de abonado y el ID de puerta para identificar la puerta de forma exclusiva.

A continuación se describe un algoritmo que puede ser empleado para asignar valores de ID de puerta. La palabra de 32 bits se divide en dos partes: una parte índice y una parte aleatoria. La parte índice identifica la puerta con un índice dentro de un pequeño cuadro, mientras que la parte aleatoria da al valor un cierto nivel de oscuridad. Con independencia del algoritmo elegido, el

CMTS DEBERÍA tratar de minimizar la posibilidad de que existan ambigüedades en el ID de puerta asegurando que ningún ID de puerta se utiliza dentro de los tres minutos siguientes a su cierre o supresión precedente. En el caso del algoritmo propuesto, esto podría conseguirse mediante un simple incremento de la parte índice por cada ID de puerta asignado consecutivamente, retornando a cero cuando se alcance el valor entero máximo de la parte índice.

6.1.2 Identificador de gestor de aplicación (AMID)

A cada gestor de aplicación se le adjudica previamente un AMID que es exclusivo dentro del universo de un proveedor de servicio único; el gestor de aplicación incluye este identificador en todos los mensajes que envía al servidor de política. El servidor de política pasa transparentemente esta información al CMTS vía mensajes de control por puerta. El CMTS DEBE devolver el AMID asociado a la puerta al servidor de política. El servidor de política utiliza esta información para asociar mensajes de puerta a un determinado gestor de aplicación.

El AMID DEBE ser un valor globalmente exclusivo asignado al gestor de aplicación por el proveedor de servicio. El gestor de aplicación DEBE utilizar el AMID asignado en todas sus interacciones con servidores de política. Puesto que el gestor de aplicación puede ser explotado por un tercero y un solo gestor de aplicación podría interactuar con múltiples operadores proveedores de servicio, se señala que a un solo gestor de aplicación física se le pueden adjudicar múltiples AMID.

6.1.3 Identificador de abonado (SubscriberID)

El identificador de abonado (ID de abonado), formado por la dirección IP del dispositivo CPE del cliente o el CM, identifica al usuario que pide el servicio. En entornos de redes complejos esta dirección puede ser utilizada para encaminar mensajes de control por puerta entre un cierto número de servidores de política y para determinar qué CMTS está prestando servicio a un punto de extremo determinado. Además de por su dirección IP, un abonado puede ser identificado mediante un FQDN o algunos datos opacos (objeto definido más adelante) inherentes al servicio en cuestión.

6.1.4 Especificación de puerta (GateSpec)

La GateSpec describe algunos atributos de nivel alto de la puerta y contiene información a propósito del tratamiento de otros objetos especificados en el mensaje de puerta. A continuación se indica la información contenida en una GateSpec:

- ID de puerta.
- ID de clase de sesión.
- Sentido.
- Temporizador autorizado.
- Temporizador reservado.
- Temporizador comprometido.
- Temporizador de recuperación comprometida.
- Contraorden de DSCP/TOS.

El ID de puerta identifica de manera específica la puerta para la que debería efectuarse la operación.

El ID de clase de sesión proporciona al gestor de aplicación y al servidor de política una manera de agrupar puertas en clases diferentes con características de autorización diferentes. Podría utilizarse, por ejemplo, el ID de clase de sesión para representar algún esquema de priorización o de apropiación con prioridad que permitiría al servidor de política o al CMTS apropiarse de una puerta autorizada previamente facilitando la autorización de una puerta nueva con mayor derecho.

El sentido indica si la puerta es para un flujo ascendente o descendente. Dependiendo de cuál sea el sentido, el CMTS DEBE reservar y activar de conformidad los flujos DOCSIS.

El temporizador autorizado limita la cantidad de tiempo que la autorización debe permanecer válida antes de proceder a su reserva (véase 6.2).

El temporizador reservado limita la cantidad de tiempo que la reserva debe permanecer válida antes de que los recursos sean comprometidos (véase 6.2).

El temporizador comprometido limita la cantidad de tiempo durante el cual un flujo de servicio comprometido puede permanecer en reposo.

El temporizador de recuperación comprometida limita el tiempo que puede permanecer un flujo de servicio comprometido sin recibir el siguiente mensaje de renovación del PS/AM una vez que éste ha recibido la notificación de inactividad (véase 6.2).

El campo contraorden de DSCP/TOS puede ser utilizado para invalidar el campo DSCP/TOS de paquetes asociados al flujo de servicio DOCSIS que corresponde a la puerta. Este campo PUEDE no estar especificado, en cuyo caso el CMTS no sobreescribe en el campo DSCP/TOS del paquete. Este campo PUEDE ser utilizado tanto en el sentido ascendente como en el descendente.

6.1.5 Clasificador

Se DEBE definir un clasificador para una puerta. Además, los clasificadores pueden estar incluidos en el Gate-Set original. Los clasificadores pueden ser añadidos o suprimidos en un Gate-Set subsiguiente. Las implementaciones cumplidoras DEBEN ser capaces de soportar un mínimo de cuatro clasificadores cuando procesen un mensaje Gate-Set. El clasificador identifica el flujo IP cuya correspondencia se establecerá con el flujo de servicio DOCSIS asociado a la puerta. El clasificador utilizado para construir un flujo de servicio DEBE concordar con el clasificador especificado para la puerta. En el escenario 1, cuando el CMTS crea el flujo dinámico DEBE utilizar el clasificador de puerta como clasificador del flujo de servicio DOCSIS.

Un clasificador es una tupla de ocho elementos:

- Protocolo.
- Origen IP.
- Puerto de origen.
- Destino IP.
- Puerto de destino.
- Prioridad.
- Máscara DSCP/TOS.

El campo protocolo identifica el tipo de protocolo (por ejemplo, IP, ICMP, etc.).

El origen IP es la dirección IP (según se ve en el CMTS) del originador del flujo IP, mientras que el destino IP es el punto de terminación del flujo IP.

El puerto de origen y el puerto de destino especifican los puertos UDP o TCP del flujo IP.

La prioridad se puede utilizar para distinguir entre múltiples clasificadores que concuerdan con un paquete particular. Se fija normalmente en un valor por defecto ya que se pretende que los clasificadores sean por lo general únicos.

El campo DSCP/TOS identifica el campo DSCP/TOS con el que hay que concordar de modo que los paquetes puedan ser clasificados en el flujo IP. Para disponer de un grado máximo de flexibilidad al definir la estrategia de gestión de una red, se define una máscara acompañante que determina los bits del byte DSCP/TOS que se han de utilizar como filtros al clasificar los paquetes. Así es posible aplicar tanto la estrategia DiffServ como la estrategia TOS (cada una de las cuales define y utiliza bits distintos de ese byte).

Un clasificador PUEDE tener campos cuyo contenido sea indiferente (campos comodín, indicados por valores de cero), pero hay que actuar con cuidado para que no se produzca una concordancia involuntaria entre varios flujos IP y el mismo clasificador, lo que podría tener consecuencias inesperadas.

6.1.6 Perfil de tráfico

Hay tres maneras básicas de expresar cuál es el perfil de tráfico de una puerta:

1) FlowSpec.

2) Nombre de clase de servicio DOCSIS.

3) Parametrización específica de DOCSIS.

El servidor de política o el gestor de aplicación DEBEN definir el perfil de tráfico de una puerta utilizando una de las tres opciones siguientes:

1) FlowSpec;

2) nombres de clase de servicio DOCSIS; o

3) parámetros específicos de DOCSIS.

Todas las capacidades máximas que se utilicen en el perfil de tráfico DEBEN ser del mismo tipo, es decir, FlowSpec, nombres de clase de servicio DOCSIS o parámetros específicos de DOCSIS.

DEBE haber al menos un conjunto de parámetros de perfil de tráfico especificados cuando la puerta se instala por primera vez. El servidor de política y el gestor de aplicación PUEDEN especificar un segundo conjunto para representar la capacidad máxima reservada y un tercer conjunto para representar la capacidad máxima comprometida. Si al CMTS se le indica que cree un flujo dinámico inmediatamente después de recibir un mensaje Gate-Set (vía la presencia de las capacidades máximas reservadas o comprometidas), el CMTS DEBE utilizar los parámetros de perfil de tráfico de las capacidades máximas reservadas y comprometidas para llevar a cabo la mensajería del anexo B/J.112, a fin de crear el flujo, en el sentido especificado por el campo sentido de la GateSpec (siempre que la petición haya sido autorizada y existan recursos suficientes para cumplimentarla). Cuando se le indique que transite al estado comprometido, el CMTS DEBE utilizar el perfil de tráfico para activar el flujo de servicio DOCSIS. Como actuación óptima, el servidor de política PUEDE indicarle al CMTS que lleve a cabo las tres acciones (autorización, reserva y compromiso) en nombre del gestor de aplicación por medio de un único mensaje Control por puerta. De manera alternativa, el PS/AM PUEDE emitir mensajes Gate-Set separados para indicarle al CMTS que proceda a autorizar y reservar y a continuación comprometer por medio de un mensaje Gate-Set subsiguiente.

6.1.6.1 FlowSpec

El objeto FlowSpec contiene FlowSpecs (especificaciones de flujo) de RSVP que se utilizan para describir el perfil de tráfico del flujo IP. El objeto FlowSpec puede contener múltiples FlowSpecs de RSVP:

- Una FlowSpec que define la capacidad máxima de un recurso para una autorización con la cual pueden cotejarse futuras reservas.
- Una FlowSpec que define la capacidad máxima reservada con la cual pueden cotejarse futuras peticiones de compromiso.
- Una FlowSpec que define los recursos que se han de comprometer.

Las FlowSpecs de RSVP soportan dos tipos de servicio: de carga controlada [4] y garantizado [5]. La diferencia principal entre estos dos tipos de servicio se examina en la cláusula 8. Ambos tipos de servicio se distinguen en base al número de servicio FlowSpec, que se especifica en la FlowSpec de RSVP. El número de servicio 5 es para servicio de carga controlada y el número de servicio 2 es para servicio garantizado. Un servicio de carga controlada DEBE contener solamente los

parámetros de colector testigo de la TSpec y no de la RSpec. Un servicio garantizado DEBE contener tanto la TSpec como la RSpec.

Para la información sobre cómo establecer de manera explícita la correspondencia entre los parámetros RSVP y los parámetros DOCSIS, consúltese la cláusula 8. Cuando los parámetros DOCSIS se obtienen utilizando los parámetros de FlowSpec de RSVP, algunos de esos parámetros DOCSIS derivados tienen unos valores muy aproximados. Si las aproximaciones no dan al servidor de política o al gestor de aplicación el control que desean, el PS/AM PUEDE utilizar los otros métodos de definición del perfil de tráfico, que incluyen la posibilidad de definir algunos parámetros específicos de DOCSIS. Estos parámetros permiten al servidor de política o al gestor de aplicación ajustar de manera precisa la correspondencia normalizada entre FlowSpecs y parámetros DOCSIS.

6.1.6.2 Nombre de clase de servicio DOCSIS

El nombre de clase de servicio DOCSIS indica la clase de servicio DOCSIS que se ha de utilizar para describir los atributos de QoS. Un CMTS DEBE soportar nombres de clase de servicio DOCSIS.

El nombre de clase de servicio DOCSIS permite utilizar parámetros de QoS DOCSIS adjudicados previamente en el CMTS. En el CMTS se pueden configurar clases de servicios denominados DOCSIS con perfiles diferentes de QoS DOCSIS y hacer referencia a continuación al nombre de clase de servicio DOCSIS de la puerta para asociar indirectamente un perfil de QoS a una puerta determinada. DOCSIS permite también modificar los parámetros utilizando codificaciones TLV. Un CMTS DEBE devolver la indicación de error "Nombre de clase de servicio no definido" si se pide introducir modificaciones en los parámetros de QoS del nombre de clase de servicio (véase 6.4.2.14).

Para más información sobre las clases de servicio DOCSIS, véase B.10.1.3/J.112 [1].

6.1.6.3 Parametrización específica de DOCSIS

La tercera manera de definir el perfil de tráfico consiste en utilizar un perfil de tráfico específico de DOCSIS; de este modo el gestor de aplicación puede especificar explícitamente los parámetros DOCSIS del flujo DOCSIS. Si el gestor de aplicación desea utilizar este tercer procedimiento de definición de un perfil de tráfico, DEBE incluir un objeto que contenga los parámetros específicos de DOCSIS.

Todos los tipos de calendarización de flujo de servicio DOCSIS son soportados mediante distintos tipos S (S-Types) de perfil de tráfico. Cada S-Type tiene una codificación diferente de los parámetros específicos de DOCSIS inherentes a ese tipo de calendarización de flujo de servicio. Para más detalles sobre la parametrización específica de DOCSIS, véase 6.4.2.7.

6.1.7 Información de generación de evento

Este objeto contiene información que interesa al CMTS para el soporte de las funciones de contabilidad y facturación. Sus atributos son como sigue:

- Dirección primaria: Puerto del servidor de mantenimiento de registros primario al que el CMTS DEBE enviar registros de eventos.
- Dirección secundaria: Puerto del servidor de mantenimiento de registros secundario que el CMTS DEBE utilizar como se especifica en [10] si el primario no está disponible.
- Bandera que indica si el CMTS DEBE enviar mensajes de evento al servidor de mantenimiento de registros en tiempo real o si el CMTS DEBE tomar los mensajes de evento en el modo lotes y enviarlos a intervalos periódicos.
- ID de correlación de facturación, que el CMTS DEBE pasar al servidor de mantenimiento de registros con cada registro de evento.

La omisión del objeto Información de generación de evento indica que el CMTS NO DEBE generar mensajes de evento para una puerta específica.

6.1.8 Límite de utilización basado en tiempo

Este objeto especifica la cantidad de tiempo que una puerta puede permanecer comprometida antes de alcanzar el umbral del límite de tiempo correspondiente a esa puerta. Este objeto es opaco para el CMTS. El CMTS no es responsable de la aplicación de los límites de tiempo, pero DEBE almacenar este objeto y devolverlo cuando se le pida.

6.1.9 Límite de utilización basado en volumen

El gestor de aplicación utiliza el límite de utilización basado en volumen para indicar al CMTS que genere un mensaje Control por puerta cuando el volumen de datos especificado haya atravesado la puerta. El CMTS no es responsable de la aplicación de los límites de volumen, pero DEBE avisar al PS/AM cuando se alcance un límite de volumen.

6.1.10 Datos opacos

El objeto Datos opacos consiste en la información general que un servidor de política o gestor de aplicación puede almacenar en un CMTS. Estos datos permanecen opacos al CMTS, pero contienen información útil para el PS/AM. Si lo proporciona el PS/AM, el CMTS devolverá este objeto en todas las respuestas (véase 6.4.2.11).

6.1.11 Información de tiempo de puerta

El objeto Información de tiempo de puerta contiene una indicación de tiempo que representa la hora en que la puerta fue comprometida. Este objeto puede ser consultado y utilizado por un servidor de política o un gestor de aplicación para aplicar políticas de red basadas en el tiempo.

6.1.12 Información de utilización de puerta

El objeto Información de utilización de puerta consiste en un contador de octetos que indica el número de bytes de datos transmitidos por esa puerta (véase 6.4.2.13). De manera análoga al objeto Información de tiempo de puerta, esta información puede ser utilizada por un servidor de política o un gestor de aplicación para aplicar políticas de red basadas en el volumen.

6.2 Transiciones de puerta

Como se ha indicado anteriormente de forma resumida, una puerta puede hallarse en los estados lógicos siguientes:

- Autorizado: Un servidor de política ha autorizado el flujo con límites de recursos definidos.
- Reservado: Se han reservado recursos para el flujo.
- Comprometido: Hay recursos activos y están siendo utilizados.
- Recuperación comprometida: se ha detectado inactividad en el flujo; pendiente de la recuperación del recurso.

En el caso de la máquina descrita en la figura 3, el CMTS DEBE completar el evento desencadenante con resultado satisfactorio antes de hacer que una puerta transite de un estado a otro. En el caso de eventos de control por puerta, el CMTS NO DEBE cambiar un estado hasta que la petición haya sido procesada por completo (incluyendo cualesquiera transiciones de flujo resultantes) y el CMTS haya determinado que se ha de transmitir un reconocimiento de éxito.

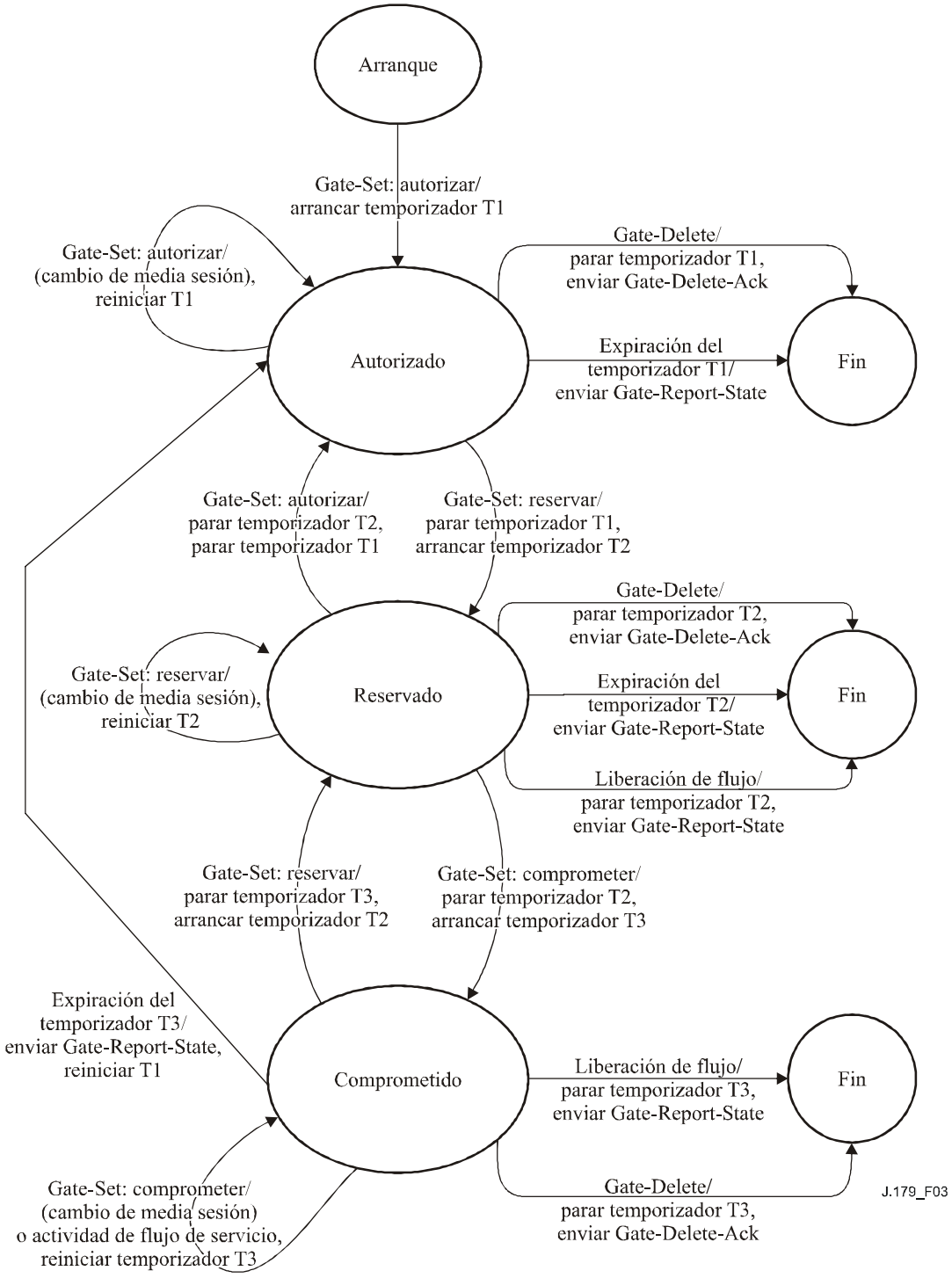


Figura 3/J.179 – Transiciones de estado de puerta

El CMTS DEBE soportar estados y transiciones de puerta como se muestra en la figura 3 y se describe en esta cláusula. El CMTS DEBE implementar además transiciones para el procesamiento de errores de protocolo.

En la presente cláusula se describen las transiciones de estado de puerta en el CMTS resultantes de eventos externos (mensajes Control por puerta procedentes del servidor de política), así como las transiciones resultantes de eventos internos (por ejemplo, la expiración de un temporizador). Se señala que el servidor de política no es el origen de los eventos externos; el servidor de política no hace sino actuar simplemente como un apoderado del gestor de aplicación, que es el desencadenante de los eventos.

6.2.1 Autorizado

Una instrucción Gate-Set procedente del servidor de política crea en el CMTS una puerta. El CMTS le adjudica un identificador único llamado ID de puerta. La puerta, se dice ahora, está en el estado autorizado y el CMTS DEBE arrancar el temporizador T1. El temporizador T1 limita la cantidad de tiempo durante el cual la autorización se mantiene válida.

Tras la recepción de un mensaje Gate-Delete, una puerta que se encuentre en el estado autorizado DEBE ser suprimida. Cuando esto ocurre el CMTS DEBE responder con un mensaje Gate-Delete-Ack y DEBE parar el temporizador T1.

Es preciso que el CMTS soporte las transiciones de estado siguientes mientras una puerta esté en el estado autorizado:

Transiciones de estado autorizado:

- Conexión en bucle autorizado a autorizado: Modificar la capacidad máxima autorizada.
- Conexión en bucle autorizado a reservado (define capacidad máxima reservada ≤ capacidad máxima autorizada).
- Autorizado a fin (suprime la capacidad máxima autorizada).

El CMTS NO DEBE soportar ninguna otra transición de estado de una puerta que se encuentre en el estado autorizado, pero un cierto número de estímulos independientes pueden dar lugar a las transiciones descritas.

Cuando se instala la puerta se dice que está en un estado autorizado. Mientras está en el estado autorizado, el servidor de política PUEDE modificar cualquiera de los parámetros asociados a una puerta (por ejemplo, perfil de tráfico, clasificador, etc.). Si estando en un estado autorizado se recibe un mensaje Gate-Set que no provoca el tránsito de la puerta a los estados reservado o comprometido, el CMTS DEBE rearrancar el temporizador T1.

Mientras está en el estado autorizado, el CMTS DEBE provocar el tránsito de la puerta al estado reservado cuando se produzca una petición exitosa del servidor de política. El CMTS DEBE hacer que la puerta transite al estado fin tras la recepción de un mensaje Gate-Delete procedente del servidor de política o tras la expiración del temporizador T1.

6.2.2 Reservado

Cuando una puerta se encuentra en el estado autorizado, está esperando que el cliente trate de reservar recursos. En el escenario 1, el servidor de política reserva los recursos en nombre del cliente. Para reservar recursos, el servidor de política DEBE emitir un mensaje Gate-Set subsiguiente con un perfil de tráfico que incluya la capacidad máxima reservada. Al recibir esta petición de reserva, el CMTS DEBE comprobar que la petición se halla dentro de los límites de la autorización establecidos para la puerta y DEBE llevar a cabo los procedimientos de control de admisión.

Si la petición de reserva no llega antes de que expire el temporizador T1, el CMTS DEBE suprimir la puerta y notificar al servidor de política el cambio de estado. Si el control de admisión se produce de manera satisfactoria y sólo se hubiera pedido reserva de recurso, el CMTS DEBE poner la puerta en el estado reservado. De manera simultánea, el CMTS DEBE parar el temporizador T1 y arrancar el temporizador T2 (temporizador reservado). Si los procedimientos de control de admisión no son exitosos, el CMTS DEBE mantener la puerta en el estado autorizado y dar una respuesta Gate-Set-Err al PS.

Se REQUIERE que el CMTS soporte las transiciones de estado siguientes mientras una puerta esté en el estado reservado:

Transiciones de estado reservado:

- Conexión en bucle reservado a reservado: Modificar la capacidad máxima autorizada (≥ capacidad máxima reservada).
- Conexión en bucle reservado a reservado: Modificar la capacidad máxima reservada (≤ la capacidad máxima autorizada).
- Reservado a comprometido (define la capacidad máxima comprometida ≤ la capacidad máxima reservada).
- Reservado a fin (suprime las capacidades máximas reservada y autorizada).

El CMTS NO DEBE soportar ninguna otra transición de estado de una puerta que se encuentre en el estado reservado, pero un cierto número de estímulos independientes pueden dar lugar a las transiciones descritas.

Desde el estado autorizado, el CMTS DEBE hacer que la puerta transite al estado reservado, si lo pide el servidor de política y la capacidad máxima reservada es menor o igual que la autorizada, la petición pasa el control de admisión y el flujo es reservado de manera satisfactoria. Una vez en el estado reservado, la capacidad máxima autorizada de la puerta PUEDE modificarse mediante un mensaje Gate-Set. La capacidad máxima reservada de la puerta también puede modificarse en el estado reservado (véase 6.5.6). Si estando en el estado reservado se recibe un mensaje Gate-Set que no provoca el tránsito de la puerta a los estados autorizado o comprometido, el CMTS DEBE rearrancar el temporizador T2.

Si la petición de compromiso no llega antes de que expire el temporizador T2, el CMTS DEBE suprimir la puerta y notificar el cambio de estado al servidor de política.

La capacidad máxima reservada DEBE ser siempre menor o igual que la capacidad máxima autorizada. En el estado reservado, para que un CMTS provoque el tránsito de una puerta al estado comprometido la capacidad máxima comprometida DEBE ser menor o igual que la reservada (véase 6.5.3).

Mientras está en el estado reservado, el servidor de política debe modificar la capacidad máxima autorizada especificando un nuevo perfil de tráfico en un mensaje Gate-Set. El nuevo perfil de tráfico definirá una capacidad máxima autorizada modificada y la misma capacidad máxima reservada que se utilizó previamente para que la puerta transitara al estado reservado. Sin embargo, todas las peticiones de modificación de las capacidades máximas autorizada, reservada o comprometida DEBEN atenerse a la regla general siguiente:

Capacidad máxima autorizada ≥ Capacidad máxima reservada ≥ Capacidad máxima comprometida

El servidor de política PUEDE suprimir una puerta que se halle en el estado reservado emitiendo un mensaje Gate-Delete.

6.2.3 Comprometido

Cuando una puerta se encuentra en el estado reservado, está esperando que el cliente comprometa recursos y, por consiguiente, los active. En el escenario 1, el servidor de política compromete los recursos en nombre del cliente. Para comprometer recursos, el servidor de política DEBE emitir una instrucción Gate-Set con un perfil de tráfico que incluya la capacidad máxima comprometida. El CMTS DEBE autorizar de nuevo la QoS cotejando la petición con la capacidad máxima reservada. Si la autorización se produce de manera satisfactoria, el CMTS DEBE arrancar el temporizador T3 y parar el temporizador T2, si la capacidad máxima autorizada es igual a la comprometida, o rearrancar el temporizador T2 si la capacidad máxima autorizada es mayor que la comprometida. Si la autorización falla, el CMTS DEBE reiniciar el temporizador T2.

Se señala que, una vez que el flujo de servicio DOCSIS haya sido activado, el CMTS DEBE reiniciar el temporizador T3 cuando se transfieran datos por el flujo. Si no hay actividad en el flujo durante un tiempo igual al del temporizador T3, el CMTS DEBE notificar al servidor de política el

cambio de estado. De manera similar, el servidor de política DEBE notificar al gestor de aplicación el cambio de estado.

En el estado comprometido, el gestor de aplicación PUEDE suprimir la puerta enviando un mensaje Gate-Delete al servidor de política, que a su vez DEBE reenviar el mensaje por el CMTS. Si el servidor de política envía un mensaje Gate-Delete al CMTS, el CMTS DEBE suprimir la puerta y el flujo de servicio correspondiente y parar el temporizador T2 y el T3, si están en marcha.

Se REQUIERE que el CMTS soporte las transiciones de estado siguientes mientras una puerta esté en el estado comprometido:

Transiciones del estado comprometido:

- Conexión en bucle comprometido a comprometido: Modificar la capacidad máxima autorizada (≥ capacidad máxima reservada).
- Conexión en bucle comprometido a comprometido: Modificar la capacidad máxima reservada (≥ capacidad máxima comprometida y ≤ capacidad máxima autorizada).
- Conexión en bucle comprometido a comprometido: Modificar la capacidad máxima comprometida (≤ capacidad máxima reservada).
- Comprometido a reservado (elimina la capacidad máxima comprometida).
- Comprometido a recuperación comprometida (inicia el proceso de recuperación de recursos).
- Comprometido a fin (elimina las capacidades máximas comprometida, reservada y autorizada).

El CMTS NO DEBE soportar ninguna otra transición de estado de una puerta que se encuentre en el estado comprometido, pero un cierto número de estímulos independientes pueden dar lugar a las transiciones descritas.

Mientras está en el estado reservado, el CMTS DEBE provocar el tránsito de la puerta al estado comprometido, si lo pide el servidor de política y la capacidad máxima comprometida es menor o igual que la reservada (véase 6.5.3). Mientras está en el estado comprometido, el servidor de política PUEDE modificar la capacidad máxima autorizada de la puerta mediante un mensaje Gate-Set, siempre que la capacidad máxima autorizada sea mayor o igual que la reservada. En este estado, el servidor de política PUEDE modificar también la capacidad máxima reservada, si ésta es mayor o igual que la comprometida. En este estado, el servidor de política PUEDE incluso modificar la capacidad máxima comprometida, siempre que la nueva capacidad máxima sea menor o igual que la capacidad máxima reservada. Si se recibe una petición de descomprometer todos los recursos comprometidos (pero mantenerlos reservados) mientras la puerta está en el estado comprometido, el CMTS DEBE parar el temporizador T3, (re)arrancar el temporizador T2 y hacer que retorne al estado reservado. En el escenario 1, el servidor de política PUEDE pedir esta acción emitiendo un mensaje Gate-Set con un perfil de tráfico que incluya las capacidades máximas autorizada y reservada, pero que no incluya una capacidad máxima comprometida.

Mientras está en el estado comprometido, el CMTS DEBE hacer que una puerta transite al estado fin tras recibir un mensaje Gate-Delete procedente del servidor de política. Mientras está en el estado comprometido, el servidor de política PUEDE modificar la capacidad máxima autorizada o la reservada especificando simplemente el nuevo perfil de tráfico; el perfil de tráfico nuevo DEBE contener capacidades máximas autorizadas o reservadas modificadas y la misma capacidad máxima comprometida que se utilizó previamente para el tránsito de la puerta al estado comprometido.

Al pasar (nuevamente) al estado comprometido tras recibir un mensaje Gate-Set, el CMTS DEBE (re)arrancar el temporizador T2, si la capacidad máxima reservada es mayor que la comprometida, o DEBE parar el temporizador T2 si estaba previamente en marcha y la capacidad máxima reservada es ahora igual a la comprometida.

Mientras está en el estado comprometido:

1) si el temporizador T2 expira, la puerta DEBE permanecer en el estado comprometido y el CMTS DEBE enviar al servidor de política un mensaje Gate-Report-State con el código de motivo 9 (estado de puerta inalterado, pero la expiración del temporizador T2 causó una reducción de la reserva) indicando la reducción de los recursos reservados;
2) si el mensaje Gate-Set hace volver la puerta al estado reservado, DEBE arrancarse el temporizador T2 si no estaba en marcha o rearrancarse si había estado funcionando; y
3) si se produce una transición al estado fin, DEBEN pararse los temporizadores T2 y T3 si están en marcha.

Como actuación óptima, para el escenario 1, el servidor de política PUEDE autorizar, reservar y comprometer al mismo tiempo emitiendo un mensaje Gate-Set con el perfil de tráfico que incluye las tres capacidades máxima fijadas de tal modo que al CMTS se le indique que ejecute las tres acciones de manera secuencial sin ninguna interacción con el servidor de política, es decir, que las tres deben ser exitosas (si tal es el caso, el CMTS DEBE indicarlo mediante un mensaje Gate-Set-Ack) o las tres deben fallar (si tal es el caso, el CMTS DEBE indicarlo mediante un mensaje Gate-Set-Err).

Desde el estado comprometido, la puerta pasa al estado recuperación comprometida debido a la expiración del temporizador T3. Si el CMTS detecta que no ha habido actividad en el flujo asociado mientras dura la temporización de T3, DEBE arrancar el temporizador T4, generar un mensaje Gate-Report-State dirigido al servidor de política indicando que el flujo ha estado inactivo durante el tiempo definido por T3 y pasar al estado recuperación comprometida, dejando el flujo asociado en el estado activado. El servidor de política DEBE reenviar el mensaje Gate-Report-State al gestor de aplicación. El gestor de aplicación DEBE renovar la política emitiendo un nuevo mensaje Gate-Set o bien suprimir la puerta emitiendo un mensaje Gate-Delete.

Ciertas aplicaciones pueden no desear ser notificadas cuando cesa la actividad del flujo. En tal caso, el gestor de aplicación puede poner a 0 el temporizador T3 (que corresponde al temporizador activo DOCSIS). Como se especifica en [1], un valor 0 del temporizador activo DOCSIS indica que se desactiva la detección de actividad en el CMTS para ese flujo. Por consiguiente, la puerta permanecerá en el estado comprometido hasta que se reciba un mensaje Gate-Delete o el CM deje de estar en línea.

6.2.4 Recuperación comprometida

En el estado comprometido el flujo asociado a la puerta está activo. Si el CMTS detecta que el flujo no se utiliza durante un tiempo superior al del temporizador T3, el CMTS notifica al servidor de política (que lo notifica al AM) que el flujo de servicio asociado a la puerta no ha sido utilizado, arranca el temporizador T4 y hace que la puerta pase al estado recuperación comprometida.

NOTA – Si el T2 está en marcha, seguirá estándolo. No DEBE reiniciarse.

El AM debe decidir si renovar la política emitiendo un mensaje Gate-Set al servidor de política o si suprimir la puerta emitiéndole un mensaje Gate-Delete. El servidor de política DEBE reenviar el mensaje Gate-Set o el mensaje Gate-Delete al CMTS.

Si, mientras está en el estado recuperación comprometida, el CMTS recibe un mensaje Gate-Set para esa puerta antes de que expire el temporizador T4, el CMTS DEBE parar el T4, rearrancar el T3, hacer que la puerta vuelva al estado comprometido y (re)arrancar el temporizador T2, si la capacidad máxima reservada es mayor que la comprometida, o pararlo si la nueva capacidad máxima reservada es igual a la comprometida.

Si, mientras está en el estado recuperación comprometida, el CMTS recibe un mensaje Gate-Delete antes de que expire el temporizador T4, el CMTS DEBE parar el T4, suprimir la puerta y el correspondiente flujo de servicio y parar el temporizador T2 si está en marcha.

Si el temporizador T4 expira mientras está en el estado recuperación comprometida, el CMTS DEBE enviar un mensaje Gate-Report-State al servidor de política, parar el temporizador T2, si está en marcha eliminar el flujo de servicio asociado a la puerta, y luego suprimir la puerta. Asimismo, el servidor de política DEBE notificar al gestor de aplicación el cambio de estado.

Si el temporizador T2 expira mientras está en el estado recuperación comprometida, la puerta DEBE permanecer en el estado recuperación comprometida y el CMTS DEBE enviar al servidor de política un mensaje Gate-Report-State con el código de motivo 9 (estado de puerta inalterado, pero la expiración del temporizador T2 causó una reducción de la reserva) indicando la reducción de los recursos reservados.

El CMTS DEBE soportar las transiciones de estado siguientes mientras una puerta está en el estado recuperación comprometida:

Transiciones del estado recuperación comprometida:

- recuperación comprometida a comprometido: (la política ha sido renovada).
- recuperación comprometida a fin: (suprime las capacidades máximas comprometida, reservada y autorizada).
- recuperación comprometida a recuperación comprometida: (expira el temporizador T2; envía un mensaje Gate-Report-State).

El CMTS NO DEBE soportar ninguna otra transición de estado para una puerta en el estado recuperación comprometida, pero algunos estímulos separados pueden causar las transiciones descritas.

Puede haber aplicaciones que no deseen mantener una puerta una vez que se ha detectado inactividad. En este caso, el gestor de aplicación puede poner a 0 el temporizador T4. Cuando T4 es puesto a cero, no se gasta prácticamente tiempo en el estado recuperación comprometida y la puerta (y el flujo) DEBE suprimirse cuando expira el temporizador T3.

6.3 Perfil de COPS para multimedia IPCablecom

Como se ha definido más arriba, el control de admisión conlleva el proceso de gestión de las peticiones de recurso QoS en base a las políticas administrativas y los recursos disponibles. En el apéndice I se describen los módulos operativos de alto nivel asociados a este proceso. Según este modelo, las políticas administrativas se almacenan en una base de datos de políticas y son controladas por el servidor de política.

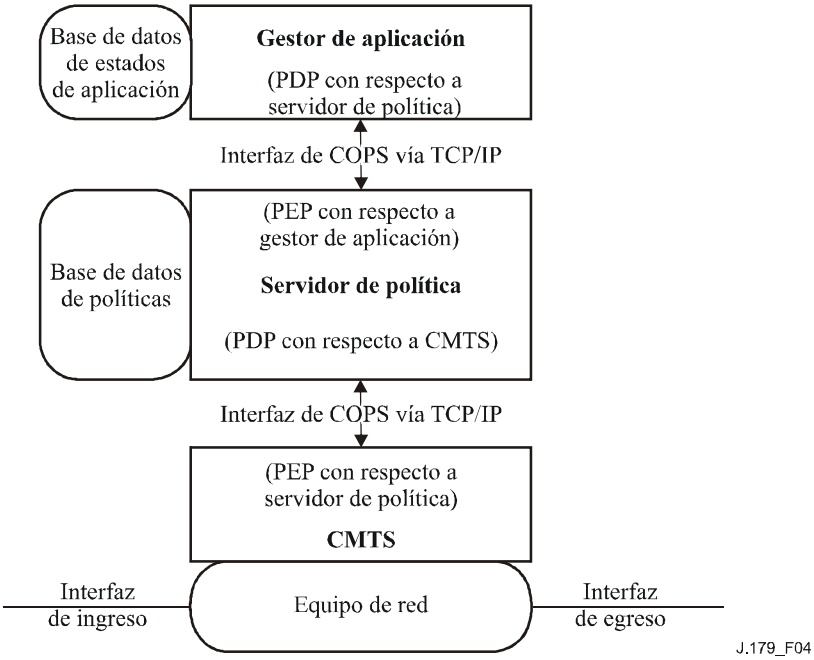


Figura 4/J.179 – Disposición de control de admisión de QoS

Las decisiones sobre control de admisión tomadas por el servidor de política DEBEN ser comunicadas al CMTS o al gestor de aplicación utilizando el COPS. El CMTS PUEDE hacer peticiones de control de admisión de QoS al servidor de COPS en base a eventos de red desencadenados por el protocolo de señalización de QoS o mediante mecanismos de detección de flujos de datos. El evento de red puede necesitar también gestión de anchura de banda de QoS, por ejemplo, porque una nueva interfaz con capacidad de QoS pase a estar operativa.

Las decisiones de tipo político de QoS tomadas por el servidor de política PUEDEN ser empujadas hacia el CMTS en base a una petición procedente del gestor de aplicación. El CMTS PUEDE acceder a la información relativa a esas decisiones para tomar decisiones sobre la puesta en vigor de políticas sobre peticiones de sesión entrantes recibidas en el CMTS. El CMTS NO DEBE soportar mensajes DSx iniciados por un CM en multimedia IPCablecom. El CMTS DEBE tratar un mensaje iniciado por un CM como una petición con ID de puerta no válido.

En el protocolo de COPS de IETF [7] se especifica una configuración cliente/servidor de COPS que soporta el control de admisión de QoS. Dicho protocolo incluye las operaciones siguientes:

- Client-Open (OPN)/Client-Accept (CAT)/Client-Close (CC): El cliente de COPS (PEP) envía un mensaje OPN para iniciar una conexión con el servidor de COPS (PDP) y el servidor responde con un mensaje CAT para aceptar la conexión. El servidor o el cliente envían un mensaje CC para terminar la conexión.
- Petición (REQ, *request*). El cliente envía un mensaje REQ al servidor para pedir información sobre una decisión de control de admisión o información sobre la configuración del dispositivo. El mensaje REQ puede contener información específica del cliente que el servidor utiliza junto con datos de la base de datos de políticas de admisión a la sesión, para tomar decisiones basadas en políticas.
- Decisión (DEC, *decision*). El servidor responde a los mensajes REQ devolviendo un mensaje DEC al cliente que inició la petición original. Los mensajes DEC pueden ser enviados inmediatamente en repuesta a un REQ (es decir, un DEC solicitado) o en cualquier momento tras el cambio o la actualización de una decisión previa (es decir, un DEC no solicitado).

- Report-State (RPT). El cliente envía un mensaje RPT al servidor indicando cambios del estado de la petición en el cliente. El cliente envía este mensaje para informar al servidor a propósito del recurso efectivamente reservado después de que el servidor haya concedido la admisión. El cliente puede utilizar también Report-State para informar periódicamente al servidor sobre el estado en que se encuentra el cliente.
- Delete-Request-State (DRQ). El cliente envía un mensaje DEL al servidor para pedir que se borre el estado. Puede ser el resultado de la liberación de un recurso QoS por el cliente.
- Keep-Alive (KA). Enviado tanto por el cliente como por el servidor para detectar fallos de comunicación.
- Synchronize-State-Request (SSQ)/Synchronize-State-Complete (SSC). El servidor envía el mensaje SSQ al cliente pidiendo información sobre el estado actual. El cliente reenvía consultas sobre la petición al servidor para llevar a cabo la sincronización y a continuación envía un mensaje SSC para indicar la compleción del evento de sincronización. Un servidor de política PUEDE soportar funciones de sincronización SSQ/SSC si necesita adquirir o rehacer un estado a partir del CMTS. El CMTS DEBE soportar las funciones de sincronización SSQ/SSC.

Dentro de la arquitectura de multimedia IPCablecom, las relaciones PDP-PEP son como sigue:

- El gestor de aplicación es un punto de decisión de la política (PDP) de COPS con respecto al servidor de política.
- El servidor de política de política es un PEP con respecto al gestor de aplicación.
- El servidor de política es un PDP con respecto al CMTS.
- El CMTS es un PEP con respecto al servidor de política.

Aunque el contenido de los mensajes COPS requeridos para los multimedia IPCablecom son coherentes con el protocolo de COPS, hay una ligera diferencia en la manera en que comienza la sesión de COPS y una relajación de los requisitos de ordenación de respuesta. La norma RFC 2748 [7] establece lo siguiente:

"El protocolo de COPS utiliza una única conexión TCP persistente entre el PEP y un PDP distante. Una implementación PDP por servidor DEBE ponerse a la escucha en un puerto TCP de número conocido (COPS = 3288 [IANA]). El PEP es responsable de la iniciación de la conexión del TCP con un PDP."

La última línea de la declaración indica que el PEP se encarga de iniciar la conexión del TCP. Por el contrario, en el modelo IPCablecom, el CMTS (PEP) es el que está a la escucha en el puerto de número 3918 asignado y es el servidor de política el que DEBE iniciar la conexión del TCP con el CMTS. Esto es lo opuesto al modelo descrito en la norma RFC. Sin embargo, una vez establecida la conexión del TCP, el CMTS se comporta de manera coherente con el cliente, o PEP, en el protocolo de COPS. De manera similar, el servidor de política (PEP) está a la escucha en el puerto de número 3918 asignado y es el gestor de aplicación el que DEBE iniciar la conexión del TCP con el servidor de política.

Se señala que los multimedia IPCablecom y DQoS de IPCablecom-T están a la escucha en puertos diferentes, por lo que el CMTS puede iniciar la sesión de COPS con el Client-Type (tipo de cliente) apropiado.

La RFC 2748 establece también:

"Los mensajes RPT solicitados por decisiones para una determinada asa de cliente (Client-Handle) DEBEN fijar la bandera de mensaje solicitado y DEBEN enviarse en el mismo orden en que se recibieron los correspondientes mensajes Decisión."

El protocolo COPS utiliza el orden de los mensajes RPT y de decisión para hacer concordar las peticiones con las respuestas. En cambio, las implementaciones multimedia PacketCable DEBEN utilizar el objeto TransactionID para hacer concordar las respuestas con las peticiones y DEBERÍAN enviar mensajes RPT tan pronto como estén listas.

Los detalles del protocolo de COPS se dan en la RFC 2748. Esta norma RFC del IETF proporciona una descripción del protocolo de COPS base, con independencia del Client-Type. La arquitectura IPCablecom se atiene también IETF RFC 3084 [19]. El COPS-PR establece lo siguiente:

"En el COPS-PR, las peticiones de política describen el PEP y sus parámetros configurables (más bien que un evento operativo). Si se produce un cambio en estos parámetros básicos, se envía una petición actualizada. Por ello, muy rara vez se emiten peticiones. La correspondencia entre decisiones y peticiones no necesariamente se establece de manera directa y la mayoría de las veces las peticiones se formulan cuando el PDP responde a eventos externos o eventos PDP (actualizaciones de políticas)."

Cuando se hace corresponder este concepto con la arquitectura de multimedia IPCablecom, el PEP plantea una petición al PDP, especificando un Client-Handle (asa de cliente). El Client-Handle se utiliza luego en todos los futuros mensajes Decisión del PDP al PEP. Los mensajes Decisión llevan mensajes Control por puerta (es decir, Gate-Set, Gate-Info y Gate-Delete) definidos para los Client-Types de DQoS y multimedia. El Client-Handle se emplea para identificar de manera exclusiva la asociación PDP-PEP.

En la arquitectura de multimedia IPCablecom puede haber múltiples gestores de aplicación interactuando con uno o más servidores de política. Hay un solo ejemplar de una sesión de COPS de multimedia IPCablecom por conexión TCP; donde una sesión de COPS de multimedia IPCablecom se refiere a los mensajes de puerta entre el PDP y el PEP asociado a un solo Client-Handle. Esto significa que existe una conexión COPS-TCP entre un gestor de aplicación y un servidor de política. De manera similar, puede haber uno o más servidores de política hablando con uno o más CMTS. Cuando esté conectado a múltiples PDP, el PEP DEBE garantizar que se utiliza un Client-Handle exclusivo por cada asociación.

6.4 Formatos de mensaje de protocolo de control por puerta

Los mensajes de protocolo para el control por puerta DEBEN ser transportados dentro de los mensajes de protocolo de COPS. El PDP y el PEP DEBEN establecer y utilizar una conexión TCP para comunicación y utilizar los mecanismos especificados en [11] para asegurar el trayecto de la comunicación.

6.4.1 Formato de mensaje común COPS

Cada mensaje COPS consta del encabezamiento COPS seguido de un cierto número de objetos tipificados. El gestor de aplicación, el servidor de política y el CMTS DEBEN utilizar el formato de mensaje común COPS que se define a continuación como formato de mensaje en todos los intercambios de mensajes. En las especificaciones de objetos que siguen, cada fila representa una palabra de 4 bytes ya que todos los objetos se alinean entre límites de palabras de 4 bytes.

0		1	2	3
Versión	Banderas	Op-Code	Client-Type	
Longitud del mensaje				

El campo versión es un campo de 4 bits que da el número de la versión de COPS actual. Este campo DEBE fijarse en 1.

El campo banderas es un campo de 4 bits. El bit menos significativo es la bandera de mensaje solicitado. Cuando se envía un mensaje COPS en respuesta a otro mensaje (por ejemplo, una decisión solicitada enviada en respuesta a un petición) esta bandera DEBE fijarse en 1. En otros

casos (por ejemplo, una decisión no solicitada) la bandera NO DEBE fijarse (valor = 0). De conformidad con el modelo DQoS, el primer mensaje Decisión enviado en respuesta a un mensaje Petición es una respuesta solicitada y DEBE fijarse su bandera de mensaje solicitado. Los demás mensajes Decisión son mensajes no solicitados y la bandera de mensaje solicitado DEBE ser liberada. Todas las demás banderas DEBEN fijarse en 0.

El campo Op-code es un campo de enteros sin signo de 1 byte que indica la operación de COPS que se ha de efectuar. Las operaciones de COPS utilizadas en esta Recomendación sobre IPCablecom son:

1 = Petición (REQ)

2 = Decisión (DEC)

3 = Report-State (Informar de estado) (RPT)

4 = Delete Request State (Suprimir petición de estado) (DRQ)

5 = Synchronize State Request (Petición de sincronización de estados) (SSQ)

6 = Client-Open (Cliente abrir) (OPN)

7 = Client-Accept (Cliente aceptar) (CAT)

8 = Cliente-Close (Cliente cerrar) (CC)

9 = Keep-Alive (Mantener vivo) (KA)

10 = Synchronize State Complete (Compleción de sincronización de estados) (SSC)

El campo Client-Type es un identificador de enteros sin signo de 2 bytes. Si se usa multimedia IPCablecom, el Client-Type DEBE fijarse en cliente de multimedia IPCablecom (0x800A). Para mensajes Keep-Alive (Op-code = 9) el Client-Type DEBE fijarse en 0, ya que el KA se utiliza para verificar la conexión en vez de para efectuar verificaciones de sesión cliente por cliente.

El campo Longitud del mensaje es un valor de enteros sin signo de 4 bytes que da el tamaño del mensaje global en octetos. Los mensajes DEBEN estar alineados en demarcaciones de 4 bytes, por lo que la longitud DEBE ser un múltiplo de 4.

Tras el encabezamiento común COPS hay uno o más objetos. Todos los objetos DEBEN atenerse al mismo formato de objeto según el cual cada objeto consta de una o más palabras de 4 bytes con un encabezamiento de 4 octetos y cuyo formato es el siguiente:

0	1	2	3
Longitud		C-Num	C-Type
Contenido del objeto			

El campo longitud es un valor de enteros sin signo de 2 bytes que DEBE dar el número de bytes (incluyendo el encabezamiento) que componen el objeto. Si la longitud original en octetos no es un múltiplo de 4, se DEBE añadir relleno al final del objeto de manera que quede alineado en la demarcación siguiente de 4 bytes.

C-Num identifica la clase de información contenida en el objeto y C-Type identifica el subtipo o versión de la información contenida en el objeto. Los objetos COPS normalizados (definidos en [7]) que se utilizan en esta Recomendación y sus valores C-Num son:

1 = Handle (Asa)

2 = Contexto

6 = Decisión

8 = Error

9 = Client Specific Info (Información específica del cliente)

10 = Keep-Alive-Timer (Temporizador mantener vivo)

11 = PEP Identification (Identificador de PEP)

12 = Report Type (Tipo de informe)

Cada uno de estos objetos DEBE atenerse al formato y las reglas correspondientes al objeto de que se trate, según se define en RFC 2748.

6.4.2 Objetos COPS adicionales para el control por puerta

Al igual que ocurre con los perfiles de COPS-PR y COPS-RSVP, el Client-Type de IPCablecom define un cierto número de formatos de objetos adicionales. Dichos objetos DEBEN colocarse dentro de un objeto Decisión, C-Num = 6, C-Type = 4 (datos de decisión específicos del cliente) cuando se llevan del PDP al PEP en un mensaje Decisión. También DEBEN colocarse en un objeto ClientSI, C-Num = 9, C-Type = 1 (ClientSI señalado) cuando se llevan del PEP al PDP en un mensaje Informar de estado o cliente abrir.

Estos objetos se codifican de forma similar a los objetos específicos del cliente de COPS-PR y, al igual que en el COPS-PR, se enumeran utilizando un espacio de número específico del cliente, que es independiente del espacio de número del objeto COPS de nivel máximo. Por este motivo, los números y tipos de objetos se dan como S-Num y S-Type, respectivamente. S-Num y S-Type DEBEN ser de un octeto. El campo longitud de COPS DEBE ser de dos octetos. En las subcláusulas que siguen se definen objetos COPS adicionales para su utilización por los multimedia IPCablecom.

6.4.2.1 ID de transacción

El ID de transacción (identificador de transacción) es una magnitud entera sin signo de 2 bytes que contiene un testigo que es utilizado por el gestor de aplicación para cotejar respuestas del servidor de política y por el servidor de política para cotejar respuestas del CMTS con las peticiones previas. El ID de transacción DEBE contener además el tipo de instrucción que identifica la acción que se ha de efectuar o bien la respuesta. El objeto ID de transacción debe atenerse al formato siguiente.

Longitud = 8	S-Num = 1	S-Type = 1
Identificador de transacción	Tipo de instrucción de puerta	

El identificador de transacción DEBE fijarse en 0 cuando se incluye en un mensaje Gate-Report-State.

El tipo de instrucción de puerta es un valor entero sin signo de 2 bytes que identifica el tipo de mensaje Control por puerta y DEBE ser uno de los siguientes:

<Reserved>	1-3
Gate-Set	4
Gate-Set-Ack	5
Gate-Set-Err	6
Gate-Info	7
Gate-Info-Ack	8
Gate-Info-Err	9
Gate-Delete	10
Gate-Delete-Ack	11
Gate-Delete-Err	12
<Reserved>	13
<Reserved>	14
Gate-Report-State	15

6.4.2.2 AMID

El AMID, ID de gestor de aplicación, es un valor entero sin signo de 4 bytes que identifica al gestor de aplicación responsable del tratamiento de la sesión. El gestor de aplicación DEBE incluir este objeto en todos los mensajes que envía al servidor de política. El servidor de política DEBE incluir el AMID recibido en todos los mensajes que envía a continuación al CMTS en respuesta a los mensajes que recibe del gestor de aplicación. El CMTS DEBE incluir el objeto AMID recibido en todos los mensajes que envía al servidor de política y, análogamente, el servidor de política DEBE incluir el AMID recibido al gestor de aplicación. El servidor de política puede utilizar el AMID de los mensajes del CMTS a fin de determinar cuál es el gestor de aplicación para el que quizá tenga que generar un mensaje. El objeto AMID DEBE atenerse al formato siguiente.

Longitud = 8	S-Num = 2	S-Type = 1
AMID		

6.4.2.3 ID de abonado

El ID de abonado (identificador de abonado) es un valor de 4 bytes que da la dirección IPv4 (representada como cuatro valores de octetos concatenados) del abonado para esta petición de servicio. Esta dirección puede ser la dirección IP real del dispositivo CPE del abonado que pide el servicio (si es encaminable y visible desde el extremo de cabecera) o puede ser la dirección IP del CM que da servicio a este abonado (si se lleva a cabo la NAT detrás del CM). Este objeto se utiliza para encaminar mensajes Control por puerta en una red compleja de elementos PS y CMTS. También se puede utilizar en la definición y aplicación de reglas de política abonado por abonado. El objeto ID de abonado DEBE atenerse al formato siguiente.

Longitud = 8	S-Num = 3	S-Type = 1
ID de abonado (dirección IPv4 de 4 octetos)		

6.4.2.4 ID de puerta

El ID de puerta (identificador de puerta) es un valor entero sin signo de 4 bytes que identifica la puerta referenciada en el mensaje de instrucción o referenciada por el CMTS para un mensaje de respuesta. El CMTS DEBE asegurar que el ID de puerta es único. Si el CMTS soporta además IPCablecom-T, el ID de puerta NO DEBE duplicar un ID de puerta de IPCablecom-T utilizado en ese momento. El objeto ID de puerta DEBE atenerse al formato siguiente.

Longitud = 8	S-Num = 4	S-Type = 1
ID de puerta		

6.4.2.5 GateSpec

El objeto GateSpec (especificación de puerta) define un conjunto específico de atributos asociados a una puerta. El objeto GateSpec DEBE atenerse al formato siguiente.

Longitud = 16		S-Num = 5	S-Type = 1
Banderas	Campo DSCP/TOS	Máscara DSCP/TOS	ID de clase de sesión
Temporizador T1		Temporizador T2	
Temporizador T3		Temporizador T4	

Banderas es un valor de campo de bits de 1 byte definido como sigue:

- Bit 0: bit de sentido, que DEBE ser cero para una puerta en sentido descendente o uno para una puerta en sentido ascendente.

- Bit 1: bit "habilitar" DSCP/TOS, que DEBE ser cero para inhabilitar la sobreescritura del DSCP o uno para habilitarla.
- Bits 2 a 7: reservados, DEBEN ser cero.

El ID de clase de sesión es un valor entero sin signo de 1 byte que identifica la política de control de admisión o los parámetros apropiados que se han de aplicar para la puerta de que se trate. El SessionClassID es un campo de bits, definido como sigue:

- Bit 0-2: prioridad, número de 0 a 7, donde 0 representa la menor prioridad y 7 la mayor.
- Bit 3: apropiación con prioridad, fijado para permitir apoderarse de la anchura de banda atribuida a sesiones de menor prioridad, en caso necesario (si se soporta).
- Bits 4 a 7: configurable, su valor por defecto es 0.

El campo prioridad describe la importancia de la sesión en comparación con otras sesiones generadas por el mismo PDP. El PEP PUEDE utilizar este valor para implementar la admisión basada en prioridad (en unión del bit de apropiación con prioridad) y para defender el flujo resultante contra la apropiación (véase RFC 2751 [22], "defensa de la prioridad"). La granularidad de prioridades de un CMTS puede ser menor que los 8 valores disponibles. En este caso, el CMTS DEBERÍA distribuir sus niveles entre toda la gama de prioridades. Por ejemplo, si el CMTS define 2 niveles de prioridad, debería interpretar los valores 0 a 3 como baja prioridad y los valores 4 a 7 como alta prioridad. El servidor de política DEBERÍA normalizar o bien transformar este valor para asegurar un sistema de prioridades coherente en todos los CMTS del operador, pero responder a las peticiones de AM con el valor de prioridad original.

El bit de apropiación con prioridad es utilizado por el PDP para ordenar al PEP que aplique un control de admisión basado en prioridades. El soporte de la apropiación con prioridad es facultativo, es decir, un PEP PUEDE ignorar este bit. Si la apropiación con prioridad no es solicitada por el PDP o no es implementada por el PEP, la política de control de admisión se basará en el principio primer llegado primer servido. Si el PEP decide aplicar apropiación con prioridad, DEBE apoderarse del ancho de banda de sesiones cuya prioridad sea inferior a la de esta sesión, comenzando por la(s) sesión(es) de menor prioridad. Este bit no se utiliza para controlar qué sesiones son apropiables; en cambio, una sesión inapropiable se solicita utilizando la máxima prioridad. Si una sesión de menor prioridad termina, de resultas de una apropiación con prioridad, el PEP DEBE enviar un mensaje Gate-Report-State al PDP, con un valor del campo motivo del objeto GateState igual a 1 "cierre iniciado por el CMTS debido a una reasignación de reservas" y pasar la puerta al estado "fin".

Los gestores de aplicación que ofrecen nuevos servicios PUEDEN utilizar el campo configurable para especificar nuevas clases de sesión. El servidor de política PUEDE soportar políticas configurables basadas en este valor y PUEDE reescribir este campo antes de reenviar el mensaje al CMTS. Un CMTS PUEDE implementar una nueva métrica de clase de sesión utilizando estos bits, pero el valor 0 DEBE hacerse corresponder a un valor por defecto razonable para un PDP que no esté interesado es esta métrica.

El campo DSCP/TOS es un campo de bits de 1 byte [6] definido por las estructuras alternativas siguientes, dependiendo de la estrategia de gestión de la red. Este campo, combinado con la máscara DSCP/TOS de 1 byte, se utiliza para identificar bits particulares dentro del byte IPv4 de DSCP/TOS.

0	1	2	3	4	5	6	7
Punto de código de servicios diferenciados (DSCP)						No se utiliza	No se utiliza

0	1	2	3	4	5	6	7
Precedencia IP			TOS IP				No se utiliza

Si se fija el bit 'habilitar' del campo banderas de GateSpec, el CMTS DEBE marcar los paquetes que atraviesan el valor DSCP/TOS de CMTS. Si se libera el bit 'habilitar', el CMTS NO DEBE efectuar ninguna marcación.

Los temporizadores T1, T2, T3 y T4 son enteros sin signo de 2 bytes especificados en segundos y DEBEN ser utilizados como se indica en el diagrama de transiciones de puerta que se describe en 6.2. Un valor de cero para T1 indica que DEBE utilizarse el valor provisionado por el CMTS para el temporizador. T2 corresponde al temporizador admitido DOCSIS y T3 corresponde al temporizador activo DOCSIS. Todos los requisitos DOCSIS correspondientes se aplican a estos temporizadores. De manera específica, un valor cero para cualquiera de esos temporizadores significa que el temporizador correspondiente DEBE ser inhabilitado.

6.4.2.6 Clasificador

El objeto Clasificador especifica las reglas de concordancia de paquetes asociadas a una puerta. Como se indica en 6.4.3.1 y 6.4.3.2, se pueden incluir múltiples objetos Clasificador en el Gate-Set en previsión de reglas de clasificador complejas. El objeto Clasificador DEBE atenerse al formato siguiente.

Longitud = 24	S-Num = 6	S-Type = 1
ID de protocolo	Campo DSCP/TOS	Máscara DSCP/TOS
Dirección IP de origen (4 octetos)		
Dirección IP de destino (4 octetos)		
Puerto de origen	Puerto de destino	
Prioridad	Reservado	

La dirección IP de origen y la dirección IP de destino DEBEN ser un par de direcciones IPv4 de 4 octetos o cero en caso de no concordancia (es decir, una especificación comodín que concordará con cualquier paquete).

El puerto de origen y el puerto de destino DEBEN ser un par de valores enteros sin signo de 2 bytes o cero en caso de no concordancia.

El ID de protocolo debe ser conforme con B.C.2.1.5.2 de [1], o cero en caso de no concordancia.

El campo DSCP/TOS es un campo de bits de 1 byte que DEBE atenerse a las estructuras alternativas siguientes:

0	1	2	3	4	5	6	7
Punto de código de servicios diferenciados						No se utiliza	Habilitar

0	1	2	3	4	5	6	7
Precedencia IP			TOS IP				Habilitar

Máscara DSCP/TOS es un campo de bits de 1 byte que proporciona una máscara de bits utilizada para seleccionar bits pertinentes del valor del campo DSCP/TOS acompañante.

Si se fija el bit 'habilitar', el CMTS DEBE utilizar estos valores para construir la gama TOS IP y el campo máscara especificado en su mensajería DSx. Si se libera el bit 'habilitar', el CMTS DEBE omitir los valores de gama TOS IP y máscara de su mensajería DSx y excluir el byte TOS IP del proceso de clasificación de paquetes.

Prioridad es un campo de 1 byte que permite diferenciar entre clasificadores que podrían solaparse. Si no se requiriese un valor de prioridad específico, DEBERÍA utilizarse un valor por defecto de 64. Para un análisis más profundo del campo prioridad, véase B.C.2.1.3.5 de [1].

6.4.2.7 Perfiles de tráfico

Hay tres maneras diferentes de expresar un perfil de tráfico. El perfil de tráfico puede expresarse vía un objeto FlowSpec, o bien un nombre de clase de servicio DOCSIS o con parámetros específicos de DOCSIS. Los tres métodos se distinguen mediante un valor S-Type diferente en el objeto Perfil de tráfico (S-Num = 7). Un valor S-Type de 1 indica que el objeto contiene un perfil de tráfico especificado en formato de FlowSpec de RSVP. Un valor S-Type de 2 indica que el objeto contiene un perfil de tráfico especificado en formato de nombre de clase de servicio DOCSIS. Un valor S-Type mayor o igual que 3 indica que el objeto contiene un perfil de tráfico especificado mediante parámetros específicos de DOCSIS.

Todos los perfiles de tráfico utilizan semántica de "sustitución", lo que significa que las capacidades máximas presentes en el perfil de tráfico reemplazan a todos las capacidades máximas existentes asociados a la puerta y el flujo de servicio correspondiente. Por ello, todos los parámetros de tráfico asociados a una puerta dada DEBEN ser incluidos en cualquier mensaje que incluya un perfil de tráfico.

Todos los perfiles de tráfico comparten un campo común conocido como campo capacidad máxima. Es un campo de bits que señala los tipos de capacidad máxima (esto es, autorizada, reservada y comprometida) que están presentes en el objeto. Un valor de 1 en un campo de bits dado indica que el tipo de capacidad máxima está presente en el perfil de tráfico.

- Bit 0: Capacidad máxima autorizada.
- Bit 1: Capacidad máxima reservada.
- Bit 2: Capacidad máxima comprometida.

Así pues, un patrón de bits de 001 (o 0x01) indica la presencia de la capacidad máxima autorizada únicamente, mientras que un valor de 111 (o 0x7) indica la presencia de los tres tipos de capacidades máximas. Sólo se admiten los valores siguientes: 001, 011 y 111; el campo capacidad máxima DEBE fijarse en uno de esos tres valores admitidos. Otras limitaciones impuestas al valor del campo capacidad máxima pueden depender del estado en que se encuentre la puerta. Para más información, véase 6.2.

Para los formatos de perfil de tráfico que admitan varios conjuntos de parámetros de capacidad máxima, la correspondencia de los conjuntos de parámetros de capacidad máxima sigue uno de los métodos siguientes:

Si todos los tipos de capacidad máxima indicados en el campo capacidad máxima comparten un conjunto común de parámetros de capacidad máxima, el PDP DEBERÍA asegurarse de que en el perfil de tráfico haya un solo conjunto de parámetros de capacidad máxima. Esto permite la transmisión más eficaz y el procesamiento del perfil de tráfico en todo el sistema.

En caso contrario, el PDP DEBE asegurar que se incluya un solo conjunto de parámetros de capacidad máxima para cada uno de los tipos de capacidad máxima que se indican en el campo capacidad máxima. El orden correcto de los conjuntos de parámetros de capacidad máxima se muestra en el diagrama de mensajes adecuado que figura en 6.4.2.7.1 y 6.4.2.7.3 a 6.4.2.7.8.

Si bien todos los perfiles de tráfico terminan proporcionando QoS por la red de acceso, es importante señalar varias diferencias, un tanto sutiles, entre los mecanismos de señalización. Como se ha advertido previamente, la conversión de un objeto FlowSpec (S-Type 1) en parámetros DOCSIS por el CMTS resulta por lo general menos eficaz que la especificación de los propios parámetros DOCSIS. Dicho esto, hay que señalar que la especificación explícita de los parámetros DOCSIS (S-Types 3 a 7) tampoco es la panacea ya que la MIB de QoS sólo registra cronológicamente información de QoS sobre flujos de servicio denominados en su ServiceFlowLogTable (cuadro de registro cronológico de flujos de servicio). Por ello, sólo se registrará cronológicamente en ese cuadro la información de QoS de los flujos creados vía S-Type 2. Es posible que, a veces, esto no tenga mayor importancia, pero a efectos de depuración y seguimiento operativo en general este matiz debería ser tenido en cuenta por los operadores y vendedores de gestores de aplicación evaluando las alternativas de señalización del perfil de tráfico proporcionadas por la presente Recomendación.

6.4.2.7.1 FlowSpec

El objeto FlowSpec (especificación de flujo) define el perfil de tráfico asociado a una puerta mediante un esquema de parametrización similar al RSVP. El establecimiento de la correspondencia entre estos parámetros y los parámetros DOCSIS se especifica en la cláusula 8. El objeto FlowSpec DEBE atenerse a la especificación siguiente:

Longitud = 36 ó 64 ó 92		S-Num = 7	S-Type = 1
Capacidad máxima	Número de servicio	Reservado	Reservado
Capacidad máxima autorizada			
Velocidad de colector testigo [r] (número en coma flotante IEEE)			
Tamaño de colector testigo [b] (número en coma flotante IEEE)			
Velocidad de datos de cresta (p) (número en coma flotante IEEE)			
Unidad mínima sujeta a aplicación de política [m] (entero)			
Tamaño de paquete máximo [M] (entero)			
Velocidad [R] (número en coma flotante IEEE)			
Término suelto [S] (entero)			
Capacidad máxima reservada (facultativo)			
Velocidad de colector testigo [r] (número en coma flotante IEEE)			
Tamaño de colector testigo [b] (número en coma flotante IEEE)			
Velocidad de datos de cresta (p) (número en coma flotante IEEE)			
Unidad mínima sujeta a aplicación de política [m] (entero)			
Tamaño de paquete máximo [M] (entero)			
Velocidad [R] (número en coma flotante IEEE)			
Término suelto [S] (entero)			
Capacidad máxima comprometido (facultativo)			
Velocidad de colector testigo [r] (número en coma flotante IEEE)			
Tamaño de colector testigo [b] (número en coma flotante IEEE)			
Velocidad de datos de cresta (p) (número en coma flotante IEEE)			
Unidad mínima sujeta a aplicación de política [m] (entero)			
Tamaño de paquete máximo [M] (entero)			
Velocidad [R] (número en coma flotante IEEE)			
Término suelto [S] (entero)			

El campo número de servicio corresponde al número de servicio FlowSpec de RSVP definido en [3]. Si el número de servicio se fija en 5, ello indica que el servicio de carga controlada y el CMTS DEBEN utilizar solamente los valores de TSpec (es decir, parámetros de colector testigo) para llevar a cabo las operaciones de autorización, reserva y compromiso necesarias. En el caso del servicio de carga controlada, el CMTS DEBE ignorar los campos R y S de RSpec.

Si el número de servicio se fija en 2, ello indica que el servicio garantizado y el CMTS DEBEN utilizar tanto los valores de TSpec como los de RSpec para llevar a cabo las operaciones de autorización, reserva y compromiso necesarias.

Los valores de r, b, p, m, M, R y s se definen y describen en la cláusula 9.

6.4.2.7.2 Nombre de clase de servicio DOCSIS

El objeto Nombre de clase de servicio DOCSIS define el nombre de clase de servicio preconfigurado asociado a una puerta. El objeto Nombre de clase de servicio DOCSIS DEBE atenerse a la especificación siguiente:

Longitud = 12 ó 16 ó 20 ó 24		S-Num = 7	S-Type = 2
Capacidad máxima	Reservado	Reservado	Reservado
Nombre de clase de servicio			

El nombre de clase de servicio DEBE estar constituido por 2 a 16 bytes que forman una cadena ASCII terminada en el carácter "nulo". (Véase B.C.2.2.3.4 de [1]). Este nombre DEBE rellenarse con bytes de valor nulo de modo que puedan alinearse en demarcaciones de 4 bytes.

Se señala que, a diferencia de un perfil de tráfico de FlowSpec que permite asociar diferentes parámetros a cada capacidad máxima, el perfil de tráfico de nombre de clase de servicio DOCSIS soporta diferentes estados de la puerta especificados por el campo capacidad máxima, pero cada capacidad máxima se define por el mismo nombre de clase de servicio DOCSIS asociado. Así es posible hacer que operaciones de compromiso bifásicas utilicen los nombres de clase de servicio DOCSIS, pero las capacidades máximas deben ser idénticas. Se señala que también es posible cambiar el nombre de clase de servicio DOCSIS asociado a una puerta, pero ese cambio se aplica a todos las capacidades máximas asociados a una puerta dada.

6.4.2.7.3 Servicio de mejor esfuerzo

El objeto Mejor esfuerzo define el perfil de tráfico asociado a una puerta mediante un esquema de parametrización específico de DOCSIS en sentido ascendente. El objeto Mejor esfuerzo DEBE atenerse a la especificación siguiente:

Longitud = 32, 56 u 80		S-Num = 7	S-Type = 3
Capacidad máxima	Reservado	Reservado	Reservado
Capacidad máxima autorizada			
Prioridad de tráfico	Reservado		
Política de petición/transmisión			
Velocidad de tráfico sostenida máxima			
Ráfaga de tráfico máxima			
Velocidad de tráfico reservada mínima			
Tamaño asumido de paquete de velocidad de tráfico reservada mínima		Reservado	

Capacidad máxima reservada (facultativo)	
Prioridad de tráfico	Reservado
Política de petición/transmisión	
Velocidad de tráfico sostenida máxima	
Ráfaga de tráfico máxima	
Velocidad de tráfico reservada mínima	
Tamaño asumido de paquete de velocidad de tráfico reservada mínima	Reservado
Capacidad máxima comprometida (facultativo)	
Prioridad de tráfico	Reservado
Política de petición/transmisión	
Velocidad de tráfico sostenida máxima	
Ráfaga de tráfico máxima	
Velocidad de tráfico reservada mínima	
Tamaño asumido de paquete de velocidad de tráfico reservada mínima	Reservado

El campo prioridad de tráfico es un campo entero sin signo de 1 byte que especifica la prioridad relativa asignada al flujo de servicio en comparación con otros flujos. Este campo se define plenamente en B.C.2.2.5.1 de [1]. Si no se requiriese un valor de prioridad de tráfico específico, DEBERÍA utilizarse una prioridad de tráfico por defecto de 0.

El campo política de petición/transmisión es un campo de bits de 4 bytes definido en B.C.2.2.6.3 de [1]. Si no se requiriese un valor de política de petición/transmisión específico, DEBERÍA utilizarse un valor de política de petición/transmisión por defecto de 0.

El campo velocidad de tráfico sostenida máxima es un campo entero sin signo de 4 bytes que especifica el parámetro velocidad, en bit/s, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.2 de [1]. Un valor de 0 indica que se pide una velocidad sostenida máxima no aplicada explícitamente. Si no se requiriese una velocidad de tráfico sostenida máxima específica, DEBERÍA utilizarse una velocidad de tráfico sostenida máxima por defecto de 0.

El campo ráfaga de tráfico máxima es un campo entero sin signo de 4 bytes que especifica el tamaño del colector testigo, en bytes, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.3 de [1]. Si no se requiriese una ráfaga de tráfico máxima específica, DEBERÍA utilizarse una ráfaga de tráfico máxima por defecto de 3044 bytes. El valor de este parámetro no tiene efecto a menos que se haya proporcionado un valor distinto de cero para el parámetro velocidad de tráfico sostenida máxima.

El campo velocidad de tráfico reservada mínima es un campo entero sin signo de 4 bytes que especifica la velocidad mínima, en bit/s, reservada para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.4 de [1]. Si no se requiriese una velocidad de tráfico reservada mínima específica, DEBERÍA utilizarse una velocidad de tráfico reservada mínima por defecto de 0.

El campo tamaño asumido de paquete de velocidad de tráfico reservada mínima es un campo entero sin signo de 2 bytes que especifica un tamaño asumido de paquete mínimo, en bytes, para el que se proporcionará la velocidad de tráfico reservada mínima para este flujo. Este campo se define plenamente en B.C.2.2.5.5 de [1]. Si no se requiriese un tamaño asumido de paquete de velocidad de tráfico reservada mínima específico, DEBERÍA utilizarse un tamaño asumido de paquete de velocidad de tráfico reservada mínima por defecto de 0. Tras la recepción de un valor de 0, el CMTS DEBE utilizar su tamaño por defecto específico de la implementación para este parámetro, no 0 bytes.

6.4.2.7.4 Servicio de interrogación secuencial no en tiempo real

El objeto Interrogación secuencial no en tiempo real define el perfil de tráfico asociado a una puerta en sentido ascendente mediante un esquema de parametrización específico de DOCSIS. El objeto Interrogación secuencial no en tiempo real DEBE atenerse a la especificación siguiente:

Longitud = 36, 64 ó 92		S-Num = 7	S-Type = 4
Capacidad máxima	Reservado	Reservado	Reservado
Capacidad máxima autorizada			
Prioridad de tráfico	Reservado		
Política de petición/transmisión			
Velocidad de tráfico sostenida máxima			
Ráfaga de tráfico máxima			
Velocidad de tráfico reservada mínima			
Tamaño asumido de paquete de velocidad de tráfico reservada mínima		Reservado	
Intervalo de interrogación secuencial nominal			
Capacidad máxima reservada (facultativo)			
Prioridad de tráfico	Reservado		
Política de petición/transmisión			
Velocidad de tráfico sostenida máxima			
Ráfaga de tráfico máxima			
Velocidad de tráfico reservada mínima			
Tamaño asumido de paquete de velocidad de tráfico reservada mínima		Reservado	
Intervalo de interrogación secuencial nominal			
Capacidad máxima comprometida (facultativo)			
Prioridad de tráfico	Reservado		
Política de petición/transmisión			
Velocidad de tráfico sostenida máxima			
Ráfaga de tráfico máxima			
Velocidad de tráfico reservada mínima			
Tamaño asumido de paquete de velocidad de tráfico reservada mínima		Reservado	
Intervalo de interrogación secuencial nominal			

El campo prioridad de tráfico es un campo entero sin signo de 1 byte que especifica la prioridad relativa asignada al flujo de servicio en comparación con otros flujos. Este campo se define plenamente en B.C.2.2.5.1 de [1]. Si no se requiriese un valor de prioridad de tráfico específico, DEBERÍA utilizarse una prioridad de tráfico por defecto de 0.

El campo política de petición/transmisión es un campo de bits de 4 bytes definido en B.C.2.2.6.3 de [1].

NOTA – Para este tipo de calendarización de flujo de servicio no hay valor por defecto de política de petición/transmisión y todos los valores (incluido 0) tienen un significado en DOCSIS.

El campo velocidad de tráfico sostenida máxima es un campo entero sin signo de 4 bytes que especifica el parámetro velocidad, en bit/s, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.2 de [1]. Un valor de 0 indica que se pide una velocidad sostenida máxima no aplicada explícitamente. Si no se requiriese

una de velocidad de tráfico sostenida máxima específica, DEBERÍA utilizarse una velocidad de tráfico sostenida máxima por defecto de 0.

El campo ráfaga de tráfico máxima es un campo entero sin signo de 4 bytes que especifica el tamaño del colector testigo, en bytes, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.3 de [1]. Si no se requiriese una ráfaga de tráfico máxima específica, DEBERÍA utilizarse una ráfaga de tráfico máxima por defecto de 3044 bytes. El valor de este parámetro no tiene efecto a menos que se haya proporcionado un valor distinto de cero para el parámetro velocidad de tráfico sostenida máxima.

El campo velocidad de tráfico reservada mínima es un campo entero sin signo de 4 bytes que especifica la velocidad mínima, en bit/s, reservada para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.4 de [1]. Si no se requiriese una velocidad de tráfico reservada mínima específica, DEBERÍA utilizarse una velocidad de tráfico reservada mínima por defecto de 0.

El campo tamaño asumido de paquete de velocidad de tráfico reservada mínima es un campo entero sin signo de 2 bytes que especifica un tamaño asumido de paquete mínimo, en bytes, para el que se proporcionará la velocidad de tráfico reservada mínima para este flujo. Este campo se define plenamente en B.C.2.2.5.5 de [1]. Si no se requiriese un tamaño asumido de paquete de velocidad de tráfico reservada mínima específico, DEBERÍA utilizarse un Tamaño asumido de paquete de velocidad de tráfico reservada mínima por defecto de 0. Tras la recepción de un valor de 0, el CMTS DEBE utilizar su tamaño por defecto específico de la implementación para este parámetro, no 0 bytes.

El campo intervalo de interrogación secuencial nominal es un campo entero sin signo de 4 bytes que especifica el intervalo nominal (en unidades de microsegundos) entre oportunidades de petición de unidifusión sucesivas para este flujo de servicio por el canal en sentido ascendente. Este campo se define plenamente en B.C.2.2.6.4 de [1]. Si no se requiriese un intervalo de interrogación secuencial nominal específico, DEBERÍA utilizarse un intervalo de interrogación secuencial nominal por defecto de 0. Tras la recepción de un valor de 0, el CMTS DEBE utilizar su tamaño por defecto específico de la implementación para este parámetro, no 0 microsegundos.

6.4.2.7.5 Servicio de interrogación secuencial en tiempo real

El objeto Interrogación secuencial en tiempo real define el perfil de tráfico asociado a una puerta en sentido ascendente mediante un esquema de parametrización específico de DOCSIS. El objeto Interrogación secuencial en tiempo real DEBE atenerse a la especificación siguiente:

<table>
<tr><td colspan="2">Longitud = 36, 64 ó 92</td><td>S-Num = 7</td><td>S-Type = 5</td></tr>
<tr><td>Capacidad máxima</td><td>Reservado</td><td>Reservado</td><td>Reservado</td></tr>
<tr><td colspan="4">Capacidad máxima autorizada</td></tr>
<tr><td colspan="4">Política de petición/transmisión</td></tr>
<tr><td colspan="4">Velocidad de tráfico sostenida máxima</td></tr>
<tr><td colspan="4">Ráfaga de tráfico máxima</td></tr>
<tr><td colspan="4">Velocidad de tráfico reservada mínima</td></tr>
<tr><td colspan="2">Tamaño asumido de paquete de velocidad de tráfico reservada mínima</td><td colspan="2">Reservado</td></tr>
<tr><td colspan="4">Intervalo de interrogación secuencial nominal</td></tr>
<tr><td colspan="4">Fluctuación de interrogación secuencial tolerada</td></tr>
</table>

Capacidad máxima reservada (facultativo)	
Política de petición/transmisión	
Velocidad de tráfico sostenida máxima	
Ráfaga de tráfico máxima	
Velocidad de tráfico reservada mínima	
Tamaño asumido de paquete de velocidad de tráfico reservada mínima	Reservado
Intervalo de interrogación secuencial nominal	
Fluctuación de interrogación secuencial tolerada	
Capacidad máxima comprometida (facultativo)	
Política de petición/transmisión	
Velocidad de tráfico sostenida máxima	
Ráfaga de tráfico máxima	
Velocidad de tráfico reservada mínima	
Tamaño asumido de paquete de velocidad de tráfico reservada mínima	Reservado
Intervalo de interrogación secuencial nominal	
Fluctuación de interrogación secuencial tolerada	

El campo política de petición/transmisión es un campo de bits de 4 bytes definido en B.C.2.2.6.3 de [1].

NOTA – Con este tipo de calendarización de flujo de servicio no hay valor por defecto para política de petición/transmisión y todos los valores (incluido 0) tienen un significado en DOCSIS.

El campo velocidad de tráfico sostenida máxima es un campo entero sin signo de 4 bytes que especifica el parámetro velocidad, en bit/s, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.2 de [1]. Un valor de 0 indica que se pide una velocidad sostenida máxima no aplicada explícitamente. Si no se requiriese una velocidad de tráfico sostenida máxima específica, DEBERÍA utilizarse una velocidad de tráfico sostenida máxima por defecto de 0.

El campo ráfaga de tráfico máxima es un campo entero sin signo de 4 bytes que especifica el tamaño del colector testigo, en bytes, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.3 de [1]. Si no se requiriese una ráfaga de tráfico máxima específica, DEBERÍA utilizarse una ráfaga de tráfico máxima por defecto de 3044 bytes. El valor de este parámetro no tiene efecto a menos que se haya proporcionado un valor distinto de cero para el parámetro velocidad de tráfico sostenida máxima.

El campo velocidad de tráfico reservada mínima es un campo entero sin signo de 4 bytes que especifica la velocidad mínima, en bits/s, reservada para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.4 de [1]. Si no se requiriese una velocidad de tráfico reservada mínima específica, DEBERÍA utilizarse una velocidad de tráfico reservada mínima por defecto de 0.

El campo tamaño asumido de paquete de velocidad de tráfico reservada mínima es un campo entero sin signo de 2 bytes que especifica un tamaño asumido de paquete mínimo, en bytes, para el que se proporcionará la velocidad de tráfico reservada mínima para este flujo. Este campo se define plenamente en B.C.2.2.5.5 de [1]. Si no se requiriese un tamaño asumido de paquete de velocidad de tráfico reservada mínima específico, DEBERÍA utilizarse un tamaño asumido de paquete de velocidad de tráfico reservada mínima por defecto de 0. Tras la recepción de un valor de 0, el CMTS DEBE utilizar su tamaño por defecto específico de la implementación para este parámetro, no 0 bytes.

El campo intervalo de interrogación secuencial nominal es un campo entero sin signo de 4 bytes que especifica el intervalo nominal (en unidades de microsegundos) entre oportunidades de petición de unidifusión sucesivas para este flujo de servicio por el canal en sentido ascendente. Este campo se define plenamente en B.C.2.2.6.4 de [1]. Para este tipo de calendarización de flujo de servicio no hay valor por defecto de intervalo de interrogación secuencial nominal.

El campo fluctuación de interrogación secuencial tolerada es un campo entero sin signo de 4 bytes que especifica la cantidad máxima de tiempo que se puede demorar el intervalo de petición de unidifusión con respecto al calendario periódico nominal (medido en microsegundos) Este campo se define plenamente en B.C.2.2.6.5 de [1]. Si no se requiriese una fluctuación de interrogación secuencial tolerada específica, DEBERÍA utilizarse una fluctuación de interrogación secuencial tolerada por defecto de 0. Tras la recepción de un valor de 0, el CMTS DEBE utilizar su tamaño por defecto específico de la implementación para este parámetro – no 0 microsegundos.

6.4.2.7.6 Servicio de concesión no solicitada

El objeto Concesión no solicitada define el perfil de tráfico asociado a una puerta en sentido ascendente mediante un esquema de parametrización específico de DOCSIS. El objeto Concesión no solicitada DEBE atenerse a la especificación siguiente:

Longitud = 24, 40 ó 56		S-Num = 7	S-Type = 6
Capacidad máxima	Reservado	Reservado	Reservado
Capacidad máxima autorizada			
Política de petición/transmisión			
Tamaño de concesión no solicitada		Concesiones por intervalo	Reservado
Intervalo de concesión nominal			
Fluctuación de concesión tolerada			
Capacidad máxima reservada (facultativo)			
Política de petición/transmisión			
Tamaño de concesión no solicitada		Concesiones por intervalo	Reservado
Intervalo de concesión nominal			
Fluctuación de concesión tolerada			
Capacidad máxima comprometida (facultativo)			
Política de petición/transmisión			
Tamaño de concesión no solicitada		Concesiones por intervalo	Reservado
Intervalo de concesión nominal			
Fluctuación de concesión tolerada			

El campo política de petición/transmisión es un campo de bits de 4 bytes definido en B.C.2.2.6.3 de [1].

NOTA – Para este tipo de calendarización de flujo de servicio no hay valor por defecto de política de petición/transmisión y todos los valores (incluido 0) tienen un significado en DOCSIS.

El campo tamaño de concesión no solicitada es un campo entero sin signo de 2 bytes que especifica el tamaño de la concesión, en bytes, definido en B.C.2.2.6.6 de [1]. No hay valor por defecto para tamaño de concesión no solicitada.

El campo concesiones por intervalo es un campo entero sin signo de 1 byte que especifica el número de concesiones por intervalo de concesión nominal definido en B.C.2.2.6.9 de [1]. No hay valor por defecto para concesiones por intervalo, pero se recomienda un valor de 1.

El campo intervalo de concesión nominal es un campo entero sin signo de 4 bytes que especifica el tiempo nominal entre oportunidades de concesión de datos sucesivas para este flujo de servicio (en unidades de microsegundos) definido en B.C.2.2.6.7 de [1]. No hay valor por defecto para intervalo de concesión nominal.

El campo fluctuación de concesión tolerada es un campo entero sin signo de 4 bytes que especifica la cantidad máxima de tiempo que se pueden demorar las oportunidades de transmisión con respecto al calendario periódico nominal (en unidades de microsegundos) definida en B.C.2.2.6.8 de [1]. No hay valor por defecto para fluctuación de concesión tolerada.

6.4.2.7.7 Servicio de concesión no solicitada con detección de actividad

El objeto Concesión no solicitada con detección de actividad define el perfil de tráfico asociado a una puerta en sentido ascendente mediante un esquema de parametrización específico de DOCSIS. El objeto Concesión no solicitada con detección de actividad DEBE atenerse a la especificación siguiente:

Longitud = 32, 56 u 80		S-Num = 7	S-Type = 7
Capacidad máxima	Reservado	Reservado	Reservado
Capacidad máxima autorizada			
Política de petición/transmisión			
Tamaño de concesión no solicitada		Concesiones por intervalo	Reservado
Intervalo de concesión nominal			
Fluctuación de concesión tolerada			
Intervalo de interrogación secuencial nominal			
Fluctuación de interrogación secuencial tolerada			
Capacidad máxima reservada (facultativo)			
Política de petición/transmisión			
Tamaño de concesión no solicitada		Concesiones por intervalo	Reservado
Intervalo de concesión nominal			
Fluctuación de concesión tolerada			
Intervalo de interrogación secuencial nominal			
Fluctuación de interrogación secuencial tolerada			
Capacidad máxima comprometida (facultativo)			
Política de petición/transmisión			
Tamaño de concesión no solicitada		Concesiones por intervalo	Reservado
Intervalo de concesión nominal			
Fluctuación de concesión tolerada			
Intervalo de interrogación secuencial nominal			
Fluctuación de interrogación secuencial tolerada			

El campo política de petición/transmisión es un campo de bits de 4 bytes definido en B.C.2.2.6.3 de [1].

NOTA – Para este tipo de calendarización de flujo de servicio no hay valor por defecto de política de petición/transmisión y todos los valores (incluido 0) tienen un significado en DOCSIS.

El campo tamaño de concesión no solicitada es un campo entero sin signo de 2 bytes que especifica el tamaño de la concesión, en bytes, definido en B.C.2.2.6.6 de [1]. No hay valor por defecto para tamaño de concesión no solicitada.

El campo concesiones por intervalo es un campo entero sin signo de 1 byte que especifica el número de concesiones por intervalo de concesión nominal definido en B.C.2.2.6.9 de [1]. No hay valor por defecto para concesiones por intervalo, pero se recomienda un valor de 1.

El campo intervalo de concesión nominal es un campo entero sin signo de 4 bytes que especifica el tiempo nominal entre oportunidades de concesión de datos sucesivas para este flujo de servicio (en unidades de microsegundos) definido en B.C.2.2.6.7 de [1]. No hay valor por defecto para intervalo de concesión nominal.

El campo fluctuación de concesión tolerada es un campo entero sin signo de 4 bytes que especifica la cantidad máxima de tiempo que se pueden demorar las oportunidades de transmisión con respecto al calendario periódico nominal (en unidades de microsegundos) definida en B.C.2.2.6.8 de [1]. No hay valor por defecto para fluctuación de concesión tolerada.

El campo intervalo de interrogación secuencial nominal es un campo entero sin signo de 4 bytes que especifica el intervalo nominal (en unidades de microsegundos) entre oportunidades de petición de unidifusión sucesivas para este flujo de servicio por el canal en sentido ascendente. Este campo se define plenamente en B.C.2.2.6.4 de [1]. No hay valor por defecto para intervalo de interrogación secuencial nominal.

El campo fluctuación de interrogación secuencial tolerada es un campo entero sin signo de 4 bytes que especifica la cantidad máxima de tiempo que se puede demorar el intervalo de petición de unidifusión con respecto al calendario periódico nominal (en unidades de microsegundos). Este campo se define plenamente en B.C.2.2.6.5 de [1]. Tras la recepción de un valor de 0, el CMTS DEBE utilizar su tamaño por defecto específico de la implementación para este parámetro, no 0 microsegundos.

6.4.2.7.8 Servicio en sentido descendente

El objeto Sentido descendente define el perfil de tráfico asociado a una puerta mediante un esquema de parametrización específico de DOCSIS en sentido descendente. El objeto Sentido descendente DEBE atenerse a la especificación siguiente:

<table>
<tr><td colspan="2">Longitud = 32, 56 u 80</td><td>S-Num = 7</td><td>S-Type = 8</td></tr>
<tr><td>Capacidad máxima</td><td>Reservado</td><td>Reservado</td><td>Reservado</td></tr>
<tr><td colspan="4">Capacidad máxima autorizada</td></tr>
<tr><td>Prioridad de tráfico</td><td colspan="3">Reservado</td></tr>
<tr><td colspan="4">Velocidad de tráfico sostenida máxima</td></tr>
<tr><td colspan="4">Ráfaga de tráfico máxima</td></tr>
<tr><td colspan="4">Velocidad de tráfico reservada mínima</td></tr>
<tr><td colspan="2">Tamaño asumido de paquete de velocidad de tráfico reservada mínima</td><td colspan="2">Reservado</td></tr>
<tr><td colspan="4">Latencia en sentido descendente máxima</td></tr>
<tr><td colspan="4">Capacidad máxima reservada (facultativo)</td></tr>
<tr><td>Prioridad de tráfico</td><td colspan="3">Reservado</td></tr>
<tr><td colspan="4">Velocidad de tráfico sostenida máxima</td></tr>
<tr><td colspan="4">Ráfaga de tráfico máxima</td></tr>
<tr><td colspan="4">Velocidad de tráfico reservada mínima</td></tr>
<tr><td colspan="2">Tamaño asumido de paquete de velocidad de tráfico reservada mínima</td><td colspan="2">Reservado</td></tr>
<tr><td colspan="4">Latencia en sentido descendente máxima</td></tr>
</table>

Capacidad máxima comprometida (facultativo)	
Prioridad de tráfico	Reservado
Velocidad de tráfico sostenida máxima	
Ráfaga de tráfico máxima	
Velocidad de tráfico reservada mínima	
Tamaño asumido de paquete de velocidad de tráfico reservada mínima	Reservado
Latencia en sentido descendente máxima	

El campo prioridad de tráfico es un campo entero sin signo de 1 byte que especifica la prioridad relativa asignada al flujo de servicio en comparación con otros flujos. Este campo se define plenamente en B.C.2.2.5.1 de [1]. Si no se requiriese un valor de prioridad de tráfico específico, DEBERÍA utilizarse una prioridad de tráfico por defecto de 0.

El campo velocidad de tráfico sostenida máxima es un campo entero sin signo de 4 bytes que especifica el parámetro velocidad, en bit/s, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.2 de [1]. Un valor de 0 indica que se pide una velocidad sostenida máxima no aplicada explícitamente. Si no se requiriese una velocidad de tráfico sostenida máxima específica, DEBERÍA utilizarse una velocidad de tráfico sostenida máxima por defecto de 0.

El campo ráfaga de tráfico máxima es un campo entero sin signo de 4 bytes que especifica el tamaño del colector testigo, en bytes, para un límite de velocidad basado en el colector testigo para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.3 de [1]. Si no se requiriese una ráfaga de tráfico máxima específica, DEBERÍA utilizarse una ráfaga de tráfico máxima por defecto de 3044 bytes. El valor de este parámetro no tiene efecto a menos que se haya proporcionado un valor distinto de cero para el parámetro velocidad de tráfico sostenida máxima.

El campo velocidad de tráfico reservada mínima es un campo entero sin signo de 4 bytes que especifica la velocidad mínima, en bit/s, reservada para este flujo de servicio. Este campo se define plenamente en B.C.2.2.5.4 de [1]. Si no se requiriese una velocidad de tráfico reservada mínima específica, DEBERÍA utilizarse una velocidad de tráfico reservada mínima por defecto de 0.

El campo tamaño asumido de paquete de velocidad de tráfico reservada mínima es un campo entero sin signo de 2 bytes que especifica un tamaño asumido de paquete mínimo, en bytes, para el que se proporcionará la velocidad de tráfico reservada mínima para este flujo. Este campo se define plenamente en B.C.2.2.5.5 de [1]. Si no se requiriese un tamaño asumido de paquete de velocidad de tráfico reservada mínima específico, DEBERÍA utilizarse un tamaño asumido de paquete de velocidad de tráfico reservada mínima por defecto de 0. Tras la recepción de un valor de 0, el CMTS DEBE utilizar su tamaño por defecto específico de la implementación para este parámetro, no 0 bytes.

El campo latencia en sentido descendente máxima es un campo entero sin signo de 4 bytes que especifica la latencia máxima entre la recepción de un paquete en la NSI del CMTS y el reenvío del paquete por su interfaz RF definida en B.C.2.2.7.1 de [1]. Si no se requiriese una latencia en sentido descendente máxima específica, DEBERÍA utilizarse una latencia en sentido descendente máxima por defecto de 0. Tras la recepción de un valor de 0, el CMTS NO DEBE incluir este parámetro en su señalización DOCSIS para este flujo de servicio.

6.4.2.8 Información de generación de evento

El objeto Información de generación de evento contiene toda la información necesaria para soportar los mensajes de evento especificados y requeridos en la Rec. UIT-T J.164. El objeto Información de generación de evento DEBE atenerse a la especificación siguiente:

Longitud = 44	S-Num = 8	S-Type = 1
Primary-Record-Keeping-Server-IP-Address (4 octetos)		
Primary-Record-Keeping-Server-Port	Reservado	
Secondary-Record-Keeping-Server-IP-Address (4 octetos)		
Secondary-Record-Keeping-Server-Port	Reservado	
Billing-Correlation-ID (24 bytes)		

El campo Primary-Record-Keeping-Server-IP-Address (dirección IP de servidor de mantenimiento de registros primario) es un campo de 4 bytes que DEBE contener la dirección IPv4 del RKS primario a donde se han de enviar los registros de eventos.

El campo Primary-Record-Keeping-Server-Port (puerto de servidor de mantenimiento de registros primario) es un entero sin signo de 2 bytes que DEBE contener el número de puerto del RKS primario a donde se han de enviar los registros de eventos.

El campo Secondary-Record-Keeping-Server-IP-Address (dirección IP de servidor de mantenimiento de registros secundario) es un campo de 4 bytes que DEBE contener la dirección IPv4 del RKS secundario a donde se han de enviar los registros si el RKS primario no está disponible.

El campo Secondary-Record-Keeping-Server-Port (puerto de servidor de mantenimiento de registros secundario) es un entero sin signo de 2 bytes que DEBE contener el número de puerto del RKS secundario a donde se han de enviar los registros de eventos.

El campo Billing-Correlation-ID es un campo de 24 bytes que DEBE contener el identificador asignado por el AM o el PS para todos los registros relacionados con esta sesión. Para la definición y el formato de este atributo, véase [10].

6.4.2.9 Límite de utilización basado en volumen

El objeto Límite de utilización basado en volumen especifica la cantidad de datos que pueden ser transmitidos por esta puerta antes de alcanzar un umbral límite de volumen. Este objeto es FACULTATIVO en un mensaje Gate-Set y un mensaje Gate-Info-Ack. NO DEBE ser utilizado en ningún otro mensaje. El objeto Límite de utilización basado en volumen DEBE atenerse a la especificación siguiente:

Longitud = 12	S-Num =9	S-Type = 1
Límite de utilización		

Límite de utilización es un entero sin signo de 8 bytes definido en unidades de kilobytes. Un valor de cero indica que no se impone ningún límite de volumen. Los bytes contados hacia el límite van desde el byte que sigue a la secuencia de verificación de encabezamiento (HCS, *header check*

sequence) del encabezamiento de MAC DOCSIS hasta el final de la verificación por redundancia cíclica (CRC, *cyclic redundancy check*) para todos los paquetes transmitidos por el flujo de servicio asociado a esta puerta.

6.4.2.10 Límite de utilización basado en tiempo

El objeto Límite de utilización basado en tiempo especifica la cantidad de tiempo que una puerta puede permanecer comprometida antes de alcanzar un umbral límite de tiempo. El objeto Límite de utilización basado en tiempo DEBE atenerse a la especificación siguiente:

Longitud = 8	S-Num =10	S-Type = 1
Límite de tiempo		

Límite de tiempo es un entero sin signo de 4 bytes definido en unidades de segundos. Se trata del límite impuesto a la cantidad de tiempo que una puerta puede estar en estado comprometido. Este objeto es FACULTATIVO en un mensaje Gate-Set. Si se incluye en un mensaje Gate-Set, este objeto DEBE ser almacenado por el CMTS y proporcionado en respuesta a cualesquiera consultas de puerta subsiguientes. Mientras que el gestor de aplicación TIENE QUE suprimir las puertas asociadas a una sesión de medios que haya rebasado su límite de utilización basado en tiempo, el CMTS o el servidor de política PUEDEN utilizar este objeto para controlar la aplicación por el gestor de aplicación de los límites de utilización basados en tiempo. El gestor de aplicación o el servidor de política PUEDEN también efectuar indagaciones con respecto a este objeto como parte de la recuperación tras un fallo o de otro mecanismo.

Un valor de cero indica que no hay límite de tiempo para la puerta asociada.

6.4.2.11 Datos opacos

El objeto Datos opacos contiene información que un servidor de política o gestor de aplicación PUEDE almacenar en un CMTS permaneciendo opaca al CMTS. El objeto Datos opacos es facultativo en un mensaje Gate-Set. NO DEBE ser utilizado en ningún otro mensaje enviado por el PDP al PEP. Si el objeto está presente, el CMTS DEBE almacenar el objeto Datos opacos localmente, e incluirlo en todos los mensajes que genere hacia el servidor de política asociado a la puerta.

Si el objeto Datos opacos está incluido en un mensaje Gate-Set que vaya del gestor de aplicación a un servidor de política, el servidor de política DEBE reenviar este objeto al CMTS. La longitud del objeto Datos opacos está fijada en 8 bytes.

Longitud = 12	S-Num =11	S-Type = 1
Datos opacos		

6.4.2.12 Información de tiempo de puerta

El objeto Información de tiempo de puerta contiene la cantidad total de tiempo que la puerta permaneció en los estados comprometidos y recuperación comprometida. Este contador DEBE pararse cuando la puerta pase de los estados comprometidos o recuperación comprometida a los estados reservado o autorizado. Si la puerta vuelve más tarde al estado comprometido, este contador DEBE rearrancarse donde se paró la última vez, es decir, cuando salió de los estados comprometido o recuperación comprometida. El objeto Información de tiempo de puerta DEBE atenerse a la especificación siguiente:

Longitud = 8	S-Num =12	S-Type = 1
Tiempo comprometido		

Tiempo comprometido es un entero sin signo de 4 bytes que indica el número de segundos que esta puerta ha estado en el estado comprometido o en el estado recuperación comprometida.

NOTA – Se pretende que esto sea idéntico a docsQosServiceFlowTimeActive de la MIB de QoS [17].

6.4.2.13 Información de utilización de puerta

El objeto Información de utilización de puerta contiene un contador que indica el número de kilobytes transmitidos por esta puerta. El objeto Información de utilización de puerta DEBE atenerse a la especificación siguiente:

Longitud = 12	S-Num =13	S-Type = 1
Cuenta de octetos		

Cuenta de octetos es un entero sin signo de 4 bytes que indica el número de bytes (contados desde la HCS del encabezamiento de MAC DOCSIS hasta el final de la CRC) que han atravesado el flujo de servicio asociado a la puerta en unidades de 1024 bytes.

6.4.2.14 Error de IPCablecom

El objeto Error de IPCablecom contiene información sobre el tipo de error que se ha producido. El error se genera en respuesta a una instrucción de control por puerta y está contenido en mensajes Gate-Set-Err, Gate-Info-Err y Gate-Delete-Err. El objeto Error de IPCablecom DEBE atenerse a la especificación siguiente:

Longitud = 8	S-Num =14	S-Type = 1
Código de error	Subcódigo de error	

Código de error es un entero sin signo de 2 bytes que representa un error específico y DEBE ser uno de los siguientes:

1 = Recursos insuficientes

2 = ID de puerta desconocido

6 = Objeto requerido faltante

7 = Objeto no válido

8 = Límite de utilización basado en volumen rebasado

9 = Límite de utilización basado en tiempo rebasado

10 = Límite de clase de sesión rebasado

11 = Nombre de clase de servicio no definido

12 = Capacidad máxima incompatible

13 = ID de abonado no válido

14 = AMID no autorizado

15 = Número de clasificadores no soportado

127 = Otro, error no especificado

Subcódigo de error es un campo de 2 bytes que contiene un entero sin signo y se utiliza para proporcionar más información sobre el error. En el caso de los códigos de error 6 y 7, este campo de 16 bits DEBE contener el S-Num y el S-Type, de 8 bits cada uno, del objeto que falta o es erróneo. El orden de los valores S-Num y S-Type dentro del subcódigo de error DEBE ser el mismo que en el mensaje original. Cuando existan múltiples alternativas válidas para el S-Type del objeto que falta, esta porción del subcódigo de error DEBE fijarse en cero. Si el código de error es 15, el campo subcódigo de error DEBE contener el número de clasificadores que soporta cada puerta.

Los códigos de error 8, 9 y 10 se generan como resultado de una petición de política que no cumple los requisitos de la autorización de un servidor de política. Cuando el gestor de aplicación envía un mensaje Gate-Set con un límite basado en volumen o en tiempo al servidor de política, el servidor de política PUEDE rechazar la petición en base a las reglas de política instaladas en el servidor de política. Una de esas reglas de política puede estipular, por ejemplo, que si una petición de límite de volumen rebasa un valor máximo, el servidor de política debe rechazar la petición.

6.4.2.15 Estado de puerta

La información del objeto Estado de puerta refleja el estado en que se encuentra la puerta. El CMTS DEBE incluir el objeto Estado de puerta en cualesquiera mensajes no solicitados que envíe al servidor de política. El servidor de política puede utilizar esta información para informar del estado al gestor de aplicación o para poner en vigor reglas complejas que podrían requerir el conocimiento del estado de la puerta.

Lo normal es que el servidor de política esté al corriente de las transiciones de estado ya que normalmente da al CMTS el estímulo para que se produzcan esas transiciones, pero en algunos casos la puerta puede transitar localmente en el CMTS sin la participación del servidor de política. Si ocurre así, el CMTS DEBE informar de la transición de estado al servidor de política vía mensajes Gate-Report-State. Cuando emita mensajes Gate-Report-State, el PEP DEBE asegurarse de que se libera la bandera de mensaje solicitado en el mensaje COPS y de que el tipo de informe en el encabezamiento se fija en "contabilidad". El objeto Estado de puerta DEBE atenerse a la especificación siguiente.

Longitud = 8	S-Num =15	S-Type = 1
Estado	Motivo	

Estado es un campo de 2 bytes que contiene un entero sin signo que DEBE indicar uno de los estados siguientes:

1 = Reposo/Cerrado

2 = Autorizado

3 = Reservado

4 = Comprometido

5 = Recuperación comprometida

Motivo es un campo de 2 bytes que contiene un entero sin signo que DEBE indicar uno de los motivos siguientes para esta actualización:

1 = Cierre iniciado por el CMTS debido a reasignación de reserva

2 = Cierre iniciado por el CMTS debido a falta de respuestas de capa MAC DOCSIS

3 = Cierre iniciado por el CMTS debido a la expiración del temporizador T1

4 = Cierre iniciado por el CMTS debido a la expiración del temporizador T2

5 = Expiración del temporizador de inactividad debido a la inactividad del flujo de servicio (expiración del temporizador T3)

6 = Cierre iniciado por el CMTS debido a falta de mantenimiento de reserva

7 = Estado de puerta inalterado, pero límite de volumen alcanzado

8 = Cierre iniciado por el CMTS debido a la expiración del temporizador T4

9 = Estado de puerta inalterado, pero la expiración del temporizador T2 causó una reducción de la reserva

65535 = Otro

6.4.2.16 Información de versión

El objeto información de versión se utiliza para permitir a las aplicaciones multimedia adaptar sus interacciones con otros dispositivos, para que pueda conseguirse interoperabilidad entre productos que soportan versiones de protocolo diferentes. Tanto el número de versión principal como el número de versión secundaria son enteros sin signo de 2 bytes. El PDP y el PEP deben incluir este objeto como se especifica en 6.5.1.

Longitud = 8	S-Num = 16	S-Type = 1
Número de versión principal	Número de versión secundaria	

6.4.3 Mensajes de control por puerta

Hay dos perfiles independientes para los mensajes de control por puerta: uno para mensajes intercambiados entre el gestor de aplicación y el servidor de política, y otro para mensajes entre el servidor de política y el CMTS. Aunque son similares, estos dos perfiles muestran algunas pequeñas diferencias.

Las siguientes declaraciones describen los formatos de mensaje PCMM, para los objetos COPS y los PCMM. Estas declaraciones especifican el contenido de los mensajes, pero no implican una determinada ordenación de los objetos dentro de cada mensaje. En particular, cualquier ordenación de objetos PCMM DEBE aceptarse como válida (y puede generarse), y el orden de los objetos COPS DEBE ser el especificado en la RFC 2748. Obsérvese que como los objetos PCMM sólo existen dentro de objetos COPS, la distinción entre estos dos conjuntos es clara. Este modelo de contenencia asegura también que no haya problemas en cuanto al orden relativo de los objetos COPS y PCMM.

6.4.3.1 Perfil de interfaz entre gestor de aplicación y servidor de política

Los mensajes que efectúan el control por puerta entre el gestor de aplicación y el servidor de política están definidos y DEBEN ser formateados como sigue.

Se señala que los mensajes que van del gestor de aplicación al servidor de política DEBEN ser formateados como mensajes Decisión COPS y los mensajes que van del servidor de política al gestor de aplicación DEBEN ser formateados como mensajes Report-State de COPS.

<Client Open> = <COPS Common Header> <COPS PEPID> <ClientSI Info>
<ClientSI Info> = <COPS Client SI Header> <MM Version Info>
<Gate Control Command> = <COPS Common Header> <Client Handle> <Context>
<Decision Flags> <ClientSI Data>
<ClientSI Data> = <Gate-Set> | <Gate-Info> | <Gate-Delete>
<Gate Control Response> = <COPS Common Header> <Client Handle> <Report Type>
<ClientSI Object>
<ClientSI Object> = <Gate-Set-Ack> | <Gate-Set-Err> | <Gate-Info-Ack>
| <Gate-Info-Err> |<Gate-Delete-Ack> | <Gate-Delete-Err>
| <Gate-State-Report>
<Gate-Set> = <Decision Header> <TransactionID> <AMID> <SubscriberID> [<GateID>]
<GateSpec> <Traffic Profile> <Classifier> [<Classifier>]
[<Event Generation Info>]
[<Volume-Based Usage Limit>] [<Time-Based Usage Limit>] [<Opaque Data>]

<Gate-Set-Ack> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<GateID>
[<Opaque Data>]
<Gate-Set-Err> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<IPCablecom Error> [<Opaque Data>]
<Gate-Info> = <Decision Header> <TransactionID> <AMID> <SubscriberID><GateID>
<Gate-Info-Ack> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<GateID>
[<Event Generation Info>] <GateSpec> <GateState> <Classifier>
<Classifier> <Traffic Profile> <Gate Time Info>
<Gate Usage Info> [<Volume-Based Usage Limit>]
[<Time-Based Usage Limit>] [<Opaque Data>]
<Gate-Info-Err> = <ClientSI Header> <TransactionID> <AMID> <GateID>
<IPCablecomErr>
[<Opaque Data>]
<Gate-Delete> = <Decision Header> <TransactionID> <AMID> <SubscriberID> <GateID>
<Gate-Delete-Ack> = <ClientSI Header> <TransactionID> <AMID> <GateID> [<Opaque Data>]
<Gate-Delete-Err> = <ClientSI Header> <TransactionID> <AMID> <GateID>
<IPCablecom Error> [<Opaque Data>]
<Gate-Report-State> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<GateID> <GateState>
<Gate Time Info> <Gate Usage Info> [<Opaque Data>]

6.4.3.2 Perfil de interfaz entre servidor de política y CMTS

Los mensajes que efectúan el control por puerta entre el servidor de política y el CMTS están definidos y DEBEN ser formateados como sigue.

Se señala que los mensajes que van del servidor de política al CMTS DEBEN ser formateados como mensajes Decisión COPS y los mensajes que van del CMTS al servidor de política DEBEN ser formateados como mensajes Report-State COPS.

<Client Open> = <COPS Common Header> <COPS PEPID> <ClientSI Info>
<ClientSI Info> = <COPS Client SI Header> <MM Version Info>
<Gate Control Command> = <COPS Common Header> <Client Handle> <Context>
<Decision Flags> <ClientSI Data>
<ClientSI Data> = <Gate-Set> | <Gate-Info> | <Gate-Delete>
<Gate Control Response> = <COPS Common Header> <Client Handle> <Report Type>
<ClientSI Object>
<ClientSI Object> = <Gate-Set-Ack> | <Gate-Set-Err> | <Gate-Info-Ack>
| <Gate-Info-Err> |
<Gate-Delete-Ack> | <Gate-Delete-Err> | <Gate-Report-State>
<Gate-Set> = <Decision Header> <TransactionID> <AMID> <SubscriberID> [<GateID>]
<GateSpec> <Traffic Profile> <Classifier> [<Classifier>] [<Event Generation Info>]
[<Volume-Based Usage Limit>] [<Time-Based Usage Limit>] [<Opaque Data>]

<Gate-Set-Ack> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<GateID>
[<Opaque Data>]
<Gate-Set-Err> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<IPCablecom Error> [<Opaque Data>]
<Gate-Info> = <Decision Header> <TransactionID> <AMID> <SubscriberID> <GateID>
<Gate-Info-Ack> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<GateID>
[<Event Generation Info>] <Gate-Spec> <Classifier> <Classifier>
<Traffic Profile> <Gate Time Info> <Gate Usage Info> [<Volume-Based Usage Limit>]
[<Time-Based Usage Limit>] [<Opaque Data>] <Gate State>
<Gate-Info-Err> = <ClientSI Header> <TransactionID> <AMID> <GateID>
<IPCablecomErr>
[<Opaque Data>]
<Gate-Delete> = <Decision Header> <TransactionID> <AMID> <SubscriberID> <GateID>
<Gate-Delete-Ack> = <ClientSI Header> <TransactionID> <AMID> <GateID> [<Opaque Data>]
<Gate-Delete-Err> = <ClientSI Header> <TransactionID> <AMID> <GateID>
<IPCablecom Error> [<Opaque Data>]
<Gate-Report-State> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
<GateID> <GateState>
<Gate Time Info> <Gate Usage Info> [<Opaque Data>]

Hay tres mensajes de instrucción de control por puerta básicos: Gate-Set, Gate-Info y Gate-Delete. Estos mensajes están incorporados en los datos de decisión específicos del cliente de un mensaje Decisión COPS. Para los mensajes de instrucción de control por puerta, el objeto Contexto (C-Num = 2, C-Type = 1) del mensaje Decisión COPS DEBE tener el valor R-Type (bandera de tipo de petición) fijado en 0x08 (petición de configuración) y el M-Type fijado en cero. El campo código de instrucción del objeto Banderas de decisión obligatorio (C-Num = 6, C-Type = 1) DEBE estar fijado en 1 (instalar configuración). Otros valores DEBEN hacer que el CMTS genere un mensaje Report-State indicando fracaso. El subcampo banderas PUEDE tener cualquier valor y DEBE ser ignorado por el PEP. El campo tipo de instrucción de puerta del objeto ID de transacción distingue el tipo de instrucción que se emite.

Hay siete mensajes de respuesta de control por puerta: Gate-Set-Ack, Gate-Set-Err, Gate-Info-Ack, Gate-Info-Err, Gate-Delete-Ack, Gate-Delete-Err y Gate-Report-State. Los seis primeros mensajes de respuesta de control por puerta son respuestas solicitadas a mensajes de instrucción de control por puerta. El séptimo, Gate-Report-State, es una respuesta no solicitada al PS del CMTS para informar de un cambio de estado.

Estos mensajes están incorporados en el objeto Información específica del cliente de los mensajes Report-State de COPS. El objeto Tipo de informe (C-Num = 12, C-Type = 1) incluido en el mensaje Report-State de COPS para respuestas de control por puerta DEBE tener el campo tipo de informe fijado en 1 (éxito) o 2 (fracaso) dependiendo del resultado de la instrucción de control por puerta. Los mensajes Report-State en respuesta a una instrucción de control por puerta DEBEN tener el bit bandera de mensaje solicitado fijado en el encabezamiento COPS. El campo tipo de instrucción de puerta del objeto ID de transacción distingue el tipo de respuesta que se utiliza.

El CMTS genera el mensaje Gate-Report-State cuando hay una transición de estado en la puerta que no se debe a un mensaje Decisión o cuando se ha alcanzado algún límite de política. Para el mensaje Gate-State-Report, el campo tipo de informe DEBE fijarse en 3 (contabilidad) y la bandera de mensaje solicitado del encabezamiento común DEBE ser liberada.

Si un objeto recibido en un mensaje Control por puerta contiene un S-Num o S-Type que no es reconocido, dicho objeto DEBE ser ignorado. La presencia de un objeto como ése dentro de un mensaje Control por puerta NO DEBE ser tratada como un error ya que una vez que ese parámetro es eliminado, todos los objetos requeridos están presentes en el mensaje.

6.5 Funcionamiento del protocolo de control por puerta

6.5.1 Secuencia de inicialización

Cuando un PEP (servidor de política o CMTS) arranca, DEBE ponerse a la escucha de conexiones COPS entrantes en el puerto TCP número 3918 asignado por el IANA. Cualquier gestor de aplicación o servidor de política (PDP) que necesite contactar con un PEP DEBE iniciar una conexión con el PEP en ese puerto. Se prevé que múltiples gestores de aplicación establecerán conexiones COPS con múltiples servidores de política y que múltiples servidores de política establecerán conexiones COPS con múltiples CMTS. Cuando se establece la conexión TCP entre el PEP y el PDP, el PEP DEBE enviar información sobre él mismo al PDP en forma de mensaje Client-Open. Este mensaje DEBE incluir el objeto información de versión multimedia, que informará al PDP de la versión vigente del protocolo multimedia que utiliza el PEP.

Tras recibir de manera satisfactoria el mensaje Client-Open, el PDP DEBE enviar un mensaje Client-Accept si soporta la versión del protocolo especificada en el objeto información sobre la versión. Este mensaje DEBE incluir el objeto Keep-Alive-Timer, que indica al PEP el intervalo máximo entre mensajes Keep-Alive.

Si no soporta la versión del protocolo suministrada por el PEP, el PDP DEBE enviar mensajes Client-Close con un objeto de error COPS que especifique el código de error 4 (imposible procesar). Tras enviar el mensaje Client-Close, el PDP DEBE mantener la conexión TCP y la asociación de seguridad con el PEP para que éste pueda reintentar la inicialización COPS sin restablecer la conexión TCP y la asociación de seguridad. Tras recibir un mensaje Client-Close del PDP que incluya un objeto de error COPS que especifique el código de error 4, el PEP PUEDE reintentar la inicialización de la conexión COPS, enviando otro mensaje Client-Open con otro número de versión en el objeto información de versión. Este proceso puede continuar hasta que el PEP reciba un mensaje Client-Accept del PDP o bien se hayan agotado todas las versiones de protocolo disponibles. Una vez que el PEP ha intentado todas las versiones del protocolo que soporta, el PEP DEBE enviar un mensaje Client-Open con un número de versión principal igual a 0 y un número de versión secundaria también igual a 0, para indicar que el proceso de negociación de versión no ha concluido con éxito. El PDP DEBE entonces enviar un mensaje Client-Close para acusar que la negociación de protocolo ha fracasado. Al recibir el Client-Close, el PEP DEBE cerrar la conexión TCP. En este punto, el PDP PUEDE intentar periódicamente restablecer la conexión.

Los dispositivos conformes con esta especificación DEBEN utilizar la versión 1.0, es decir, un objeto de información de la versión con un número de versión principal igual a 1 y un número de versión secundaria igual a 0.

Tras recibir de manera satisfactoria el mensaje Client-Accept, el PEP DEBE enviar un mensaje Petición incluyendo los objetos Client-Handle y Contexto. El objeto Contexto (C-Num = 2, C-Type = 1) DEBE tener el valor R-Type (bandera de tipo de petición) fijado en 0x08 (petición de configuración) y el M-Type fijado en cero. El objeto Client-Handle contiene un valor que DEBE ser elegido por el PEP. El único requisito que se impone con respecto a este número es que un PEP NO DEBE utilizar el mismo valor para dos peticiones diferentes en una sola conexión TCP. Así se completa la secuencia de inicialización, que a continuación se describe visualmente.

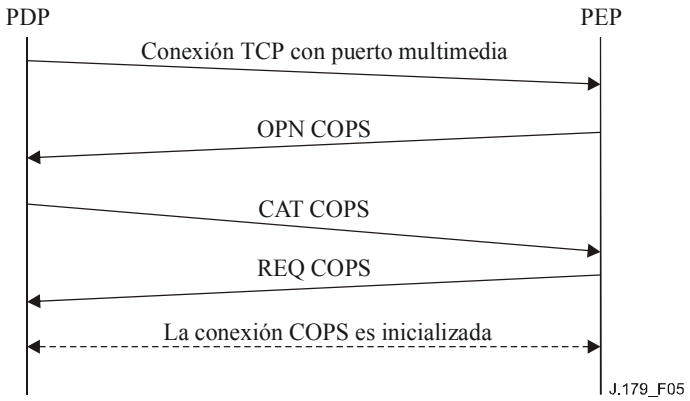


Figura 5/J.179 – Establecimiento de conexión COPS

Periódicamente, el PEP DEBE enviar un mensaje Keep-Alive (KA) COPS al PDP. Tras la recepción del mensaje KA COPS, el PDP DEBE devolver en eco un mensaje de KA COPS al PEP. En la figura 6 se muestra esta transacción, que está plenamente documentada en [7]. El PEP DEBE enviar un mensaje Keep-Alive al menos con la frecuencia especificada en el objeto Keep-Alive-Timer devuelto en el mensaje Client-Accept. El mensaje Keep-Alive DEBE ser enviado con Client-Type fijado en cero y la bandera de mensaje solicitado DEBE ser liberada.

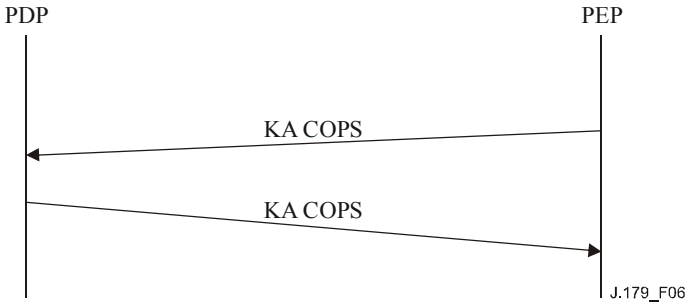


Figura 6/J.179 – Intercambio de mensajes Keep-Alive COPS

6.5.2 Secuencia de funcionamiento

El protocolo entre el PDP y el PEP se utiliza a efectos de política de control de recursos y asignación de recursos. El gestor de aplicación pide decisiones de tipo político del servidor de política y el servidor de política autoriza las peticiones y las instala en el CMTS para su puesta en vigor mediante la utilización de puertas.

Entre los mensajes que PUEDEN ser iniciados por el gestor de aplicación y el servidor de política figuran los de Gate-Set, Gate-Info y Gate-Delete. El CMTS PUEDE iniciar mensajes Gate-Report-State. Los procedimientos correspondientes a estos mensajes se describen en las cláusulas que siguen. Todos los mensajes del PDP al PEP DEBEN ser enviados utilizando objetos específicos del cliente dentro del objeto Decisión de un mensaje Decisión COPS. Las respuestas solicitadas del PEP DEBEN ser enviadas como un mensaje de Report-State con objetos específicos del cliente en el objeto ClientSI y la bandera de mensaje solicitado DEBE estar fijada. Los mensajes Gate-Report-State del CMTS DEBEN ser enviados como mensajes Report-State no solicitados vía objetos específicos del cliente en el objeto ClientSI.

Los mensajes Decisión y los mensajes Report-State DEBEN contener el mismo objeto Client-Handle proporcionado en la petición inicial enviada por el CMTS cuando se inició la conexión COPS.

Gate-Set inicializa y modifica todos los parámetros de política y tráfico de la puerta y establece la información de facturación. El mensaje Gate-Set se puede utilizar también para controlar y actualizar el estado de una puerta en el CMTS.

Gate-Info es un mecanismo mediante el cual el servidor de política puede consultar las fijaciones en que se encuentran todos los estados y parámetros de una puerta existente.

Gate-Delete hace posible que el servidor de política suprima una puerta específica y cualquier flujo de servicio asociado a la misma.

Gate-Report-State permite al CMTS informar al servidor de política de que la puerta ha transitado a un nuevo estado. Los mensajes Gate-Report-State DEBEN ser generados cuando la transición de estado se produce de manera asíncrona (es decir, no en respuesta a un mensaje Gate-Set). Los mensajes Gate-Report-State NO DEBEN ser generados cuando la transición de estado se produce de manera síncrona.

El PEP DEBE enviar periódicamente un mensaje Keep-Alive (KA) al PDP para facilitar la detección de fallos de conexión TCP. El PDP DEBE mantenerse al corriente de cuándo se reciben los KA. Si el PDP no ha recibido un KA del PEP en el intervalo de tiempo especificado en [7] o no ha recibido una indicación de error procedente de la conexión TCP, el PDP DEBE deshacer la conexión TCP y tratar de reestablecerla.

Las reglas que siguen se utilizan para encaminar mensajes Control por puerta a través del marco de los multimedia IPCablecom. Se señalan, en concreto, las disposiciones para el envío hacia adelante de mensajes Control por puerta (es decir, AM a PS a CMTS) y el retorno de los mismos (es decir, CMTS a PS a AM) a través de una compleja red por capas en el que múltiples ejemplares de cada elemento interactúan con elementos de la(s) capa(s) adyacente(s).

Como se describe en 6.4.3.1, cada petición de control por puerta iniciada por un AM (es decir, Gate-Set, Gate-Info y Gate-Delete) DEBE incluir (además de otros objetos obligatorios) tanto el objeto AMID como el objeto ID de abonado.

Tras la recepción de un mensaje Control por puerta procedente de un AM, un PS aplicará cualesquiera reglas de política provisionadas y determinará si se admite o rechaza la petición. Si la petición es admitida de manera satisfactoria, el PS DEBE encaminar el mensaje al CMTS apropiado en base al ID de abonado incluido en el mensaje. Este establecimiento de correspondencia entre ID de abonado y CMTS PUEDE llevarse a cabo dinámicamente efectuando una consulta a la infraestructura OSS o bien PUEDE reflejar la información de encaminamiento provisionada previamente relativa a la(s) gama(s) de subredes IP que están asociadas a cada CMTS.

Si una petición de control por puerta es rechazada por el PS, DEBE devolverse una respuesta de error al AM emisor por la conexión por la que se recibió la petición original. Si se detecta un fallo en esta conexión entre el momento en que se recibe una petición y el momento en que se entrega la respuesta, el PS DEBE desechar la respuesta.

Tras la recepción de un mensaje Control por puerta procedente de un PS, un CMTS efectuará la operación pedida. Si esta operación tiene éxito con la intervención de una operación Gate-Set o Gate-Info, el CMTS DEBE registrar el AMID y el ID de abonado incluidos en el mensaje y mantener una asociación con la puerta referenciada. Esta información debe ser utilizada como garantía de que sólo al AM que creó originalmente la puerta se le permite consultarla o modificarla. Cualesquiera mensajes Control por puerta que hagan referencia a una puerta pero que contengan un AMID distinto del asociado a la misma DEBEN ser rechazados por el CMTS con el error "AMID no autorizado". Finalmente, los mensajes Gate-Report-State DEBEN ser entregados al elemento PS, identificado mediante su dirección IP, que originalmente creó la puerta. Si no se dispone de una conexión con ese PS, el CMST DEBE suprimir los mensajes Gate-Report-State.

Cuando un PS recibe un mensaje Gate-Report-State procedente de un CMTS, el PS DEBE reenviar dicho mensaje al AM asociado al AMID incluido en el mismo. Para mantener un nivel de abstracción entre capas no adyacentes y ocultar información relativa a la topología de red procedente de la capa AM, el PS NO DEBE incluir información alguna que identifique directamente un CMTS particular a la capa AM.

6.5.3 Procedimientos de validación de capacidades máximas de recursos

Se denomina capacidad máxima al conjunto de características de los flujos de servicio de datos importantes a efectos de la prestación de un servicio con calidad mejorada. Una puerta de multimedia IPCablecom contiene hasta tres capacidades máximas: uno que indica los recursos autorizados, otro que indica los recursos reservados y un tercero que indica los recursos comprometidos para el flujo de servicio correspondiente a la puerta. En cualquier momento, la capacidad máxima comprometida DEBE encajar dentro de la capacidad máxima reservada que a su vez DEBE encajar dentro de la capacidad máxima autorizada.

Cuando un CMTS recibe un mensaje Gate-Set, DEBE validar la relación entre las capacidades máximas comprometida, reservada y autorizada de la puerta. Si la relación entre las capacidades máximas no es válida, el CMTS DEBE replicar con un mensaje Gate-Set-Err con código de error IPCablecom de "capacidad máxima incompatible".

El CMTS DEBE además efectuar el control de admisión cuando quiera que se pida un cambio (incluida una adición) de la capacidad máxima reservada. El control de admisión es el proceso de asignación de recursos para el flujo correspondiente a la puerta. Si los recursos no pueden ser asignados, el CMTS DEBE replicar con un mensaje Gate-Set-Err con código de error IPCablecom de "recursos insuficientes".

6.5.3.1 FlowSpec

En el cuadro 2, la segunda columna indica la operación que debería efectuarse para comparar un parámetro de la capacidad máxima A con un parámetro correspondiente de la capacidad máxima B. En otras palabras, la capacidad máxima A encaja dentro de la capacidad máxima B si cada parámetro de A cumple los criterios especificados en el cuadro.

Cuadro 2/J.179 – Reglas de comparación de capacidades máximas

Parámetro	A {OP} B
Velocidad de colector testigo [r]	≤
Tamaño de colector testigo [b]	≤
Velocidad de datos de cresta [p]	≤
Unidad mínima sujeta a aplicación de política [m]	≥
Tamaño de paquete máximo [M]	≤
Velocidad [R]	≤
Término suelto [S]	≥

6.5.3.2 Nombre de clase de servicio DOCSIS

En el caso de los perfiles de tráfico en forma de nombre de clase de servicio, la cadena nombre de clase de servicio DEBE concordar exactamente con el nombre de clase de servicio preexistente en el CMTS. No es necesario comparar las capacidades máximas ya que las tres capacidades máximas deben compartir los mismos parámetros.

6.5.3.3 Parámetros de flujo de servicio DOCSIS

6.5.3.3.1 Codificaciones en sentido ascendente

En el cuadro 3, la segunda columna indica la operación que debería efectuarse para comparar un parámetro de la capacidad máxima A con un parámetro correspondiente de la capacidad máxima B. En otras palabras, la capacidad máxima A encaja dentro la B si cada parámetro de A cumple los criterios especificados en el cuadro.

Cuadro 3/J.179 – Comparación entre capacidades máximas en sentido ascendente

Parámetro	A {OP} B
Prioridad de tráfico (BE y NRTPS)	≤
Política de petición/transmisión (todo)	= =
Velocidad de tráfico sostenida máxima (BE, NRTPS, RTPS)	≤
Ráfaga de tráfico máxima (BE, NRTPS, RTPS)	≤
Velocidad de tráfico reservada mínima (BE, NRTPS, RTPS)	≤
Tamaño asumido de paquete de velocidad de tráfico reservada mínima (BE, NRTPS, RTPS)	≥
Intervalo de interrogación secuencial nominal (NRTPS, RTPS, UGS/AD)	Véase la descripción más adelante
Fluctuación de interrogación secuencial tolerada (RTPS, UGS/AD)	≥
Tamaño de concesión no solicitada (UGS y UGS/AD)	≤
Concesiones por intervalo (UGS y UGS/AD)	≤
Intervalo de concesión nominal (UGS y UGS/AD)	Véase la descripción más adelante
Fluctuación de concesión tolerada (UGS y UGS/AD)	≥

Intervalos – A es un subconjunto de B si el parámetro en A es un múltiplo entero del mismo parámetro en B.

6.5.3.3.2 Codificaciones en sentido descendente

En el cuadro 4, la segunda columna indica la operación que debería efectuarse para comparar un parámetro de la capacidad máxima A con un parámetro correspondiente de la capacidad máxima B. En otras palabras, la capacidad máxima A encaja dentro de la B si cada parámetro de A cumple los criterios especificados en el cuadro.

Cuadro 4/J.179 – Comparación entre capacidades máximas en sentido descendente

Parámetro	A {OP} B
Prioridad de tráfico	≤
Velocidad de tráfico sostenida máxima	≤
Ráfaga de tráfico máxima	≤
Velocidad de tráfico reservada mínima	≤
Tamaño asumido de paquete de velocidad de tráfico reservada mínima	≥
Latencia en sentido descendente máxima	≥

6.5.4 Procedimientos de autorización de recursos a través de una puerta

El mensaje Gate-Set PUEDE ser enviado por el PDP al PEP para inicializar o modificar los parámetros operativos de una puerta. La figura 7 que sigue da un ejemplo de señalización de Gate-Set.

NOTA – El mensaje "Comenzar sesión" puede ser utilizado, por ejemplo, para indicar al cliente que los recursos han sido autorizados.

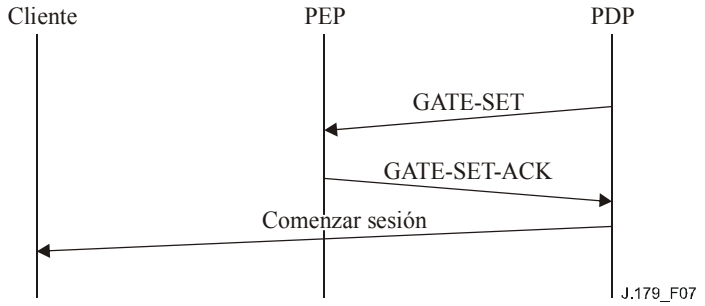


Figura 7/J.179 – Ejemplo de señalización de Gate-Set

Si en el mensaje Gate-Set está presente un objeto ID de puerta, la petición es de modificación de una puerta existente. Si en el mensaje Gate-Set está ausente el objeto ID de puerta, se trata de una petición de atribución de una nueva puerta. El mensaje Gate-Set DEBE contener exactamente un objeto GateSpec, describiendo una puerta en sentido ascendente o en sentido descendente.

El mensaje Gate-Set contiene también el ID de abonado. El CMTS DEBE utilizar esta dirección IP (es decir, el ID de abonado) para determinar el CM que da servicio y DEBE utilizar la dirección MAC del CM para la mensajería de capa MAC subsiguiente.

El PEP DEBE responder a un mensaje Gate-Set con un Gate-Set-Ack, indicando éxito, o un Gate-Set-Err, indicando fracaso. El ID de transacción de la respuesta DEBE concordar con el ID de transacción de la petición. Los errores en la atribución o autorización de puertas DEBEN ser notificados mediante una respuesta Gate-Set-Err. Véase 6.4.2.14.

En el escenario 1, el servidor de política PUEDE especificar las capacidades máximas autorizada, reservada y comprometida por medio de un perfil de tráfico enviado en el mensaje Gate-Set. PUEDE indicar al CMTS, simultáneamente, que autorice, reserve y comprometa recursos.

Tras la recepción de un Gate-Set, el CMTS DEBE satisfacer primero los requisitos especificados en 6.5.3 y efectuar a continuación las acciones pedidas. Una vez completadas de manera satisfactoria las acciones pedidas en el Gate-Set (por ejemplo, la creación de un flujo de servicio DOCSIS) el CMTS DEBE responder con un Gate-Set-Ack. El CMTS NO DEBE responder con un Gate-Set-Ack sino hasta que haya completado un número suficiente de pasos como para asegurar que no fallarán cualesquiera peticiones subsiguientes de admisión o compromiso de la puerta debido a una falta de recursos.

Un CMTS PUEDE efectuar una autorización compleja en base no solamente a la QoS pedida y la FlowSpec autorizada de la puerta, sino también en base al ID de clase de sesión especificado en el Gate-Spec. El CMTS PUEDE haber provisionado políticas que definen la cantidad de recursos atribuidos exclusivamente a la clase de sesión particular, así como reglas de 'toma en préstamo' y de 'apropiación con prioridad' aplicables a la utilización de los recursos. La especificidad de estos tipos de políticas y reglas en el CMTS queda fuera del alcance de la presente Recomendación.

Tras la recepción de un Gate-Set-Ack o Gate-Set-Err procedente de un CMTS, el servidor de política DEBE reenviar el mensaje al gestor de aplicación correspondiente al AMID del Gate-Set-Ack. El servidor de política NO DEBE transmitir un Gate-Set-Ack a un gestor de

aplicación antes de recibir un Gate-Set-Ack del CMTS. Si el gestor de aplicación pide un servicio que, sin embargo, no pasa las verificaciones de política del servidor de política, el servidor de política NO DEBE enviar el Gate-Set al CMTS y DEBE enviar un Gate-Set-Err al gestor de aplicación con el conjunto de errores apropiado.

6.5.5 Procedimientos de consulta de una puerta

Cuando un servidor de política o gestor de aplicación desea consultar las fijaciones que tienen los parámetros de una puerta, envía al CMTS un mensaje Gate-Info. El CMTS DEBE responder a un mensaje Gate-Info bien con un Gate-Info-Ack, indicando éxito, o bien con un Gate-Info-Err, indicando fracaso. Un Gate-Info-Ack DEBE contener información sobre la puerta asociada al ID de puerta del mensaje Gate-Info. Si la puerta que se consulta tiene un límite de utilización basado en volumen y/o basado en tiempo existente, el CMTS DEBE incluir estos objetos en el Gate-Info-Ack. Un PS o AM puede utilizar esa información para recuperar información del estado de puerta del CMTS a efectos de control o recuperación tras error o por otros motivos. El ID de transacción de la respuesta DEBE concordar con el ID de transacción de la petición.

Los errores en las consultas de las puertas DEBEN ser notificados mediante una respuesta Gate-Inf-Err. El objeto Error de un mensaje Gate-Inf-Err DEBE contener uno de los códigos de error siguientes:

2 = ID de puerta desconocido

127 = Otro, error no especificado

6.5.6 Procedimientos de modificación de una puerta

Para modificar el perfil de tráfico asociado a una puerta existente, un gestor de aplicación PUEDE enviar un mensaje Gate-Set con el ID de puerta de la puerta que se ha de modificar y el nuevo perfil de tráfico. Si el Gate-Set no pasa las verificaciones del servidor de política, el servidor de política DEBE enviar un Gate-Set-Err al gestor de aplicación y NO DEBE enviar un Gate-Set al CMTS. Sin embargo, si el Gate-Set pasa las verificaciones de política del servidor de política, el servidor de política DEBE enviar el Gate-Set al CMTS. El ID de transacción del Gate-Set del servidor de política DEBE concordar con el ID de transacción del Gate-Set del gestor de aplicación.

Tras la recepción de un Gate-Set, el CMTS debe satisfacer primero los requisitos especificados en 6.5.3 y efectuar a continuación las acciones pedidas. Al igual que en la creación de una puerta nueva, tras la compleción satisfactorias de las acciones pedidas en el Gate-Set (por ejemplo, modificación de un flujo de servicio DOCSIS) el CMTS DEBE responder con un Gate-Set-Ack. El CMTS NO DEBE responder con un Gate-Set-Ack sino hasta que haya completado un número suficiente de pasos como para asegurar que no fallarán cualesquiera peticiones subsiguientes de admisión o compromiso de la puerta debido a una falta de recursos.

Tras la recepción de un Gate-Set-Ack o Gate-Set-Err procedente del CMTS, el servidor de política DEBE reenviar la respuesta al gestor de aplicación.

Para modificar los límites de utilización asociados a una puerta existente, un gestor de aplicación PUEDE enviar un mensaje Gate-Set con el ID de puerta de la puerta que se ha de modificar. Si el perfil de tráfico del Gate-Set es diferente del perfil de tráfico asociado a la sazón a la puerta, se aplican las reglas previas. En cualquier caso, si está presente el límite de utilización basado en tiempo o el límite de utilización basado en volumen del flujo, los límites existentes asociados a este/estos parámetro(s) DEBEN ser sustituidos por el(los) nuevo(s) parámetro(s) y cualesquiera contadores o temporizadores existentes DEBEN ser reiniciados. Sin embargo, la ausencia de estos parámetros en un mensaje Gate-Set indica que incluso si el perfil de tráfico de la puerta está siendo modificado, el límite o los límites de utilización basados en tiempo o en volumen de la puerta siguen siendo aplicables. Si estos parámetros no están presentes en un mensaje Gate-Set, los límites existentes DEBEN ser mantenidos y sus contadores/temporizadores asociados DEBEN continuar a partir de los valores que tienen en ese momento sin reiniciación.

6.5.7 Procedimientos de soporte de los límites de utilización

El gestor de aplicación, el servidor de política y el CMTS desempeñan, los tres, un cometido en la puesta en vigor de los límites de utilización. Hay diferencias un tanto sutiles entre límites basados en tiempo y límites basados en volumen por lo que cada uno de ellos se describe por separado.

6.5.7.1 Procedimientos al alcanzar un límite de utilización basado en volumen

Puesto que el CMTS es el único dispositivo de multimedia IPCablecom fiduciario del trayecto de paquetes, sólo él puede seguir con precisión la utilización de puertas individuales. Por ello, el CMTS DEBE proceder al seguimiento de la utilización de todas las puertas con independencia de si tienen o no asociado un límite de utilización basado en volumen. El CMTS DEBE informar del volumen de datos transferidos vía una puerta en todos los mensajes Gate-Info-Ack y en todos los mensajes Gate-Report-State.

Si la puerta tiene asociado un límite de utilización basado en volumen cuando el volumen de datos que ha atravesado la puerta iguale el límite de utilización basado en volumen, el CMTS DEBE enviar un mensaje Gate-Report-State con el bit de mensaje solicitado fijado en 0. El mensaje Gate-Report-State DEBE incluir un objeto Estado de puerta con el motivo fijado en 7 (estado de puerta inalterado, pero límite de volumen alcanzado). Tras la recepción de un mensaje Gate-State-Report, el comportamiento del PDP depende de su función; un servidor de política DEBE reenviar el mensaje Gate-Report-State al gestor de aplicación o bien manipular él mismo el informe. El servidor de política DEBERÍA manipular el informe únicamente si hizo que el informe se generase modificando el conjunto de puertas original. En otras palabras, las acciones del servidor de política deberían ser transparentes para el gestor de aplicación: el gestor de aplicación DEBE manipular los informes recibidos. Un PDP manipula un mensaje Gate-Report-State con el motivo fijado en 7, efectuando una de las acciones siguientes:

- Enviar un mensaje Gate-Set con un objeto Límite de utilización basado en volumen nuevo, que el CMTS debe utilizar para "reiniciar" la contabilidad correspondiente a esta puerta.
- Enviar un mensaje Gate-Set con un límite de utilización basado en volumen fijado en 0 para inhabilitar la característica y permitir que el CMTS continúe dando servicio a la sesión.
- Cerrar la puerta emitiendo una instrucción Gate-Delete.

6.5.7.2 Procedimientos al alcanzar un límite de utilización basado en tiempo

Si bien el mantenimiento de los procedimientos límite de utilización basado en volumen y límite de utilización basado en tiempo tan similares como sea posible es un objetivo de diseño deseable, el número de interrupciones del CMTS requerido para soportar la puesta en vigor de límites de utilización basados en tiempo por el CMTS hace que dicho objetivo resulte imposible. Así pues, el gestor de aplicación DEBE aplicar el límite de utilización basado en tiempo de la puerta. Tras la recepción del Gate-Set-Ack para una puerta con un límite de utilización basado en tiempo, el AM DEBE arrancar un temporizador de aplicación. Cuando el temporizador de aplicación alcance el límite de utilización basado en tiempo, el gestor de aplicación DEBE responder efectuando una de las acciones siguientes:

- Enviar un mensaje Gate-Set con un objeto Límite de utilización basado en tiempo nuevo y reiniciar su temporizador de aplicación.
- Enviar un mensaje Gate-Set con un límite de utilización basado en tiempo fijado en 0 para inhabilitar la característica.
- Cerrar la puerta emitiendo una instrucción Gate-Delete.

NOTA – En cierto modo tiene más sentido que el gestor de aplicación aplique límites de utilización, ya que el límite de utilización basado en tiempo y el límite de utilización basado en volumen no hacen sino reflejar el servicio que se está ofreciendo y son de la responsabilidad del dominio de control de servicio. Lo que realmente es inusual es el procedimiento límite de utilización basado en volumen, pero el CMTS es el único dispositivo que puede aplicar con exactitud este límite.

6.5.7.3 Recuperación de recursos y recuperación tras error

Aunque es preciso que el gestor de aplicación efectúe una de entre varias acciones cuando se alcance el límite de utilización de una puerta, siempre hay la posibilidad de que el gestor de aplicación no responda apropiadamente. En este caso, el RKS seguirá registrando la utilización de la puerta con lo que esta actividad seguirá siendo facturable, pero en algunos casos quizá convenga recuperar los recursos que están siendo utilizados 'ilegalmente' por el gestor de aplicación. Un servidor de política PUEDE basarse en los mensajes entre AM y CMTS en los que actúa como apoderado para determinar con precisión si el límite de utilización basado en volumen o basado en tiempo de una puerta ha sido rebasado. La utilización de la técnica de 'determinación' minuciosa implica el que el servidor de política sea un servidor basado en estados, pero un servidor de política que no se base en estados puede aún recuperar recursos aplicando una segunda técnica que se describe a continuación.

Un servidor de política PUEDE, de manera alternativa, consultar ocasionalmente el CMTS con un mensaje Gate-Info. La repuesta contendrá cualquier límite de utilización basado en volumen e información de utilización de la puerta (o límite de utilización basado en tiempo e información de tiempo de puerta). El servidor de política puede comparar a continuación esos valores. Con independencia de cómo se entera un servidor de política de que una puerta ha rebasado un límite, el servidor PUEDE emitir un Gate-Delete para puertas con límites rebasados. Tras la recepción del Gate-Set-Ack (o Gate-Set-Err) del CMTS, el servidor de política DEBE enviar el mensaje al gestor de aplicación.

De manera similar, aunque no se requiera para recuperar recursos de puertas con límites rebasados, un CMTS PUEDE efectuar por sí mismo las mismas comparaciones y PUEDE suprimir puertas con límites rebasados. En 6.5.8 se describen requisitos adicionales para este escenario.

6.5.7.4 Seguimiento de los límites de utilización basados en tiempo y basados en volumen

Las puertas de multimedia IPCablecom pueden comprometerse y descomprometerse múltiples veces (soportando así, por ejemplo, una función 'pausa' en un juego o en medios de flujo continuo). Puesto que un abonado no puede transmitir/recibir datos mientras la puerta no esté en el estado comprometido, estos periodos no deberían contabilizarse en su contra. Para los límites de utilización basados en volumen este requisito no tiene efecto: no hay paquetes que pudieran ser contabilizados en exceso ya que no se pueden enviar paquetes si una puerta no está comprometida. Sin embargo, para los límites de utilización basados en tiempo el CMTS DEBE parar su temporizador de información de tiempo de puerta cuando la puerta no esté en el estado comprometido o en el estado recuperación comprometida. Si la puerta es comprometida de nuevo sin cambios en el límite basado en tiempo, el temporizador de información de tiempo de puerta DEBE ser rearrancado desde el cómputo en que se paró. Si se introducen cambios en el límite basado en tiempo, el temporizador de información de tiempo de puerta DEBE ser repuesto a 0 y rearrancado cuando la puerta sea comprometida de nuevo.

NOTA – Es preciso que el gestor de aplicación mantenga un temporizador independiente del temporizador del CMTS para aplicar el límite de utilización basado en tiempo. Este temporizador es independiente del propio CMTS por lo que los retardos en la mensajería podrían provocar discrepancias entre estos dos temporizadores. En el caso de aplicaciones que precisen un alto grado de exactitud en el tiempo, el AM PUEDE consultar el CMTS a propósito de su objeto Información de tiempo de puerta después de que haga pasar una puerta al estado comprometido o la saque del mismo.

6.5.8 Procedimientos de supresión de una puerta

Normalmente, cuando termina una sesión de multimedia, el gestor de aplicación le dice al servidor de política que la sesión ha terminado y el servidor de política a su vez le dice al CMTS que elimine la puerta mediante un mensaje Gate-Delete. El CMTS DEBE responder a un mensaje Gate-Delete con un Gate-Delete-Ack, que indica éxito, o bien un Gate-Delete-Err, que indica fracaso. El ID de transacción de la respuesta DEBE concordar con el ID de transacción de la petición.

Los errores en la supresión de puertas DEBEN ser notificados mediante una respuesta Gate-Delete-Err. El objeto Error DEBE contener uno de los códigos de error siguientes:

2 = ID de puerta desconocido

127 = Otro, error no especificado

En el CMTS, si expira el temporizador T1, T2 (sólo cuando se halle en el estado reservado) o T4, la puerta DEBE ser suprimida. Cuando un CMTS suprime una puerta sin que se lo haya solicitado el servidor de política, el CMTS DEBE enviar un mensaje Gate-Report-State (con el bit de mensaje solicitado fijado en 0) al servidor de política indicando que la puerta ha sido suprimida. Si el temporizador T2 expira mientras se halla en el estado reservado, el CMTS DEBE suprimir el flujo DOCSIS utilizando mecanismos DOCSIS (es decir, un mensaje DSD) y enviar un mensaje Gate-Report-State (con el bit de mensaje solicitado fijado en 0) al PS informando de esta transición de estado. Obsérvese que si el temporizador T2 expira mientras se encuentra en el estado comprometido o recuperación comprometida, el CMTS debe enviar un DSC, definido en DOCSIS, para liberar los recursos reservados que sobran de entre los recursos activos, emitir un mensaje Gate-Report-State al PS informándole de la reducción de los recursos reservados, y permanecer en el mismo estado. Tras la recepción de un mensaje Gate-Report-State, el servidor de política DEBE reenviarlo al gestor de aplicación.

6.5.9 Procedimiento de comprometimiento de una puerta

En el escenario 1, el servidor de política se encarga de comprometer una puerta mediante un perfil de tráfico que contiene una capacidad máxima comprometida. El CMTS compromete la puerta y activa el flujo de servicio DOCSIS utilizando los parámetros que le ha transferido el servidor de política.

6.5.10 Secuencia de terminación

Cuando el PEP clausura su conexión TCP con el PDP, PUEDE enviar primero un mensaje Delete-Request-State (DRQ) (incluyendo el objeto Asa utilizado en el mensaje Petición inicial). Si el PEP decide enviar el mensaje DRQ, el PEP DEBE utilizar el código de motivo 4 de COPS (eliminar). El PEP PUEDE enviar a continuación un mensaje Client-Close. El PDP DEBE, en respuesta, suprimir automáticamente cualquier estado asociado al PEP cuando termina la conexión TCP. Cuando el PDP se vaya a cerrar, DEBERÍA enviar un mensaje Client-Close de COPS al PEP. En el mensaje Client-Close de COPS el PDP NO DEBERÍA enviar el objeto de dirección de redireccionamiento PDP (PDPRedirAddr). Si el PEP recibe un mensaje Client-Close de COPS procedente del PDP con un objeto PDPRedirAddr, el PEP DEBE ignorar el PDPRedirAddr mientras procesa el mensaje Client-Close de COPS.

El PS y el CMTS NO DEBEN eliminar puertas como consecuencia de una conexión COPS fallida.

6.5.11 Procedimientos de sincronización de estados

Cuando un servidor de política desea sincronizar su estado con el de un CMTS PUEDE enviar un mensaje Synchronize-State-Request (SSQ). Este SSQ PUEDE contener el objeto Client-Handle del servidor de política. Si el Client-Handle facultativo está presente, sólo se sincroniza el estado asociado a este asa. Si el CMTS no reconoce el asa pedida, DEBE enviar inmediatamente un mensaje Delete-Request-State (DRQ) al servidor de política para el asa que fue especificada en el mensaje SSQ. Si en el mensaje SSQ no se especifica ningún objeto Client-Handle, todos los estados activos del cliente con el Client-Type de multimedia IPCablecom DEBEN ser sincronizados con el PDP.

El CMTS lleva a cabo la sincronización de estados emitiendo mensajes Petición para puertas asociadas al Client-Handle (si se incluye en el SSQ) o para todas las puertas conocidas (si no se proporciona Client-Handle). Una vez completada la sincronización, el CMTS DEBE enviar un

mensaje Synchronize-State-Complete (SSC) al PDP. Si el SSQ iniciador contiene un Client-Handle, el SSC DEBE contener también el Client-Handle.

7 Descripción de la interfaz de mensajería de eventos

7.1 Introducción

Al igual que en la arquitectura IPCablecom-T, los mensajes de evento por multimedia IPCablecom proporcionan información detallada sobre la utilización del recurso QoS, tal como la relativa a su reserva, activación y liberación. Un aspecto nuevo del marco multimedia IPCablecom es la necesidad de proceder al seguimiento del estado de las decisiones de tipo político (peticiones, actualizaciones, supresiones). Además, puesto que la utilización de recursos de red queda fuera del alcance de los perfiles en IPCablecom-T (utilización constante a lo largo del tiempo), es preciso proporcionar información sobre la utilización basada en volumen y basada en tiempo.

Los mensajes de evento (EM, *event message*), definidos en este marco, son generados por elementos de red y almacenados en el servidor de mantenimiento de registros (RKS). A continuación el RKS u otro sistema de fondo de oficina (*back-office system*) correlaciona estos EM para registrar un único ejemplar de un servicio. Los registros se pueden utilizar para obtener información sobre facturación del servicio, esquemas de utilización de recursos de red, planificación de capacidades, etc. No obstante, los EM no tienen por objeto la supervisión técnica de averías.

Actualmente, sólo el CMTS y el servidor de política, que forman parte de la red del operador de cable y se consideran entidades fiduciarias, generan mensajes de evento dentro del marco multimedia. Otros elementos de la red, tales como los distintos tipos de clientes, no se consideran fiduciarios. El gestor de aplicación es un elemento que puede formar parte o no de la red de cable del operador y por tanto no proporciona directamente mensajes de evento al RKS. El AM puede, no obstante, dar información complementaria como parte de los campos de datos opacos al PS, que a continuación los incluiría en los EM que generase.

Los mensajes de evento IPCablecom para multimedia representan una simplificación y modificación de los mensajes de evento de IPCablecom-T. Los eventos específicos de la telefonía, tales como Call_Answer y Call_Disconnect, se consideran facultativos ya que son mensajes de evento específicos del servicio de telefonía (por ejemplo, ejemplar de servicio y). El objetivo es influir lo más posible de manera positiva en las implementaciones de EM existentes al tiempo que se proporcionan mecanismos de abstracción suficientes para soportar servicios multimedia de carácter general.

De manera específica, de los catorce tipos de mensajes EM definidos en soporte de los servicios de voz IPCablecom-T se requerirán cuatro en multimedia IPCablecom, a saber: QoS_Reserve, QoS_Commit, QoS_Release y Time_Change. Se definen tres tipos de mensajes EM nuevos relativos a decisiones de tipo político: Policy_Request, Policy_Delete y Policy_Update. El cuadro 5 que sigue da una visión general resumida de los tipos de mensajes EM de multimedia IPCablecom.

Cuadro 5/J.179 – Tipos de mensajes EM de multimedia IPCablecom

ID de mensaje de evento	Mensaje de evento	Elemento de origen	Descripción
7	QoS_Reserve	CMTS	Indica el momento en que el CMTS reserva anchura de banda en la red de acceso IPCablecom. El CMTS debe generar también este evento si cambia la anchura de banda reservada.
8	QoS_Release	CMTS	Indica el momento en que el CMTS libera su compromiso de anchura de banda en la red de acceso IPCablecom.
17	Time_Change	PS, CMTS	Recoge un ejemplar de cambio de hora. Siempre que el reloj (IPCablecom) de un elemento de red fiduciario (PS y CMTS) se cambia en más de 200 milisegundos, el elemento de red debe generar un mensaje Time_Change.
19	QoS_Commit	CMTS	Indica el momento en que el CMTS compromete anchura de banda en la red de acceso IPCablecom. El CMTS debe generar también este evento si cambia la anchura de banda comprometida.
31	Policy_Request	PS	Indica el momento en que el servidor de política recibe una petición de política nueva procedente del AM.
32	Policy_Delete	PS	Indica el momento en que el servidor de política suprime una política.
33	Policy_Update	PS	Indica el momento en que el servidor de política recibe una petición de actualización de una política.

Aunque los mensajes de evento de multimedia IPCablecom se basan en IPCablecom-T, los eventos específicos de la telefonía son facultativos para multimedia IPCablecom y su relación figura a continuación. Para más detalles sobre estos eventos y los atributos asociados, véase la Rec. UIT-T J.164 [10].

Cuadro 6/J.179 – Tipos de mensajes EM de telefonía IPCablecom-T

ID de mensaje de evento	Mensaje de evento	Descripción
1	Signaling_Start	Indica el momento en que comienza la señalización.
2	Signaling_Stop	Indica el momento en que termina la señalización.
3	Database_Query	Indica el momento en que un periférico inteligente (por ejemplo, base de datos de número 800, base de datos de portabilidad de número local) efectúa una transacción de petición/respuesta directa o mediante consulta de una base de datos.
6	Service_Instance	Indica el momento en que el CMS proporciona un ejemplar de un servicio de control de llamada o una prestación relativa a una llamada (por ejemplo, de retención de llamada o de llamada en espera).
9	Service_Activation	Indica el momento en que el CMS registra una tentativa de activación de un servicio (por ejemplo, de reenvío de llamada o de llamada en espera).

Cuadro 6/J.179 – Tipos de mensajes EM de telefonía IPCablecom-T

ID de mensaje de evento	Mensaje de evento	Descripción
10	Service_Deactivation	Indica el momento en que el CMS registra una tentativa de desactivación de un servicio (por ejemplo, de reenvío de llamada o de llamada en espera).
13	Interconnect_Start	Indica el momento en que se produce el comienzo de la señalización de la interconexión de red.
14	Interconnect_Stop	Indica la terminación de la anchura de banda entre la red IPCablecom y la RTPC.
15	Call_Answer	Indica que la conexión del medio está abierta porque se ha producido una respuesta.
16	Call_Disconnect	Indica el momento en que se cierra la conexión del medio porque la parte llamante ha terminado la llamada colgando o porque la parte destino ha colgado y el temporizador de continuación de la llamada de la parte llamada ha expirado.
20	Media_Alive	Indica que el servicio está activo debido a la existencia continuada de una conexión portadora. Este mensaje puede ser generado por cualquier elemento de red IPCablecom fiduciario (CMS, MGC y CMTS) según crea conveniente el vendedor.

7.2 Requisitos del servidor de mantenimiento de registros

El servidor de mantenimiento de registros (RKS) es una función de elemento de red fiduciario. El RKS se presenta por lo general en esta Recomendación como un elemento autónomo distinto, pero la presente Recomendación no excluye que alguna otra aplicación realice las funciones de un RKS, siempre que la aplicación cumpla los requisitos que aquí se indican.

El RKS es la capa de mediación entre la red de multimedia IPCablecom y las aplicaciones de fondo de oficina. Se prevé que el RKS procese los datos recibidos de la red de multimedia IPCablecom y los presente a las aplicaciones de fondo de oficina en el formato y dentro de los límites de tiempo que considere necesarios el operador de cable. El RKS actúa por tanto como un punto de demarcación entre la red IPCablecom y las aplicaciones de fondo de oficina.

El RKS DEBE ser capaz de recibir y procesar mensajes de evento formateados de acuerdo con esta Recomendación.

Los mensajes RADIUS dentro de los cuales se encapsulan los mensajes de evento son transportados por el UDP, lo cual no garantiza una entrega fiable de mensajes; de ahí el carácter de petición/respuesta del protocolo que aquí se define. Cuando un RKS recibe y registra de manera satisfactoria todos los mensajes de evento IPCablecom contenidos en un mensaje Petición de contabilidad RADIUS, DEBE transmitir un mensaje Respuesta de contabilidad al cliente. El RKS NO DEBE transmitir un mensaje Respuesta de contabilidad si no registra de manera satisfactoria todos los mensajes de evento de un mensaje Petición de contabilidad RADIUS.

El RKS DEBERÍA ignorar los mensajes de evento en los que no esté reconocido el tipo de mensaje de evento IPCablecom. El RKS DEBERÍA ignorar también los atributos de evento IPCablecom en los que no esté reconocido el ID de atributo de evento.

7.3 Requisitos generales del elemento de red de multimedia IPCablecom

Esta cláusula contiene la relación de los requisitos impuestos a los elementos de red de multimedia IPCablecom.

7.3.1 ID de elemento

Cada elemento de red IPCablecom que genera un mensaje de evento DEBE identificarse a sí mismo con un ID de elemento exclusivo y estático. El ID de elemento es un número de elemento configurado estáticamente, exclusivo dentro de un dominio IPCablecom, que DEBE estar en la gama de 0 a 99 999.

7.3.2 Temporización

Es importante que los elementos que generan mensajes de evento permanezcan estrechamente sincronizados entre sí y con un reloj normalizado. Con los requisitos que se especifican en esta subcláusula se asegura que tales elementos mantienen esa sincronización e informan de los eventos con indicaciones de tiempo exactas y precisas.

Los elementos que generan mensajes de evento DEBEN utilizar el protocolo de tiempo de red definido en [2]. Los elementos DEBEN funcionar en modo 3 (modo cliente). El valor de NTP.MAXPOLL NO DEBE exceder de once, lo que corresponde a 2048 segundos.

Los mensajes de evento DEBEN incluir indicaciones de tiempo con una precisión de un milisegundo.

7.3.3 Consideraciones relativas al RKS primario y al RKS secundario

Los multimedia IPCablecom soportan una arquitectura que consta de un RKS primario y un RKS secundario. El RKS secundario se utiliza como RKS de repliegue cuando un elemento de red (PS, CMTS) no es capaz de enviar de manera satisfactoria un mensaje al RKS primario. Los elementos de red de multimedia IPCablecom DEBEN soportar el transporte de mensajes de evento a un RKS primario y cambiar a un RKS secundario cuando falle la comunicación con el RKS primario. Una vez que un elemento de red cambia por fallo al RKS secundario, el secundario pasa a ser primario mientras dure esa sesión o puerta. Al servidor de política se le provisionan RKS primarios y secundarios según requiera la aplicación que soporta. El PS DEBE proporcionar la dirección y el puerto IP del RKS primario y, facultativamente, la del RKS secundario al CMTS en los mensajes de decisión de tipo político (Gate-Set). El PS DEBE soportar múltiples conjuntos de RKS primarios y secundarios.

Para garantizar la transferencia fiable de datos, los elementos de red deberán implementar un intervalo de tiempo de reintentos configurable por el usuario así como el número de veces que requiere el cliente para retransmitir el evento. El intervalo de tiempo deberá ser configurable (se sugiere de 10 ms a 10 s) y también deberá ser configurable el número de reintentos (se sugiere de 0 a 9). Los reintentos deberán poderse efectuar tanto en el RKS primario como en el RKS secundario. Una vez agotado el número de reintentos, el mensaje de evento deberá introducirse en un fichero de errores y a continuación podrá ser eliminado del elemento de red.

Si el elemento de red IPCablecom no recibe un mensaje Respuesta de contabilidad dentro del intervalo de tiempo de reintentos configurado, DEBE continuar reenviando el mensaje Petición de contabilidad hasta que reciba un mensaje Respuesta de contabilidad de un RKS o se haya alcanzado el número máximo de reintentos. El elemento de red IPCablecom DEBE enviar de nuevo el mismo mensaje Petición de contabilidad al RKS primario y, si se alcanza el límite de reintentos, enviar de nuevo el mismo mensaje Petición de contabilidad al RKS secundario.

Todos los elementos de red DEBEN almacenar mensajes de evento hasta que hayan recibido un acuse de recibo (mensaje Respuesta de contabilidad) de un RKS indicando que los datos han sido recibidos correctamente y almacenados o hasta que se haya alcanzado el número máximo de reintentos. Sólo cuando se recibe un acuse de recibo o se alcanza el número máximo de reintentos están autorizados los elementos de red a suprimir esos mensajes de evento.

Una vez que un elemento de red logre enviar mensajes de evento al RKS secundario, se produce un cambio por fallo al RKS secundario. Se trata de un cambio por fallo no reversible, lo que significa que el RKS secundario pasa a estar activo y es el nuevo RKS primario. Los mensajes de evento subsiguientes de la sesión DEBEN ser enviados al RKS secundario ahora activo. Para todas las sesiones nuevas, el PDP DEBE indicar al PEP que utilice el nuevo RKS activo como primario (es decir, el RKS secundario anterior se convierte en el nuevo primario de la sesión subsiguiente). Se señala la posibilidad de que, en determinadas circunstancias, uno de esos elementos, PS o CMTS, sea capaz de comunicar con el RKS primario mientras que el otro quizás no lo sea en la misma sesión. En casos como este se prevé que el RKS pueda conciliar mensajes de evento entre el RKS primario y el secundario.

7.3.4 Interacción con el RKS PacketCable

Un gestor de aplicación PUEDE proporcionar un objeto facultativo de información de generación de evento en un mensaje Gate-Set. De estar presente, este objeto DEBE contener un BCID válido que pueda utilizar el AM, el PS y el CMTS para cotejar información de facturación para el flujo. Si el gestor de aplicación proporciona un BCID al servidor de política, y éste confía en el AM, el PS PUEDE utilizar el BCID proporcionado por el gestor de aplicación.

Si un gestor de aplicación proporciona un objeto facultativo de información de generación de evento en el que se especifican las direcciones IP del RKS primario y secundario de las que el servidor de política no tiene conocimiento, el servidor de política DEBE enviar los mensajes Event para esa transacción a la dirección IP del RKS primario por defecto, salvo en circunstancias de fallo, en cuyo caso los mensajes Event DEBEN enviarse a la dirección IP del RKS secundario por defecto.

El gestor de aplicación PUEDE especificar una dirección IP del RKS primario en el objeto facultativo información de generación de evento o el gestor de aplicación PUEDE permitir que el servidor de política utilice sus direcciones IP del RKS primario y secundario por defecto. Si especifica una dirección IP de RKS primario, el AM PUEDE especificar también una dirección IP de RKS secundario. El gestor de aplicación indica que no se especifica un RKS, poniendo a cero el valor del puerto y las direcciones IP de RKS primario y secundario.

Independientemente de lo que el servidor de política pueda recibir del gestor de aplicación, el PS DEBE ordenar al CMTS que utilice los mismos BCID y direcciones IP y puertos de RKS primario/secundario que elija utilizar el servidor de política. El PS debe decidir a qué par de RKS enviarlo basándose en el AMID.

7.4 Mensajes de evento para multimedia IPCablecom

Esta cláusula contiene una descripción detallada y la definición de cada uno de los mensajes de evento especificados para multimedia IPCablecom.

7.4.1 Eventos de política

Los mensajes de evento de política son nuevos para los multimedia IPCablecom. Indican el momento en que el servidor de política recibe la petición de una acción de tipo político y sirven para abarcar el conjunto consiguiente de mensajes de evento para la utilización de cualquier recurso asociada a las distintas instancias de un servicio. Los mensajes de evento de política se utilizan para indicar la petición de política inicial, una actualización de la política y la supresión de una política.

El PS DEBE poner una indicación de tiempo en los mensajes de evento de política tras la recepción de un mensaje de petición de política procedente del AM. Inmediatamente después de recibir una petición de política inicial, el PS DEBE crear un ID de correlación de facturación (BCID). Cada BICD generado DEBE satisfacer los requisitos de formato de la estructura del atributo ID de correlación de facturación (BCID) del cuadro 17.

El PS DEBE incluir el BCID en el encabezamiento EM de todos los mensajes de evento de política generados a continuación y asociados a esta petición. Además, el PS DEBE incluir el BCID en el mensaje Gate-Set enviado al CMTS.

El PS DEBE generar mensajes de evento de política inmediatamente después de determinar el resultado de una petición de política. El resultado puede basarse en mecanismos de control de autorización y admisión internos del PS o producirse tras recibir una respuesta a sus mensajes Gate-Set y Gate-Delete procedente del CMTS. El PS crea una indicación de tiempo para un mensaje de evento cuando recibe una petición del AM pero no genera el evento hasta conocer el resultado de la petición.

7.4.1.1 Policy_Request

El servidor de política DEBE enviar un mensaje de evento Policy_Request al RKS si se recibe una petición de creación de una nueva política. El PS DEBE fijar el Policy_Decision_Status en aprobado (1) o denegado (2), dependiendo de cual sea el resultado del control de autorización y admisión.

NOTA – Puesto que el PS sólo envía el mensaje de evento Policy_Request después de que el CMTS responda al mensaje Gate-Set, es posible que los mensajes de evento QoS del CMTS lleguen al RKS antes que un mensaje de evento Policy_Request.

Cuadro 7/J.179 – Mensaje de evento Policy_Request

Nombre del atributo	Requerido o facultativo	Comentario
Event_Message_Header	R	Véase el cuadro 16.
Application_Manager_ID	R	Contiene el identificador del AM único en toda la red.
Subscriber_ID	R	Dirección IPv4 de abonado.
Policy_Decision_Status	R	1 – Política aprobada 2 – Política denegada
Policy_Denied_Reason	O	Se requiere cuando Policy_Decision_Status = 2 (política denegada). 1 – Fallo de control de admisión de servidor de política 2 – Recursos insuficientes 3 – Abonado desconocido 127 – Otro
FEID	R	ID de entidad financiera. Identifica la entidad pagadora. Suministrado por el PS.
AM_Opaque_Data	O	Si el gestor de aplicación incluye este objeto (ClientSI: Opaque-Data) en la "petición de política" (DEC COPS), el servidor de política DEBE incluir esto en el mensaje de evento Policy-Event.
Volume_Usage_Limit	O	Si el gestor de aplicación incluye este objeto (ClientSI: Volume-Based-Usage-Limit) en la "petición de política" (DEC COPS), el servidor de política DEBE incluir esto en el mensaje de evento Policy-Event.
Time_Usage_Limit	O	Si el gestor de aplicación incluye este objeto (ClientSI: Time-Based-Usage-Limit) en la "petición de política" (DEC COPS), el servidor de política DEBE incluir esto en el mensaje de evento Policy-Event.

7.4.1.2 Policy_Delete

El servidor de política DEBE enviar un mensaje de evento Policy_Delete al RKS cuando recibe un Gate-Delete del AM indicando que ya no se necesitan los recursos dedicados a una sesión, un Gate-Delete-Ack del CMTS en respuesta a un Gate-Delete iniciado por el PS o un Gate-Report-State del CMTS indicando que ya no se dispone de los recursos de una sesión. El PS DEBE generar un mensaje de evento Policy_Delete para cerrar una sesión siempre que se haya generado previamente un mensaje de evento Policy_Request para abrir la sesión.

Cuadro 8/J.179 – Mensaje de evento Policy_Delete

Nombre del atributo	Requerido o facultativo	Comentario
Event_Message_Header	R	Véase el cuadro 16.
Application_Manager_ID	R	Contiene el identificador del AM único en toda la red.
Subscriber_ID	R	Dirección IPv4 de abonado.
Policy_Deleted_Reason	R	1 – Petición de gestor de aplicación 2 – Decisión de CMTS 127 – Otro
FEID	R	ID de entidad financiera. Identifica la entidad pagadora. Suministrado por el PS.
AM_Opaque_Data	O	Si el gestor de aplicación incluye este objeto (ClientSI: Opaque-Data) en la "petición de política" (DEC COPS), el servidor de política DEBE incluir esto en el mensaje de evento Policy-Event.

7.4.1.3 Policy_Update

El servidor de política DEBE enviar un mensaje de evento Policy_Update al RKS si se recibe del AM una petición de cambio del perfil de tráfico, el clasificador, el límite de volumen, el límite de tiempo o los datos opacos.

Cuadro 9/J.179 – Mensaje de evento Policy_Update

Nombre del atributo	Requerido o facultativo	Comentario
Event Message Header	R	Véase el cuadro 16.
Application_Manager_ID	R	Contiene el identificador del AM único en toda la red.
SubscriberID	R	ID de abonado.
Policy_Decision_Status	R	1 – Política aprobada 2 – Política denegada
Policy_Denied_Reason	O	Se requiere cuando Policy_Decision_Status = 2 (política denegada). 1 – Fallo de control de admisión de servidor de política 2 – Recursos insuficientes 3 – Abonado desconocido 4 – AMID no autorizado 5 – Nombre de clase de servicio no definido 6 – Capacidad máxima incompatible 127 – Otro
Policy_Update_Reason	R	1 – Perfil de tráfico 2 – Clasificador 3 – Límite de volumen 4 – Límite de tiempo 5 – Datos opacos 6 – Actualizaciones múltiples (combinación de 1 a 5) 127 – Otro
FEID	R	ID de entidad financiera. Identifica la entidad pagadora. Suministrado por el PS.
AM_Opaque_Data	O	Si el gestor de aplicación incluye este objeto (ClientSI: Opaque-Data) en la "petición de política" (DEC COPS), el servidor de política DEBE incluir esto en el mensaje de evento Policy-Event.
Volume_Usage_Limit	O	Si el gestor de aplicación incluye este objeto (ClientSI: Volume-Based-Usage-Limit) en la "petición de política" (DEC COPS), el servidor de política DEBE incluir esto en el mensaje de evento Policy-Event.
Time_Usage_Limit	O	Si el gestor de aplicación incluye este objeto (ClientSI: Time-Based-Usage-Limit) en la "petición de política" (DEC COPS), el servidor de política DEBE incluir esto en el mensaje de evento Policy-Event.

7.4.2 QoS_Reserve

El mensaje de evento QoS_Reserve indica el momento en el que el CMTS reserva anchura de banda en la red de acceso IPCablecom. El CMTS DEBE generar también este evento si cambia la anchura de banda reservada.

El CMTS DEBE poner una indicación de tiempo en este mensaje inmediatamente después de la transmisión de un DSA-ACK o DSC-ACK acusando recibo de un DSA-RSP o DSC-RSP satisfactorio al CM que completa una transacción de reserva de recursos.

Si el código de confirmación de DSA-RSP o DSC-RSP procedente del CM no es satisfactorio, el CMTS NO DEBE generar este mensaje.

Cuadro 10/J.179 – Mensaje de evento QoS_Reserve

Nombre del atributo	Requerido o facultativo	Comentario
Event Message Header	R	Véase el cuadro 16
QoS_Descriptor	R	Ninguno
SF_ID	R	Ninguno
Flow_Direction	R	Ninguno
Element_Requesting_QoS	R	0 = Cliente 1 = Servidor de política 2 = Cliente incorporado

7.4.3 QoS_Commit

El mensaje de evento QoS_Commit indica el momento en el que el CMTS compromete anchura de banda en la red de acceso IPCablecom. El CMTS DEBE generar también este evento si cambia la anchura de banda comprometida.

El CMTS DEBE poner una indicación de tiempo en este mensaje inmediatamente después de la transmisión de un DSA-ACK o DSC-ACK acusando recibo de un DSA-RSP o DSC-RSP satisfactorio al CM que completa una transacción de compromiso de recursos.

Si el código de confirmación de DSA-RSP o DSC-RSP procedente del CM no es satisfactorio, el CMTS NO DEBE generar este mensaje.

Cuadro 11/J.179 – Mensaje de evento QoS_Commit

Nombre del atributo	Requerido o facultativo	Comentario
Event Message Header	R	Véase el cuadro 16
QoS_Descriptor	R	Ninguno
SF ID	R	Ninguno
Flow_Direction	R	Ninguno

7.4.4 QoS_Release

El mensaje de evento QoS_Release indica el momento en el que el CMTS libera su reserva y/o compromiso de anchura de banda en la red de acceso IPCablecom.

El CMTS DEBE poner una indicación de tiempo en este mensaje inmediatamente después de la transmisión de un DSD-REQ que indica la petición de que se suprima la anchura de banda.

Cuadro 12/J.179 – Mensaje de evento QoS_Release

Nombre del atributo	Requerido o facultativo	Comentario
Event Message Header	R	Véase el cuadro 16
SF ID	R	Ninguno
Flow_Direction	R	Ninguno
QoS_Release_Reason	R	1 – Puerta cerrada por PS 2 – Expiración de temporizador de inactividad de recuperación de recursos (T4) 3 – Fallo de CM 4 – Apropiado con prioridad 5 – Petición de PathTear RSVP 6 – Petición de CM 7 – Expiración de temporizador (T2) admitida 127 – Otro
Gate_Usage_Info	R	Ninguno
Gate_Time_Info	R	Ninguno

7.4.5 Time_Change

Este evento capta un ejemplar de cambio de hora. Siempre que el reloj (IPCablecom) del elemento de red (PS o CMTS) se cambia en más de 200 milisegundos, el elemento de red DEBE generar un mensaje Time_Change. Se incluyen aquí los eventos de desplazamiento (hora normal/hora de verano), los ajustes graduales para sincronizar con el reloj de referencia NTP y los cambios de ajuste de hora manuales. El atributo Event_Time del encabezamiento de un mensaje de evento DEBE reflejar la nueva noción de hora (ajustada). Se señala que el mensaje Time_Change no se requiere para ajustes de desviación efectuados por el NTP.

El elemento de red (PS y CMTS) DEBE enviar el mensaje Time_Change (cambio de hora) al RKS activo (primario en ese momento). El mensaje de evento Time_Change DEBE ser generado cuando en el CMTS estén presentes una o más puertas. El mensaje de evento Time_Change se envía a cada RKS primario con independencia del número de puertas que puedan existir en el CMTS. En otras palabras, si el CMTS tiene varias puertas, todas las cuales apuntan al mismo RKS, sólo deberá enviarse un mensaje de evento Time_Change a ese RKS.

El BCID del encabezamiento de mensaje de evento del mensaje de evento Time_Change DEBE ser generado localmente por el elemento de red en el momento en que ocurre el evento. El BCID no está asociado a ningún BCID relacionado con una sesión, es un BCID único para este evento.

Cuadro 13/J.179 – Mensaje de evento Time_Change

Nombre del atributo	Requerido o facultativo	Comentario
Event Message Header	R	Véase el cuadro 16
Time_Adjustment	R	Ninguno

7.5 Atributos de mensajería de eventos para multimedia IPCablecom

En esta cláusula se describen y definen los atributos IPCablecom incluidos en los mensajes de evento IPCablecom.

En el cuadro 14 se indica la correspondencia entre cada uno de los mensajes de evento IPCablecom y los atributos asociados a los mismos. El cuadro 15 presenta la descripción detallada de cada uno de esos atributos.

Cuadro 14/J.179 – Correspondencia entre atributos IPCablecom y mensajes de evento MM IPCablecom

ID del atributo de EM	Nombre del atributo de EM	7 – QoS_Reserve	8 – QoS_Release	17 – Time_Change	19 – QoS_Commit	31 – Policy_Request	32 – Policy_Delete	33 – Policy_Update
1	Event_Message_Header	X	X	X	X	X	X	X
30	SF_ID	X	X		X			
32	QoS_Descriptor	X			X			
38	Time_Adjustment			X				
49	FEID					X	X	X
50	Flow_Direction	X	X		X			
61	AM_Opaque_Data					X	X	X
62	Subscriber_ID					X	X	X
63	Volume_Usage_Limit					X		X
64	Gate_Usage_Info		X					
65	Element_Requesting_Qos	X						
66	QoS_Release_Reason		X					
67	Policy_Denied_Reason					X		X
68	Policy_Deleted_Reason						X	
69	Policy_Update_Reason							X
70	Policy_Decision_Status					X		X
71	Application_Manager_ID					X	X	X
72	Time_Usage_Limit					X		X
73	Gate_Time_Info		X					

En el cuadro 15 se define de manera pormenorizada cada uno de los atributos de los mensajes de evento IPCablecom. El valor de los datos de un atributo puede representarse mediante un formato de datos simple (un campo de datos) o mediante una estructura de datos más compleja.

Cuadro 15/J.179 – Atributos de mensajes de evento MM IPCablecom

ID del atributo de EM	Longitud del atributo de EM	Nombre del atributo de EM	Tipo de valor del atributo de EM	Descripción de los datos del atributo
1	76 bytes	EM_Header	Estructura de datos, véase el cuadro 16	Datos comunes requeridos en cada mensaje de evento IPCablecom.
30	4 bytes	SF_ID	Entero sin signo	ID de flujo de servicio, un entero de 32 bits asignado por el CMTS a cada flujo de servicios DOCSIS definido dentro de un dominio MAC RF DOCSIS. Se considera que los SFID están en el sentido ascendente (USFID) o descendente (DSFID). Los USFID y los DSFID son atribuidos desde el mismo espacio de números SFID.
32	Variable; mínimo 8 bytes	QoS_Descriptor	Estructura de datos, véase el cuadro 19	Datos de parámetros de QoS.
38	8 bytes	Time_Adjustment	Entero sin signo	Ajuste de tiempo del reloj de un elemento (PS, CMTS). Este tiempo se da en milisegundos, detallando el valor del cambio de tiempo.
49	Longitud variable; máximo 247 bytes	FEID	Cadena de caracteres ASCII	ID de entidad financiera. Los 8 primeros bytes son datos definidos por el operador de cable. Por defecto, los 8 primeros bytes se llenan con ceros. Del 9º byte en adelante, el campo contiene el nombre del dominio del operador de cable que identifica al operador de cable de manera exclusiva a efectos de facturación y liquidación. El nombre del dominio del operador de cable está limitado a 239 bytes.
50	2 bytes	Flow Direction	Entero sin signo	Sentido del flujo: 0 = Reservado 1 = Ascendente 2 = Descendente
61	8 bytes	AM_Opaque_Data	Entero sin signo	Datos opacos pasados desde el gestor de aplicación.
62	4 bytes	Subscriber_ID	Entero sin signo	Valores de 4 bytes concatenados que representan una dirección IPv4.

Cuadro 15/J.179 – Atributos de mensajes de evento MM IPCablecom

ID del atributo de EM	Longitud del atributo de EM	Nombre del atributo de EM	Tipo de valor del atributo de EM	Descripción de los datos del atributo
63	8 bytes	Volume_Usage_ Limit	Entero sin signo	Límite de volumen en octetos fijado por el AM.
64	8 bytes	Gate_Usage_Info	Entero sin signo	El número de octetos transmitidos por la red RF DOCSIS desde el byte posterior a la HCS del encabezamiento de MAC hasta el final de la CRC.
65	2 bytes	Element_ Requesting_QoS	Entero sin signo	0 = Cliente 1 = Servidor de política 2 = Cliente incorporado
66	2 bytes	QoS_Release_ Reason	Entero sin signo	1 – Puerta cerrada por PS 2 – Expiración de temporizador de inactividad de recuperación de recursos (T4) 3 – Fallo de CM 4 – Apropiado con prioridad 5 – Petición de PathTear RSVP 6 – Petición de CM 7 – Expiración de temporizador (T2) admitida 127 – Otro
67	2 bytes	Policy_Denied_ Reason	Entero sin signo	1 – Fallo de control de admisión de servidor de política 2 – Recursos insuficientes 3 – Abonado desconocido 4 –AMID no autorizado 5 – Nombre de clase de servicio no definido 6 – Capacidad máxima incompatible 127 – Otro
68	2 bytes	Policy_Deleted_ Reason	Entero sin signo	1 – Petición de gestor de aplicación 2 – Decisión de CMTS 127 – Otro
69	2 bytes	Policy_Update_ Reason	Entero sin signo	1 – Perfil de tráfico 2 – Clasificador 3 – Límite de volumen 4 – Límite de tiempo 5 – Datos opacos 6 – Actualizaciones múltiples (combinación de 1 a 5) 127 – Otro
70	2 bytes	Policy_Decision_ Status	Entero sin signo	1 – Política aprobada 2 – Política denegada

Cuadro 15/J.179 – Atributos de mensajes de evento MM IPCablecom

ID del atributo de EM	Longitud del atributo de EM	Nombre del atributo de EM	Tipo de valor del atributo de EM	Descripción de los datos del atributo
71	4 bytes	Application_ Manager_ID	Entero sin signo	Identificador único en toda la red asignado al gestor de aplicación.
72	4 bytes	Time_Usage_ Limit	Entero sin signo	Límite de tiempo en segundos fijado por el AM.
73	4 bytes	Gate_Time_Info	Entero sin signo	El número de segundos que una puerta ha estado en el estado comprometido o recuperación comprometida.

7.5.1 Estructura del atributo Event_Message_Header

El cuadro 16 contiene una descripción detallada de los cambios en la estructura del atributo Event_Message_Header (encabezamiento de mensaje de evento). Este atributo DEBE ser el primero en cada mensaje de evento IPCablecom.

Cuadro 16/J.179 – Estructura del atributo Event_Message_Header

Nombre del campo	Semántica	Tipo de valor	Longitud
ID de versión	Identifica la versión de esta estructura de encabezamiento de EM. 1 = IPCablecom 1.0 2 = IPCablecom 1.1 3 = IPCablecom multimedia NOTA – Un valor de 2 ó 3 indica que en este encabezamiento se utiliza el campo Objeto Evento. Los elementos de red del PS y el CMTS DEBE poner a 3 el valor del ID de versión.	Entero sin signo	2 bytes
BCID	Identificador único de una transacción en una red.	Estructura de datos, véase el cuadro 17	24 bytes
Tipo de mensaje de evento	Identifica el tipo del mensaje de evento.	Entero sin signo	2 bytes
Tipo de elemento	Identifica el tipo del elemento de origen: 0 = Reservado 1 = Reservado 2 = CMTS 3 = Reservado 4 = Servidor de política	Entero sin signo	2 bytes
ID de elemento	Identificador único en toda la red de 5 dígitos (número de elemento configurado estáticamente, exclusivo dentro de un dominio IPCablecom en la gama de 0 a 99999).	Cadena de caracteres ASCII con justificación derecha y relleno de espacios	8 bytes

Cuadro 16/J.179 – Estructura del atributo Event_Message_Header

Nombre del campo	Semántica	Tipo de valor	Longitud
Huso horario	Identifica la existencia de la hora normal o la hora de verano y la diferencia con respecto al tiempo universal (UTC). Hora normal/hora de verano: 0 = Hora normal 1 = Hora de verano Diferencia con respecto a la UTC + HHMMSS La diferencia se notifica desde el punto de vista del elemento de red (PS, CMTS); no en base al punto de vista del abonado.	Cadena de caracteres ASCII	1 byte 7 bytes
Número de secuencia	Cada elemento de red DEBE asignar un entero sin signo único y creciente monótonamente para cada mensaje de evento enviado a un RKS dado. A los efectos de la presente Recomendación, monotónicamente creciente ha de interpretarse como aumentando en 1. El RKS utiliza esto para determinar si faltan mensajes de evento de un elemento de red dado.	Entero sin signo	4 bytes
Hora de evento	Hora y fecha en que se genera un evento. Granularidad de milisegundos. Formato: yyymmddhhmmss.mmm	Cadena de caracteres ASCII	18 bytes
Estatus	Indicadores de estatus	Véase el cuadro 18	4 bytes
Prioridad	Indica el grado de importancia que habrá que asignar en relación con otros mensajes de evento. 255 = máxima prioridad 0 = mínima prioridad 128 = por defecto.	Entero sin signo	1 byte
Cuenta de atributos	Indica el número de atributos que siguen (o se han añadido) a este encabezamiento en el mensaje de evento en curso.	Entero sin signo	2 bytes
Objeto Evento	El campo Objeto Evento permite una agrupación de servicios, 0 = mensaje de evento cuenta 1 = reservado Los elementos de red del PS y el CMTS DEBEN poner a 0 el valor del campo Objeto Evento si el ID de versión del encabezamiento EM es 3 (mensaje de evento multimedia IPCablecom destinado al RKS). El RKS DEBE descartar los mensajes EM cuando el valor del campo Objeto Evento se pone a 1.	Entero sin signo	1 byte

7.5.2 Estructura del campo ID de correlación de facturación (BCID)

El cuadro 17 describe el campo ID de correlación de facturación (BCID). El RKS, o alguna otra aplicación de fondo de oficina, utiliza el BCID para correlacionar mensajes de evento generados por una transacción individual. Es uno de los campos del atributo encabezamiento de mensaje de

evento. El BCID es único para cada transacción en la red. Todos los mensajes de evento procedentes del mismo elemento de red con el mismo BCID DEBEN enviarse al mismo RKS primario, salvo en circunstancias de cambio por fallo, en cuyo caso los mensajes de evento DEBEN enviarse al RKS secundario.

Cuadro 17/J.179 – Descripción del campo BCID

Nombre del campo	Semántica	Tipo de valor	Longitud
Indicación de tiempo	32 bits de orden superior de la referencia de tiempo del NTP.	Entero sin signo	4 bytes
ID de elemento	Identificador único en toda la red de 5 dígitos (número de elemento configurado estáticamente, exclusivo dentro de un dominio IPCablecom en la gama de 0 a 99999).	Cadena de caracteres ASCII con justificación derecha y relleno de espacios	8 bytes
Huso horario	Identifica la existencia de la hora normal o la hora de verano y la diferencia con respecto al tiempo universal (UTC). Hora normal/hora de verano: 0 = Hora normal 1 = Hora de verano Diferencia con respecto a la UTC: ± HHMMSS La diferencia se notifica desde el punto de vista del elemento de red (PS, CMTS); no en base al punto de vista del abonado.	Cadena de caracteres ASCII	 1 byte 7 bytes
Contador de eventos	Monotónicamente creciente para cada transacción.	Entero sin signo	4 bytes

7.5.3 Estructura del campo estatus

El campo estatus del atributo encabezamiento de mensaje de evento es una máscara de 32 bits. El bit 0 es el bit de orden inferior; este campo se trata como un entero sin signo de 4 bytes. En el cuadro 18 se presenta la descripción del campo estatus.

Cuadro 18/J.179 – Descripción del campo estatus

Bit de comienzo	Semántica	Cuenta de bits
0-1	Indicador de error: 0 = Sin error 1 = Error posible 2 = Error conocido 3 = Reservado	2
2	Origen del evento: 0 = Elemento fiduciario 1 = Elemento no fiduciario	1
3	Mensaje de evento mediante apoderado: 0 = Ausencia de apoderado, todos los datos son conocidos por el elemento emisor 1 = Presencia de apoderado, datos enviados por un elemento fiduciario en nombre de un elemento no fiduciario	1
4-31	Reservado. Los bits 4 a 31 del campo de estatus DEBEN ponerse a 0.	28

7.5.4 Estructura del atributo descriptor de QoS

En el cuadro 19 se describe la estructura de datos del descriptor de QoS.

Cuadro 19/J.179 – Estructura de datos del descriptor de QoS

Nombre del campo	Semántica	Tipo de valor	Longitud
Máscara de bits de estatus	Máscara de bits que describe el contenido de la estructura. (Véase el cuadro 20)	Mapa de bits	4 bytes
Nombre de clase de servicio	Nombre de perfil de servicio	Cadena de caracteres ASCII con justificación derecha y relleno de espacios	16 bytes
Serie de parámetros de QoS	Parámetros de QoS. Contenido determinado por la máscara de bits de estatus.	Serie de enteros sin signo	Serie de longitud variable de enteros sin signo de 32 bits

En el cuadro 20 se describe el campo máscara de bits de estatus (Status_Bitmask) de QoS del atributo descriptor de QoS. Los bits 2 a 17 describen el contenido del campo serie de parámetros de QoS (QoS_Parameter_Array). Cada uno de estos bits indica la presencia (bit = 1) o ausencia (bit = 0) del parámetro de QoS denominado en la serie. La posición de un determinado parámetro de QoS en la serie concuerda con el orden de la posición del bit de ese parámetro en la máscara de bits, empezando a partir del bit de orden inferior.

Cada parámetro de QoS presente en QoS_Parameter_Array debe ocupar cuatro bytes. La definición y la codificación de los parámetros de QoS se indican en el anexo C de la Recomendación sobre RFI DOCSIS [1]. Los parámetros de QoS cuya definición especifica menos de cuatro bytes deben tener justificación derecha (donde los cuatro bytes se han de tratar como un entero sin signo) en los cuatro bytes atribuidos al elemento serie.

Cuadro 20/J.179 – Máscara de bits del estatus de QoS

Bit de comienzo	Semántica	Cuenta de bits
0	Indicación de estado 0 = Valor ilegal 1 = Recurso reservado pero no activado 2 = Valor ilegal 3 = Recurso reservado y activado	2
2	Tipo de calendarización de flujo de servicio	1
3	Intervalo de concesión nominal	1
4	Fluctuación de concesión tolerada	1
5	Concesiones por intervalo	1
6	Tamaño de concesión no solicitada	1
7	Prioridad de tráfico	1
8	Velocidad sostenida máxima	1
9	Ráfaga de tráfico máxima	1
10	Velocidad de tráfico reservada mínima	1
11	Tamaño de paquete mínimo	1
12	Ráfaga concatenada máxima	1
13	Política de petición/transmisión	1
14	Intervalo de interrogación secuencial nominal	1
15	Fluctuación de interrogación secuencial tolerada	1
16	Contraorden de tipo de servicio IP	1
17	Latencia en sentido descendente máxima	1

7.6 Protocolo de contabilidad RADIUS

En esta cláusula se especifica el protocolo utilizado entre elementos de red IPCablecom que generan mensajes de evento (PS, CMTS) y el servidor de mantenimiento de registros (RKS). Estos elementos de red DEBEN soportar la contabilidad RADIUS (RFC 2866) [8] con ampliaciones IPCablecom según se define en la presente Recomendación.

El protocolo de contabilidad RADIUS es un protocolo cliente/servidor que consta de dos tipos de mensajes: de petición de contabilidad y de respuesta de contabilidad. Los elementos de red IPCablecom que generan mensajes de evento son clientes RADIUS que envían mensajes Petición de contabilidad al RKS. El RKS es un servidor RADIUS que devuelve mensajes Respuesta de contabilidad a los elementos de red IPCablecom indicando que ha recibido de manera satisfactoria y almacenado el mensaje de evento.

Los mensajes de evento se formatean como paquetes de petición de contabilidad y de respuesta de contabilidad RADIUS según se especifica en [8].

7.6.1 Autenticación y confidencialidad

Para los detalles relativos a la utilización de IPsec con que se proporciona autenticación y confidencialidad de los mensajes RADIUS, y los detalles sobre la utilización correcta del secreto compartido RADIUS, véase la cláusula 8.

7.6.2 Atributos RADIUS normalizados

Cada mensaje RADIUS comienza con el encabezamiento de mensaje RADIUS normalizado que se muestra en el cuadro 21.

Cuadro 21/J.179 – Encabezamiento de mensaje RADIUS

Nombre del campo	Semántica	Longitud del campo
Código	Petición de contabilidad = 4 Respuesta de contabilidad = 5	1 byte
Identificador	Se utiliza para asegurar la concordancia de un mensaje Petición de contabilidad con un mensaje Respuesta de contabilidad	1 byte
Longitud	Longitud total de mensaje RADIUS Valor mínimo = 20 Valor máximo = 4096	2 bytes
Autenticador	Calculado según la especificación RADIUS	16 bytes

Dos atributos RADIUS normalizados DEBEN seguir al encabezamiento de mensaje RADIUS: NAS-IP-Address y Acct_Status_Type. Estos dos campos se incluyen para mejorar la interoperabilidad con las implementaciones de servidor RADIUS existentes ya que son atributos obligatorios en un paquete de petición de contabilidad RADIUS.

El atributo NAS-IP-Address indica el originador del mensaje Petición de contabilidad y DEBE contener la dirección IP del elemento de red IPCablecom de origen.

El atributo Acct_Status_Type indica normalmente si el mensaje Petición de contabilidad marca el comienzo (Start) o el final (Stop) del servicio de usuario. Un mensaje Petición de contabilidad IPCablecom puede contener el comienzo, el final o la actualización del servicio de usuario. Por este motivo se utiliza un valor Acct-Status-Type de Interim-Update para representar mensajes de evento IPCablecom.

Cuadro 22/J.179 – Atributos RADIUS obligatorios

Nombre	Tipo	Longitud	Valor
NAS-IP-Address	4	6	Dirección IP del elemento de red IPCablecom de origen
Acct-Status-Type	40	6	Interim-Update = 3

Cuadro 23/J.179 – Acct_Status_Type RADIUS

Tipo	Longitud	Valor
40	6 bytes	Interim-Update = 3

Los atributos IPCablecom se codifican según la estructura de los atributos específicos del vendedor (VSA, *vendor-specific attributes*) RADIUS que se describe en esta cláusula. Se pueden agregar más atributos IPCablecom o específicos del vendedor a los mensajes de evento existentes añadiendo más VSA RADIUS al mensaje.

El atributo específico del vendedor incluye un campo para identificar al vendedor; la autoridad de asignación de números Internet (IANA, *Internet assigned numbers authority*) ha asignado a IPCablecom el número de empresa privada de gestión de red SMI 4491 para la codificación de estos atributos.

Cuadro 24/J.179 – Estructura de VSA RADIUS para atributos IPCablecom

Nombre del campo	Semántica	Longitud del campo
Tipo	Específico del vendedor = 26	1 byte
Longitud	Longitud total de atributo NOTA – El valor es longitud de vendedor + 8	1 byte
ID de vendedor	CableLabs = 4491	4 bytes
Tipo de atributo de vendedor	Tipo de atributo IPCablecom	1 byte (véase el cuadro 15)
Longitud de atributo de vendedor	Longitud de atributo IPCablecom	1 byte (véase el cuadro 15) NOTA – El valor es longitud de vendedor + 2
Valor de atributo de vendedor	Valor de atributo IPCablecom	Bytes de longitud de vendedor

7.6.3 Sintaxis del paquete de petición de contabilidad RADIUS IPCablecom

```
<<RADIUS Accounting-Request> ::==
        <RADIUS message Header>
        <RADIUS NAS-IP-Address Attribute>
        <RADIUS Acct-Status-Type Attribute>
        <Packet Cable EM>
<Packet Cable EM> ::==
        <RADIUS VSA for IPCablecom EM Header Attribute>
        <IPCablecom EM Attribute List>
<IPCablecom EM Attribute List> ::==
        <RADIUS VSA for IPCablecom EM Attribute> |
        <IPCablecom EM Attribute List>
            <RADIUS VSA for Packet Cable EM Attribute>>
```

El encabezamiento de mensaje de evento es el primer atributo en un mensaje de evento dado. El orden en que aparecen los atributos del mensaje de evento que siguen al encabezamiento de mensaje de evento es arbitrario.

IPCablecom amplía la contabilidad RADIUS introduciendo nuevos atributos y nuevos valores para atributos existentes. Puesto que el protocolo RADIUS puede ampliarse de esta manera, es de prever que las implementaciones de servidor RADIUS existentes requieran sólo modificaciones mínimas para el soporte de la recogida de mensajes de evento IPCablecom en el modo lotes.

8 Requisitos de seguridad

En la seguridad de las interfaces de multimedia IPCablecom se utilizan los mecanismos de seguridad definidos en [11] y [1]. El cuadro 25 contiene un resumen de los mecanismos de seguridad de cada una de las interfaces de multimedia IPCablecom.

Cuadro 25/J.179 – Interfaces de seguridad multimedia

Interfaz	Descripción	Mecanismos de seguridad
pkt-mm-1	CMTS – CM	Autenticación basada en HMAC que se define en el anexo B/J.112 Recomendación sobre RFI.
pkt-mm-2	PS – CMTS	IPsec ESP utilizando gestión de claves basada en IKE o en Kerberos.
pkt-mm-3	AM – PS	IPsec ESP utilizando gestión de claves basada en IKE o en Kerberos.
pkt-mm-4	PS – RKS	IPsec ESP utilizando gestión de claves basada en IKE o en Kerberos.
pkt-mm-5	CMTS – RKS	IPsec ESP utilizando gestión de claves basada en IKE o en Kerberos.
pkt-mm-6	Cliente – CMTS	Fuera del alcance de esta versión de la presente Recomendación.
pkt-mm-7	Cliente – AM	Fuera del alcance de esta versión de la presente Recomendación.
pkt-mm-8	AM – Par	Fuera del alcance de esta versión de la presente Recomendación.
pkt-mm-9	CMTS – Red IP gestionada por operador de cable	Fuera del alcance de esta versión de la presente Recomendación.
pkt-mm-10	Cliente – Par	Fuera del alcance de esta versión de la presente Recomendación.

En las cláusulas que siguen se describe la seguridad que se aplica a cada interfaz de multimedia IPCablecom y se especifican requisitos adicionales o ampliaciones de seguridad cuando se necesitan.

8.1 Interfaz de QoS CMTS – CM (pkt-mm-1)

Los mensajes de QoS del anexo B/J.112 se autentican utilizando un código de autenticación de mensaje de troceo (HMAC, *hash message authentication code*), que consiste en un troceo criptográfico con claves. El cálculo del atributo HMAC que debe incluirse en los mensajes de QoS del anexo B/J.112 se especifican en B.C.1.4.1 de [1].

8.2 Interfaz de COPS servidor de política – CMTS (pkt-mm-2)

La interfaz de COPS servidor de política – CMTS DEBE asegurarse utilizando el protocolo IPsec ESP, especificado en 7.2.1.3.2 de [11]. Los requisitos de gestión de claves de esta interfaz DEBEN cumplir lo especificado en 7.2.1.4.1 de [11]. Para esta interfaz, el servidor de política DEBE satisfacer todos los requisitos de controlador de puerta que se indican en 7.2.1.3.2 y 7.2.1.4.1 de [11]. Es preciso implementar IKE con claves precompartidas, mientras que la implementación de IKE con certificados y la implementación de IPsec kerberizado son facultativas.

En el caso de que se utilice IPsec kerberizado, la cláusula 6.4.5 de [11] define los nombres principales de diversos servicios kerberizados. El primer componente del nombre principal es único para cada tipo de servicio kerberizado. En la cláusula 6.4.5 de [11] se especifica el primer componente del nombre principal del CMTS. El primer componente del nombre principal del servidor de política DEBE ser:

policyserver:<ElementID>

donde <ElementID> se define en 6.4.5 de [11].

En caso de que se utilice IKE con certificados, el nombre de asunto del certificado del servidor tiene el siguiente atributo definido en 8.2.3.4.3 de [11]:

OU=<Sub-System Name>

El valor de <Sub-System Name> identifica un tipo de servidor. El valor de <Sub-System Name> para un CMTS se especifica en 8.2.3.4.3 de [11]. El valor de <Sub-System Name> para un servidor de política DEBE ser la siguiente cadena: policyserver.

8.3 Interfaz de COPS gestor de aplicación – servidor de política (pkt-mm-3)

La interfaz de COPS gestor de aplicación – servidor de política DEBE asegurarse utilizando el protocolo IPsec ESP, especificado en 7.2.1.3.2 de [11]. Los requisitos de gestión de claves de esta interfaz DEBEN cumplir lo especificado en 7.2.1.4.1 de [11]. Para esta interfaz, el gestor de aplicación DEBE satisfacer todos los requisitos de controlador de puerta que se indican en 7.2.1.3.2 y 7.2.1.4.1 de [11]. Es preciso implementar IKE con claves precompartidas, mientras que la implementación de IKE con certificados y la implementación de IPsec kerberizado son facultativas.

En el caso de que se utilice IPsec kerberizado, la cláusula 6.4.5 [11] define los nombres principales de diversos servicios kerberizados. El primer componente del nombre principal es único para cada tipo de servicio kerberizado. El primer componente del nombre principal del servidor de política se especifica en 8.2/J.170. El primer componente del nombre principal del gestor de aplicación DEBE ser:

am:<ElementID>

donde <ElementID> se define en 6.4.5 de [11].

En caso de que se utilice IKE con certificados, el nombre del asunto del certificado del servidor tiene el siguiente atributo definido en 8.2.3.4.3 de [11]:

OU=<Sub-System Name>

El valor de <Sub-System Name> identifica un tipo de servidor. El valor de <Sub-System Name> para un servidor de política se especifica en 8.2/J.170. El valor de <Sub-System Name> para un gestor de aplicación DEBE ser la siguiente cadena de dos caracteres: am.

8.4 Interfaz de mensaje de evento servidor de política – RKS (pkt-mm-4)

La interfaz de mensaje de evento servidor de política – RKS DEBE asegurarse utilizando el protocolo IPsec ESP, especificado en 7.3.2 de [11]. La gestión de claves de esta interfaz DEBE ser idéntica a la especificada para una interfaz CMTS-RK en 7.3.3.2 de [11]. Es preciso implementar IKE con claves precompartidas, mientras que la implementación de IKE con certificados y la implementación de IPsec kerberizado son facultativas.

En el caso de que se utilice IPsec kerberizado, la cláusula 6.4.5 [11] define los nombres principales de diversos servicios kerberizados. El primer componente del nombre principal es único para cada tipo de servicio kerberizado. En la cláusula 6.4.5 de [11] se especifica el primer componente del nombre principal del RKS. El primer componente del nombre principal del servidor de política se especifica en 8.2/J.170.

En caso de que se utilice IKE con certificados, el nombre del asunto del certificado del servidor tiene el siguiente atributo definido en 8.2.3.4.3 de [11]:

OU=<Sub-System Name>

El valor de <Sub-System Name> identifica un tipo de servidor. El valor de <Sub-System Name> para un RKS se especifica en 8.2.3.4.3 de [11]. El valor de <Sub-System Name> para un servidor de política se especifica en 8.2 de [11].

8.5 Interfaz de mensaje de evento CMTS – RKS (pkt-mm-5)

La interfaz de mensaje de evento CMTS – RKS DEBE asegurarse utilizando el protocolo IPsec ESP, especificado en 7.3.2 de [11]. La gestión de claves de esta interfaz se especifica en 7.3.3.2

de [11]. Es preciso implementar IKE con claves precompartidas, mientras que la implementación de IKE con certificados y la implementación de IPsec kerberizado son facultativas.

9 Establecimiento de la correspondencia entre un perfil de tráfico de FlowSpec y DOCSIS

Un perfil de tráfico define los atributos de QoS del flujo IP o el flujo de servicio del anexo B/J.112 que se ha de utilizar al efectuar las operaciones de autorización, reserva y compromiso. Un perfil de tráfico puede definirse aplicando uno de los métodos siguientes:

- FlowSpec.
- Nombre de clase de servicio DOCSIS.
- Parametrización específica de DOCSIS.

En esta cláusula se describen los procedimientos de establecimiento de la correspondencia para obtener los parámetros de QoS específicos de DOCSIS a partir de las distintas representaciones del perfil de tráfico. Un perfil de tráfico puede incluir las capacidades máximas de autorización, reserva y compromiso. Como se define en [3], una FlowSpec consta de una TSpec y una RSpec facultativa.

9.1 Establecimiento de la correspondencia entre tipos de FlowSpecs y tipos de calendarización DOCSIS

Las FlowSpecs soportan dos tipos de servicios: de carga controlada y garantizado. Los servicios de carga controlada dan garantías de anchura de banda mínima, pero no garantías de latencia/retardo. Los servicios garantizados dan garantías tanto de anchura de banda como de latencia/retardo. Un servicio garantizado se puede aproximar de manera muy precisa mediante los tipos de calendarización DOCSIS interrogación secuencial en tiempo real y UGS. Un servicio de carga controlada se puede aproximar de manera muy precisa mediante el tipo de calendarización DOCSIS mejor esfuerzo. El número de servicio FlowSpec de la definición de FlowSpec distingue entre servicio de carga controlada y servicio garantizado. El número de servicio 5 indica que la definición es la del servicio de carga controlada, mientras que el número de servicio 2 indica que la definición es la del servicio garantizado. Además, el servicio de carga controlada contiene solamente los parámetros de colector testigo de TSpec, pero no de RSpec. El servicio garantizado DEBE contener tanto la TSpec como la RSpec.

En el caso de aplicaciones sensibles a la latencia y a la fluctuación tales como las de voz, vídeo MPEG o juegos, podría pedirse el servicio garantizado. El CMTS puede utilizar a continuación los parámetros de perfil de tráfico especificados en la FlowSpec para seleccionar uno de los dos tipos de calendarización DOCSIS que podrían proporcionar servicio garantizado: RTPS y UGS. En el caso de las aplicaciones no sensibles a la latencia podría pedirse el servicio de carga controlada, que se puede utilizar para dar garantías de anchura de banda mínima. El cuadro 26 que sigue presenta las opciones de forma resumida.

Cuadro 26/J.179 – Correspondencia de tipos de FlowSpecs

Tipo de calendarización DOCSIS	Número de servicio FlowSpec	Ejemplo de aplicación
Servicio de concesión no solicitada (UGS)	2 (Garantizado)	Voz por IP
Servicio de interrogación secuencial en tiempo real (RTPS)	2 (Garantizado)	RPV
Mejor esfuerzo (BE)	5 (Carga controlada)	Datos Internet de mejor esfuerzo

El procedimiento general de establecimiento de la correspondencia entre FlowSpec y DOCSIS para flujos de servicio en sentido ascendente es como sigue:

- Tras la recepción de un mensaje Gate-Set con una FlowSpec, el CMTS DEBE analizar el encabezamiento de servicio de TSpec para determinar si se pide servicio de carga controlada o servicio garantizado.
- Si se pide servicio de carga controlada, el CMTS DEBE utilizar solamente los parámetros de TSpec para decidir cuáles son los parámetros de calendarización DOCSIS con los que se han de definir los parámetros de tráfico DOCSIS para un tipo de calendarización de mejor esfuerzo DOCSIS.
- Si se pide servicio garantizado, el CMTS DEBE examinar los valores del parámetro de TSpec para la velocidad reservada (R) y la velocidad de colector (r). Si los dos valores son iguales, el CMTS DEBE utilizar la TSpec y la RSpec para definir los parámetros de tráfico DOCSIS para un tipo de calendarización UGS DOCSIS.
- Si la velocidad reservada (R) y la velocidad de colector (r) no son iguales, el CMTS DEBE utilizar la TSpec y la RSpec para definir los parámetros de tráfico DOCSIS para un tipo de calendarización interrogación secuencial en tiempo real DOCSIS.

Se señala que en lo anterior no se ha hecho mención de otros dos tipos de calendarización DOCSIS. Esos tipos son:

- Servicio de concesión no solicitada con detección de actividad.
- Servicio de interrogación secuencial no en tiempo real.

Si el gestor de aplicación desea pedir cualquiera de esos servicios, sólo puede hacerlo utilizando bien el nombre de clase de servicio o bien el método de parametrización específico de DOCSIS de definición del perfil de tráfico.

9.2 Establecimiento de la correspondencia entre parámetros de tráfico de FlowSpecs y DOCSIS

La FlowSpec consta de dos partes: la TSpec y la RSpec. La TSpec describe el tráfico del flujo y la RSpec describe el servicio deseado; se señala que para el servicio de carga controlada, no se utiliza la RSpec. Los parámetros de RSpec DEBEN ser especificados para un servicio garantizado. El CMTS DEBE ignorar los parámetros de RSpec en el caso de un servicio de carga controlada. La RSpec se utiliza para dar garantías de latencia en servicios garantizados. Para más información sobre cómo deberán ser utilizados estos parámetros por los gestores de aplicación para especificar el perfil de tráfico, consúltense las normas RFC 2210 [3], 1305 [2], 2211 [4] y 2212 [5]. Se señala que la interpretación multimedia IPCablecom de las FlowSpecs difiere de las normas RFC en los aspectos siguientes:

- El servicio garantizado definido en [5] controla el retardo de puesta en cola de espera de capa 3 (es decir, los retardos asociados a la calendarización de paquetes), mientras que en multimedia IPCablecom lo que más interesa es controlar el retardo de acceso de la capa MAC DOCSIS. En consecuencia, los recursos de anchura de banda se reservan de acuerdo con el parámetro r de TSpec en lugar de con R de RSpec.
- Como se indica en [4], el servicio de carga controlada define solamente una velocidad mínima garantizada para un flujo. El servicio de carga controlada de multimedia IPCablecom facilita la definición de la velocidad máxima para un flujo, así como la definición de flujos sin una velocidad mínima garantizada.
- El parámetro término suelto de servicio garantizado no se necesita en multimedia IPCablecom, por lo que el campo se define de nuevo para habilitar el control de la fluctuación de la interrogación secuencial DOCSIS.

Parámetros de TSpec:

- Profundidad de colector (b), bytes.
- Velocidad de colector (r), bytes/segundo.
- Tamaño de datagrama máximo (M), bytes.
- Unidad mínima sujeta a aplicación de política (m), bytes.
- Velocidad de cresta (p), bytes/segundo.

Parámetros de RSpec:

- Velocidad reservada (R), bytes/segundo.
- Término suelto (S), microsegundos.

El establecimiento de la correspondencia de los parámetros, en una aproximación no muy estricta, conlleva las asociaciones que se indican seguidamente para flujos de servicio de mejor esfuerzo (BE, *best effort*) en sentido ascendente y de carga controlada en sentido descendente DOCSIS. El procedimiento de establecimiento de la correspondencia real implicará la normalización de estos parámetros para tener en cuenta consideraciones relativas al encabezamiento de capa 2 y capa 3.

- Profundidad de colector TSpec (b) ~= Ráfaga de tráfico máxima DOCSIS.
- Tamaño de datagrama máximo TSpec (M) ~= <not required by DOCSIS>.
- Unidad mínima sujeta a aplicación de política TSpec (m) ~= Tamaño asumido de paquete de velocidad reservada mínima DOCSIS.
- Velocidad de colector TSpec (r) ~= Velocidad reservada mínima DOCSIS.
- Velocidad de cresta TSpec (p) ~= Velocidad sostenida máxima DOCSIS para servicio de carga controlada.

En el caso de flujos de servicio garantizado en sentido descendente, se añaden los parámetros de RSpec para proporcionar garantías de latencia y reserva.

- Profundidad de colector TSpec (b) ~= Ráfaga de tráfico máxima DOCSIS.
- Tamaño de datagrama máximo TSpec (M) ~= <not required by DOCSIS>.
- Unidad mínima sujeta a aplicación de política TSpec (m) ~= Tamaño asumido de paquete de velocidad reservada mínima DOCSIS.
- Velocidad de colector TSpec (r) ~= Velocidad reservada mínima DOCSIS.
- Velocidad reservada RSpec ~= Velocidad sostenida máxima DOCSIS para servicio garantizado.
- Término suelto RSpec ~= Latencia en sentido descendente DOCSIS.

El establecimiento de la correspondencia de los parámetros, en una aproximación no muy estricta, conlleva las asociaciones que se indican seguidamente para flujos de servicio UGS DOCSIS.

- Profundidad de colector TSpec (b) = Tamaño de datagrama máximo TSpec (M) = Unidad mínima sujeta a aplicación de política TSpec (m) ~= Tamaño de concesión no solicitada DOCSIS.
- Velocidad de colector TSpec (r) = Velocidad de cresta TSpec (p) = Velocidad reservada RSpec (R) ~= <not required by DOCSIS>.
- Término suelto RSpec ~= Fluctuación de concesión tolerada DOCSIS.

De manera similar, se aplican las asociaciones siguientes para flujos de servicio de interrogación secuencial en tiempo real DOCSIS.

- Profundidad de colector TSpec (b) ~= Ráfaga de tráfico máxima DOCSIS.
- Tamaño de datagrama máximo TSpec (M) ~= <not required by DOCSIS>.

- Velocidad de colector TSpec (r) ~= Velocidad sostenida máxima DOCSIS para servicio garantizado.
- Velocidad reservada RSpec (R) ~= Se utiliza para calcular el intervalo de interrogación secuencial.
- Término suelto RSpec ~= Fluctuación de interrogación secuencial tolerada.

Este modelo de abstracción permite implementaciones RSVP basadas en normas (según lo previsto en los escenarios 2 y 3) para pedir y recibir servicio de carga controlada o garantizado de la red sin requerir necesariamente información específica de DOCSIS.

En algunas situaciones, en las que el gestor de aplicación y el servidor de política están totalmente al corriente de DOCSIS, se PUEDE especificar el perfil de tráfico de la puerta utilizando el nombre de clase de servicio DOCSIS o el formato de parametrización específico de DOCSIS.

Se señala que hay varios parámetros de flujo de servicio DOCSIS que no se pueden deducir directamente a partir de las FlowSpecs; en tales casos, la Recomendación relativa a multimedia IPCablecom define valores por defecto para esos parámetros de flujo de servicio. Si el gestor de aplicación/servidor de política desea fijar esos parámetros de flujo de servicio en valores distintos a los valores por defecto especificados en esta Recomendación, el gestor de aplicación/servidor de política DEBE utilizar los nombres de clase de servicio o los formatos de parametrización específicos de DOCSIS para definir el perfil de tráfico.

En el caso de servicio garantizado, la velocidad reservada mínima y la velocidad sostenida máxima se fijan en el mismo valor, y se basan en la velocidad de colector, 'r'. Esto es así porque el servicios garantizado da garantías de latencia, lo que significa que un flujo no puede ser sostenido a una velocidad superior a aquella a la que el origen ha acordado generar (cuando la reserva se hizo inicialmente). Una reserva efectuada con un perfil de tráfico que especifica una velocidad de colector 'r' significa que el origen no sostendrá un flujo de tráfico superior a 'r'. Así pues, sería incorrecto utilizar la velocidad reservada 'R' para representar cualquier velocidad sostenida DOCSIS (mínima o máxima), si el servicio es servicio garantizado.

Con calendarización de interrogación secuencial en tiempo real, no obstante, el CMTS utiliza la velocidad reservada R para calcular el intervalo de interrogación secuencial, por lo que los orígenes del tráfico pueden producir ráfagas a la velocidad R sin incrementar el retardo que sufren los paquetes que esperan una oportunidad de transmisión en sentido ascendente DOCSIS. Aunque en este caso el origen del tráfico puede generar tráfico a la velocidad 'R', el CMTS asegurará que la velocidad sostenida no incumple la prescripción de valor 'r' a lo largo del tiempo.

Con servicio de carga controlada, puesto que no hay garantías de latencia y se desea posibilitar la utilización de los conceptos específicos de DOCSIS de velocidad garantizada mínima y de velocidad sostenida máxima, se hace corresponder la velocidad de colector TSpec 'r' con la velocidad mínima DOCSIS y la velocidad de cresta TSpec 'p' con la velocidad sostenida máxima DOCSIS. Si se indica un valor de cero o infinito para 'r', el parámetro velocidad reservada mínima DOCSIS DEBE ser omitido. Si se indica un valor de cero o infinito para 'p', el parámetro velocidad sostenida máxima DOCSIS DEBE ser omitido.

En caso de discrepancia sintáctica o semántica entre la especificación RFI DOCSIS y la presente especificación, prevalecerá la especificación RFI DOCSIS a menos que se indique otra cosa.

9.3 Parámetros en sentido ascendente DOCSIS

En todos los cálculos del tamaño de paquetes en sentido ascendente se ha de aplicar la regla siguiente a menos que se indique otra cosa: la PDU del paquete DEBE calcularse desde la secuencia de verificación de encabezamiento (HCS) MAC DOCSIS hasta el final de la CRC. Este valor incluye la tara de encabezamiento de Ethernet de 18 bytes (6 bytes para la dirección de origen, 6 bytes para la dirección de destino, 2 bytes para la longitud y 4 bytes para la CRC). El valor

incorpora además la tara de capa MAC DOCSIS, incluyendo el encabezamiento base DOCSIS (6 bytes), el encabezamiento ampliado UGS (3 bytes) y el encabezamiento ampliado BPI+ (5 bytes).

En las ecuaciones que figuran en las cláusulas siguientes se utilizan las siguientes variables:

ENET = Tara Ethernet (18 ó 22 bytes); a menos que se indique otra cosa, DEBE utilizarse un valor por defecto de 18 bytes (la manera en que el CMTS determina cuándo ha de emplear 22 bytes queda fuera del alcance de esta Recomendación). En el caso de un flujo UGS, se descartarán los paquetes que utilicen encabezamientos Ethernet ampliados que no se tengan en cuenta (los paquetes cuyo tamaño supere el tamaño de concesión deberán descartarse). En el caso de un flujo RTPS, los paquetes que utilicen encabezamientos Ethernet ampliados que no se tengan en cuenta se enviarán por el flujo de servicio primario (mejor esfuerzo).

DOCSIS = encabezamiento DOCSIS = 6 bytes

BPI = encabezamiento BPI DOCSIS = 5 bytes

UGS = encabezamiento ampliado UGS DOCSIS = 3 bytes

9.3.1 Calendarización de concesión no solicitada (UGS)

La calendarización de concesión no solicitada DEBE utilizarse cuando el número de servicio es 2 (garantizado), la velocidad de cresta, la velocidad de colector y la velocidad reservada son iguales, y el tamaño de datagrama máximo es igual a la unidad mínima sujeta a aplicación de política.

Los objetos en sentido ascendente DOCSIS DEBEN fijarse como se indica más adelante. A todas las codificaciones TLV de calidad de servicio de flujos de servicio que no se definen aquí se les DEBEN dar sus valores por defecto indicados por DOCSIS.

El tamaño de concesión no solicitada DOCSIS incorpora la tara de la capa MAC DOCSIS además del tamaño de la PDU del paquete calculado mediante la fórmula especificada en 9.3. La tara de capa MAC DOCSIS incluye el encabezamiento básico DOCSIS (6 bytes), el encabezamiento ampliado UGS (3 bytes) y, facultativamente, el encabezamiento ampliado BPI+ (5 bytes).

$$\text{Tamaño de concesión no solicitada DOCSIS} = M + \text{ENET} + \text{DOCSIS} + \text{UGS} + \text{BPI}$$

En el ejemplo anterior se supone que BPI+ [12] está habilitada.

Los parámetros velocidad de tráfico sostenida máxima DOCSIS y tamaño asumido de paquete de velocidad reservada mínima DOCSIS NO DEBEN ser utilizados con flujos en sentido ascendente.

El parámetro concesiones por intervalo DEBE fijarse a 1.

El parámetro intervalo de concesión nominal DOCSIS DEBE fijarse al tamaño de datagrama máximo dividido por la velocidad reservada, convertido en microsegundos.

$$\text{Intervalo de concesión nominal DOCSIS} = M/R \times 1\,000\,000$$

El parámetro fluctuación de concesión tolerada DOCSIS DEBE fijarse a término suelto. Si el valor es inferior a la duración de un miniintervalo de tiempo DOCSIS, DEBE utilizarse en cambio la duración del miniintervalo de tiempo. Si se especifica un valor de cero, DEBE utilizarse el valor por defecto de 800 μs.

El parámetro intervalo de interrogación secuencial nominal DOCSIS NO DEBE ser especificado en el perfil de tráfico para flujos de servicio UGS. El parámetro fluctuación de interrogación secuencial tolerada DOCSIS NO DEBE ser especificado en el perfil de tráfico para flujos de servicio UGS.

El parámetro política de petición/transmisión DOCSIS es una máscara de bits. Los bits 0 a 6 y 8 DEBEN fijarse para los flujos de servicio UGS.

9.3.2 Calendarización de interrogación secuencial en tiempo real

La calendarización de interrogación secuencial en tiempo real DEBE utilizarse cuando el número de servicio es 2 (servicio garantizado) y la velocidad de cresta no es igual a la velocidad de colector o el tamaño de datagrama máximo no es igual a la unidad mínima sujeta a aplicación de política.

Los objetos en sentido ascendente DOCSIS DEBEN fijarse como se indica más adelante. A todas las codificaciones TLV de calidad de servicio de flujos de servicio que no se definen aquí se les DEBEN dar sus valores por defecto indicados por DOCSIS.

El parámetro velocidad de tráfico sostenida máxima DOCSIS se da en bits por segundo e incluye la tara de capa Ethernet. La conversión a partir de parámetros específicos del IP conlleva la determinación primero de la velocidad de paquetización dividiendo la velocidad de colector por la unidad mínima sujeta a aplicación de política. Este valor se multiplica a continuación por el tamaño de paquete, la unidad mínima sujeta a aplicación de política, incluyendo la tara de capa MAC, y a la totalidad del producto se le aplica una escalación de bytes a bits.

$$\text{Velocidad de tráfico sostenida máxima DOCSIS} = r/m \times (m + \text{ENET}) \times 8$$

El parámetro ráfaga de tráfico máxima DOCSIS DEBE fijarse al valor mayor de estos dos:

1) la profundidad de colector incluida la tara Ethernet calculada utilizando la unidad mínima sujeta a aplicación de política; o
2) el valor mínimo especificado DOCSIS de 1522.

$$\text{Ráfaga de tráfico máxima DOCSIS} = \text{máx.}\ ((\text{profundidad de colector}/m) \times (m + \text{ENET}), 1522)$$

El parámetro velocidad de tráfico reservada mínima DOCSIS es lo mismo que la velocidad de tráfico sostenida máxima DOCSIS.

$$\text{Velocidad de tráfico reservada mínima DOCSIS} = r/m \times (m + \text{ENET}) \times 8$$

El parámetro política de petición/transmisión DOCSIS es una máscara de bits; el valor por defecto recomendado debería ser 0x1F.

El valor del parámetro intervalo de interrogación secuencial nominal DOCSIS DEBE ser igual a la unidad mínima sujeta a aplicación de política dividida por velocidad reservada, convertido en microsegundos.

$$\text{Intervalo de interrogación secuencial nominal DOCSIS} = m/R \times 1\,000\,000$$

El parámetro fluctuación de interrogación secuencial tolerada DOCSIS DEBE fijarse en término suelto. Si el valor es distinto de cero pero inferior a la duración de un miniintervalo de tiempo, se DEBE fijar en la duración de un miniintervalo de tiempo. Si se especifica un valor de cero, la fluctuación de interrogación secuencial tolerada DOCSIS DEBE utilizar el valor por defecto de 800 μs.

$$\text{Fluctuación de interrogación secuencial nominal DOCSIS} = S$$

9.3.3 Calendarización de mejor esfuerzo

La calendarización de mejor esfuerzo DEBE utilizarse cuando el número de servicio es 5 (carga controlada).

Los objetos en sentido ascendente DOCSIS DEBEN fijarse como se indica más adelante. A todas las codificaciones TLV de calidad de servicio de flujos de servicio que no se definen aquí se les DEBEN dar sus valores por defecto indicados por DOCSIS.

La prioridad de tráfico DOCSIS DEBE fijarse a 5.

El parámetro velocidad de tráfico sostenida máxima DOCSIS se da en bits por segundo e incluye la tara de capa Ethernet. La conversión a partir de parámetros específicos del IP conlleva la determinación primero de la velocidad de paquetización dividiendo la velocidad de colector por la unidad mínima sujeta a aplicación de política. Este valor se multiplica a continuación por el tamaño de paquete, la unidad mínima sujeta a aplicación de política, modificado para incluir la tara de capa MAC, y a la totalidad del producto se le aplica una escalación de bytes a bits. La velocidad de tráfico sostenida máxima DOCSIS DEBE convertirse a partir de la unidad mínima sujeta a aplicación de política.

$$\text{Velocidad de tráfico sostenida máxima DOCSIS} = p/m \times (m + \text{ENET}) \times 8$$

El parámetro ráfaga de tráfico máxima DOCSIS DEBE fijarse al valor mayor de estos dos:

1) la profundidad de colector incluida la tara Ethernet calculada utilizando la unidad mínima sujeta a aplicación de política; o
2) el valor mínimo especificado DOCSIS de 1522.

$$\text{Ráfaga de tráfico máxima DOCSIS} = \text{máx.}((\text{profundidad de colector}/m) \times (m + \text{ENET}), 1522)$$

El parámetro velocidad de tráfico reservada mínima DOCSIS se calcula de manera similar a la velocidad de tráfico sostenida máxima Ethernet, pero en vez de utilizar el parámetro velocidad de cresta se utiliza la velocidad de colector.

$$\text{Velocidad de tráfico reservada mínima DOCSIS} = r/m \times (m + \text{ENET}) \times 8$$

9.3.4 Codificaciones de clasificación de paquetes en sentido ascendente

9.3.4.1 Peticiones de clasificación de paquetes en sentido ascendente DOCSIS

Los objetos de clasificación en sentido ascendente DOCSIS DEBEN fijarse como se indica más adelante. A todas las codificaciones TLV de clasificación que no se definen aquí se les DEBEN dar sus valores por defecto indicados por DOCSIS.

DEBE utilizarse el parámetro identificador de clasificador DOCSIS.

DEBE utilizarse el parámetro identificador de flujo de servicio DOCSIS.

El parámetro prioridad de regla DOCSIS DEBE fijarse al valor de prioridad del objeto Clasificador.

El parámetro estado de activación de clasificación DOCSIS DEBE fijarse a activo (1) cuando la puerta que utiliza el flujo de servicio está comprometida y en todos los demás casos DEBE fijarse inactivo (0).

La acción de cambio de servicio dinámico DOCSIS PUEDE utilizar las operaciones DSC añadir clasificador (0), DSC reemplazar clasificador (1) y DSC suprimir clasificador (2) de conformidad con la Recomendación sobre RFI DOCSIS.

El parámetro protocolo IP DOCSIS DEBE fijarse al valor del ID de protocolo especificado en el objeto clasificador, si dicho valor es distinto de cero, y de lo contrario omitirse.

El parámetro dirección IP de origen DOCSIS DEBE fijarse a la misma dirección que figura en el objeto Clasificador, siempre que se proporcione un valor distinto de cero. Si la dirección especificada en el objeto Clasificador es cero, este parámetro DEBE ser omitido.

El parámetro máscara de origen IP DOCSIS DEBE ser omitido.

Los parámetros comienzo de puerto IP de origen DOCSIS y final de puerto IP de origen DOCSIS DEBEN fijarse al mismo valor de puerto que se indica en el objeto clasificador, siempre que se proporcione un valor distinto de cero. Si el valor especificado en el objeto Clasificador es cero, DEBEN omitirse ambos parámetros, a saber, comienzo de puerto IP de origen DOCSIS y final de puerto IP de origen DOCSIS.

El parámetro dirección IP de destino DOCSIS DEBE fijarse a la misma dirección que figura en el objeto Clasificador, siempre que se proporcione un valor distinto de cero. Si la dirección especificada en el objeto Clasificador es cero, este parámetro DEBE ser omitido.

El parámetro máscara de destino IP DOCSIS DEBE ser omitido.

Los parámetros comienzo de puerto IP de destino DOCSIS y final de puerto IP de destino DOCSIS DEBEN fijarse al mismo valor de puerto que se indica en el objeto Clasificador, siempre que se proporcione un valor distinto de cero. Si el valor especificado en el objeto Clasificador es cero, DEBEN omitirse ambos parámetros, a saber, comienzo de puerto IP de destino DOCSIS y final de puerto IP de destino DOCSIS.

Los parámetros codificaciones de clasificación de paquetes LLC Ethernet DOCSIS DEBEN ser omitidos.

Los parámetros codificaciones de clasificación de paquetes 802.1P/Q DOCSIS DEBEN ser omitidos.

9.4 Parámetros en sentido descendente DOCSIS

9.4.1 Codificaciones de QoS en sentido descendente para servicio garantizado

Las codificaciones TLV de calidad de servicio de los flujos de servicio en sentido descendente DOCSIS DEBEN fijarse como se indica más adelante. A todas las codificaciones TLV de calidad de servicio de los flujos de servicio que no se definen aquí se les DEBEN dar sus valores por defecto indicados por DOCSIS.

Los parámetros DOCSIS en sentido descendente se calculan utilizando el encabezamiento MAC DOCSIS desde el byte que sigue a la HCS hasta el final de la CRC. Este valor incluye la tara de encabezamiento Ethernet.

En base a esta tara, el parámetro tamaño asumido de paquete de velocidad reservada mínima DOCSIS DEBE calcularse como sigue:

$$\text{Tamaño asumido de paquete de velocidad reservada mínima DOCSIS} = m + ENET$$

El parámetro velocidad de tráfico sostenida máxima DOCSIS se da en bits por segundo e incluye la tara de capa MAC. La conversión a partir de parámetros específicos del IP conlleva la determinación primero de la velocidad de paquetización dividiendo la velocidad de colector por la unidad mínima sujeta a aplicación de política. Este valor se multiplica a continuación por el tamaño de paquete, la unidad mínima sujeta a aplicación de política, modificado para incluir la tara de capa MAC, y a la totalidad del producto se le aplica una escalación de bytes a bits. La velocidad de tráfico sostenida máxima DOCSIS se DEBE calcular como sigue:

$$\text{Velocidad de tráfico sostenida máxima DOCSIS} = r/m \times (m + ENET) \times 8$$

La velocidad de tráfico reservada mínima DOCSIS es igual a la velocidad de tráfico sostenida máxima DOCSIS.

Se señala que la velocidad de tráfico sostenida máxima DOCSIS y la velocidad de tráfico reservada mínima DOCSIS se calculan de manera ligeramente diferente en IPCablecom multimedia e IPCablecom DQoS. Los multimedia IPCablecom se basan en r y DQoS de IPCablecom se basa en p. Esto se debe a que en DQoS de IPCablecom r = p, mientras que en multimedia IPCablecom estos valores son diferentes (en este caso r es el valor de velocidad apropiado a utilizar).

El parámetro ráfaga de tráfico máxima DOCSIS DEBE fijarse al valor mayor de estos dos:

1) la profundidad de colector incluida la tara DOCSIS calculada utilizando la unidad mínima sujeta a aplicación de política; o
2) el valor mínimo especificado DOCSIS de 1522.

Ráfaga de tráfico máxima DOCSIS = máx. ((profundidad de colector/m) × (m + ENET), 1522)

El parámetro prioridad de tráfico DOCSIS se DEBE fijarse a 5.

El parámetro latencia en sentido descendente DOCSIS DEBE fijarse a término suelto. Si término suelto es cero, NO DEBE darse valor a este parámetro.

9.4.2 Codificaciones de QoS en sentido descendente para servicio de carga controlada

Las codificaciones TLV de calidad de servicio de los flujos de servicio en sentido descendente DOCSIS DEBEN fijarse como se indica más adelante. A todas las codificaciones TLV de calidad de servicio de los flujos de servicio que no se definen aquí se les DEBEN dar sus valores por defecto indicados por DOCSIS.

Los parámetros DOCSIS en sentido descendente se calculan utilizando el encabezamiento MAC DOCSIS desde el byte que sigue a la HCS hasta el final de la CRC. Este valor incluye la tara de encabezamiento Ethernet.

En base a esta tara, el parámetro tamaño asumido de paquete de velocidad reservada mínima DOCSIS DEBE calcularse como sigue:

Tamaño asumido de paquete de velocidad reservada mínima DOCSIS= m + ENET

El parámetro velocidad de tráfico sostenida máxima DOCSIS se da en bits por segundo e incluye la tara de capa MAC. La conversión a partir de parámetros específicos del IP conlleva la determinación primero de la velocidad de paquetización dividiendo la velocidad de cresta por la unidad mínima sujeta a aplicación de política. Este valor se multiplica a continuación por el tamaño de paquete, la unidad mínima sujeta a aplicación de política, modificado para incluir la tara de capa MAC, y a la totalidad del producto se le aplica una escalación de bytes a bits. La velocidad de tráfico sostenida máxima DOCSIS DEBE calcularse como sigue:

Velocidad de tráfico sostenida máxima DOCSIS = p/m × (m + ENET) × 8

El parámetro velocidad de tráfico reservada mínima DOCSIS se calcula de manera similar a la de la velocidad de tráfico sostenida máxima DOCSIS, pero en vez de utilizar la velocidad de cresta se utiliza la velocidad de colector.

Velocidad de tráfico reservada mínima DOCSIS = r/m × (m + ENET) × 8

El parámetro ráfaga de tráfico máxima DOCSIS DEBE fijarse al valor mayor de estos dos:

1) la profundidad de colector incluida la tara DOCSIS calculada utilizando el tamaño de datagrama máximo; o
2) el valor mínimo especificado DOCSIS de 1522.

Ráfaga de tráfico máxima DOCSIS = máx. ((profundidad de colector/M) × (M + ENET), 1522)

El parámetro prioridad de tráfico DOCSIS DEBE fijarse a 5.

Al parámetro latencia en sentido descendente DOCSIS NO se le DEBE dar valor.

9.4.3 Codificaciones de clasificación de paquetes en sentido descendente

9.4.3.1 Peticiones de clasificación de paquetes en sentido descendente DOCSIS

Los objetos de clasificación en sentido descendente DOCSIS DEBEN fijarse como se indica más adelante. A todas las codificaciones TLV de clasificación que no se definen aquí se les DEBEN dar sus valores por defecto indicados por DOCSIS.

El CMTS, DEBE utilizarse el parámetro identificador de clasificador DOCSIS.

El CMTS, DEBE utilizarse el parámetro identificador de flujo de servicio DOCSIS.

El parámetro prioridad de regla DOCSIS DEBE fijarse al valor de prioridad especificado en el objeto Clasificador.

El parámetro estado de activación de clasificación DOCSIS DEBE fijarse a activo (1) cuando la puerta que utiliza el flujo de servicio está comprometida y en todos los demás casos DEBE fijarse a inactivo (0).

La acción de cambio de servicio dinámico DOCSIS PUEDE utilizar las operaciones DSC añadir clasificador (0), DSC reemplazar clasificador (1) y DSC suprimir clasificador (2) de conformidad con la Recomendación sobre RFI DOCSIS.

El parámetro protocolo IP DOCSIS DEBE fijarse al valor ID de protocolo especificado en el objeto Clasificador, si dicho valor es distinto de cero y en caso contrario omitirse.

El parámetro dirección IP de origen DOCSIS DEBE fijarse a la dirección de origen que figura en el objeto Clasificador, siempre que se proporcione un valor distinto de cero. Si la dirección especificada en el objeto Clasificador es cero, este parámetro DEBE ser omitido.

El parámetro máscara de origen IP DOCSIS DEBE ser omitido.

Los parámetros comienzo de puerto IP de origen DOCSIS y final de puerto IP de origen DOCSIS DEBEN fijarse al mismo valor de puerto que en el objeto Clasificador, siempre que se proporcione un valor distinto de cero. Si el valor especificado en el objeto clasificador es cero, ambos parámetros, comienzo de puerto IP de origen DOCSIS y final de puerto IP de origen DOCSIS, DEBEN ser omitidos.

El parámetro dirección IP de destino DOCSIS DEBE fijarse al valor de la dirección de destino proporcionado en el objeto Clasificador, siempre que se proporcione un valor distinto de cero. Si la dirección especificada en el objeto Clasificador es cero, este parámetro DEBE ser omitido.

El parámetro máscara de destino IP DOCSIS DEBE ser omitido.

Los parámetros comienzo de puerto IP de destino DOCSIS y final de puerto IP de destino DOCSIS DEBEN fijarse al mismo valor de puerto que en el objeto Clasificador, siempre que se proporcione un valor distinto de cero. Si el valor especificado en el objeto clasificador es cero, ambos parámetros, comienzo de puerto IP de destino DOCSIS y final de puerto IP de destino DOCSIS, DEBEN ser omitidos.

Los parámetros codificaciones de clasificación de paquetes LLC Ethernet DOCSIS DEBEN ser omitidos.

Los parámetros codificaciones de clasificación de paquetes 802.1P/Q DOCSIS DEBEN ser omitidos.

10 Flujos de mensajes

Esta cláusula proporciona dos escenarios de interacción entre los distintos elementos de red presentados anteriormente en esta Recomendación. La primera interacción describe a un nivel relativamente alto los intercambios de mensajes que tienen lugar en el marco de multimedia IPCablecom para autorizar, reservar y comprometer recursos de red de acceso según el escenario 1. La segunda interacción hace una exposición muy pormenorizada de cada uno de los mensajes y los atributos involucrados en las interfaces de QoS y EM de multimedia IPCablecom.

10.1 Secuencia de mensajes básica

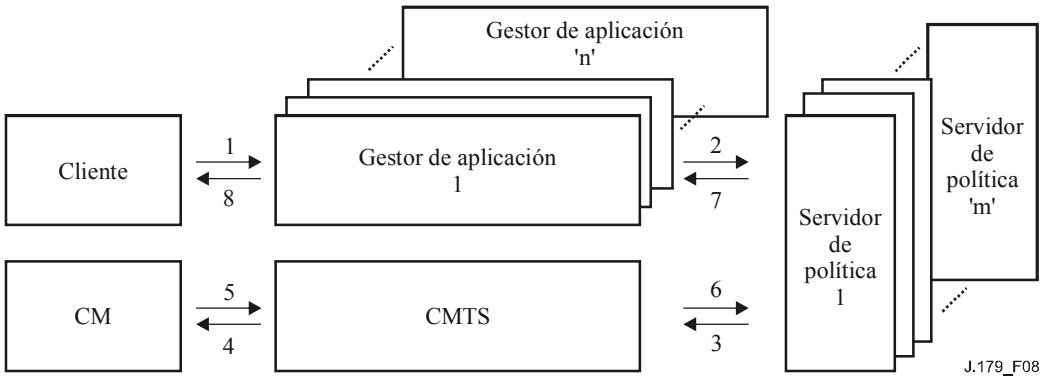


Figura 8/J.179 – Secuencia de mensajes básica

1) El cliente envía una petición de establecimiento de sesión al gestor de aplicación vía señalización de capa de aplicación. El cliente puede autenticarse a sí mismo ante el gestor de aplicación durante este paso.

2) Antes de activar la sesión, el gestor de aplicación emite un Gate-Set (en un mensaje Decisión COPS) y lo envía al servidor de política para determinar si debe permitirse que proceda la petición de establecimiento de sesión. El mensaje incluye lo siguiente:
   i) AMID.
   ii) ID de abonado.
   iii) ID de transacción.
   iv) Clasificador.
   v) Perfil de tráfico para flujo.
   vi) Especificación de puerta.

3) Tras la recepción de la petición, el servidor de política contrasta la petición con las reglas de política y si la petición es aprobada, envía un Gate-Set al CMTS. El mensaje incluye lo siguiente:
   i) AMID.
   ii) ID de abonado.
   iii) ID de transacción.
   iv) Clasificador.
   v) Perfil de tráfico para flujo (autorizado, reservado y comprometido).
   vi) Especificación de puerta.

4) El CMTS utiliza la información del clasificador y el perfil de tráfico para provocar la activación del flujo emitiendo los mensajes DSx DOCSIS apropiados.

5) El CM acusa recibo con la mensajería DSx apropiada.

6) El CMTS envía un Gate-Set-Ack al servidor de política en respuesta al mensaje Gate-Set recibido en el paso 3. El mensaje incluye lo siguiente:
   i) AMID.
   ii) ID de transacción.
   iii) ID de puerta.
   iv) ID de abonado.

7) En repuesta, el servidor de política generará un Gate-Set-Ack dirigido al AM, con el que se indica al AM que la petición de política ha sido admitida, que la petición del cliente puede proceder y que los recursos necesarios de la red subyacente han sido reservados. El mensaje incluye lo siguiente:

   i) AMID.

   ii) ID de transacción.

   iii) ID de puerta.

   iv) ID de abonado.

8) El gestor de aplicación, tras recibir el Gate-Set-Ack, informará al cliente de que el establecimiento de la sesión puede seguir su curso.

10.2 Secuencia de mensajes detallada

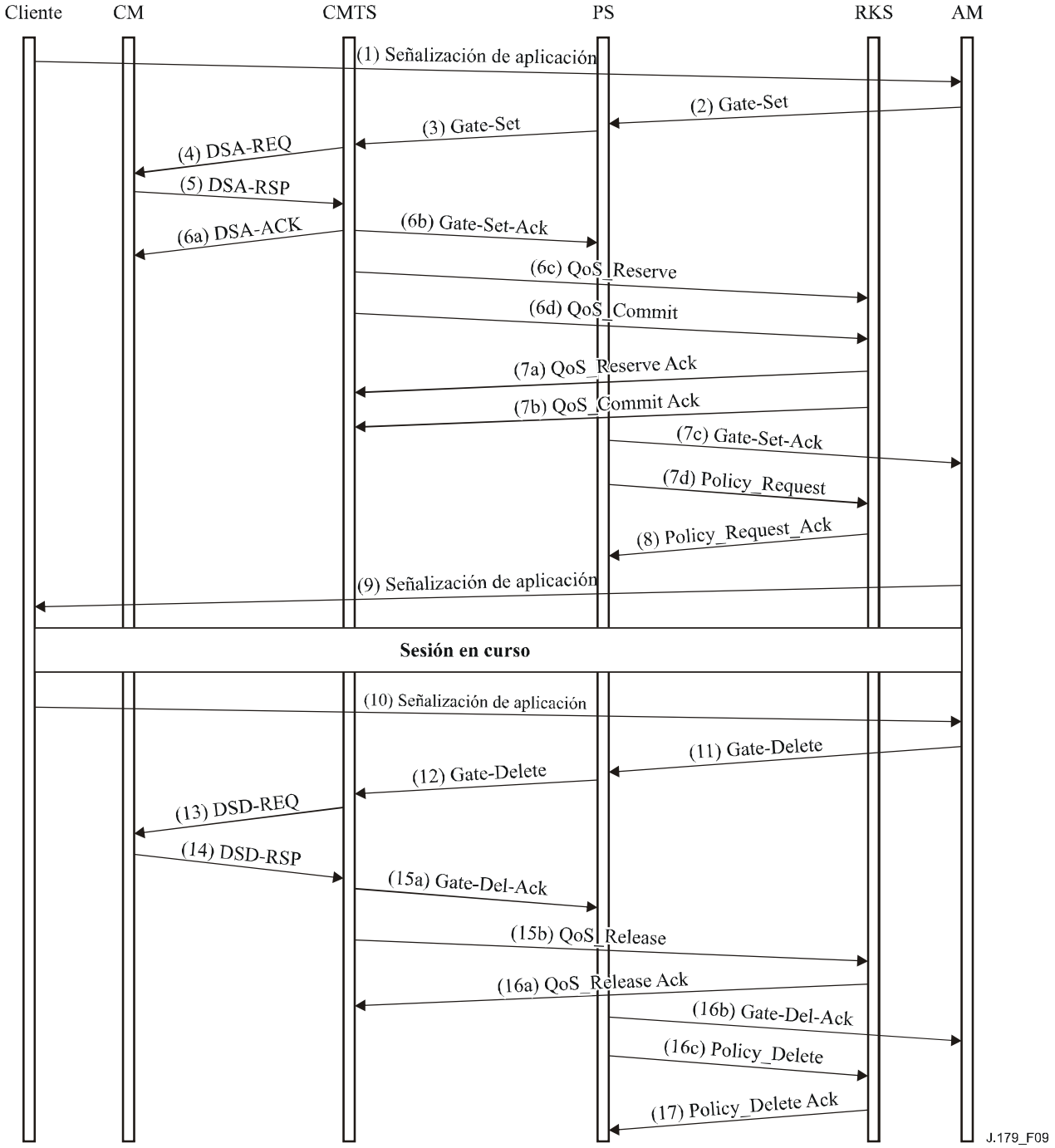


Figura 9/J.179 – Secuencia de mensajes detallada

Las páginas que siguen describen en detalle los mensajes que se intercambian en un ejemplo de sesión de multimedia IPCablecom. Los números de anchura de banda no son sino simples ejemplos y no se refieren a ningún servicio en particular. Para mayor claridad, sólo se reservan y comprometen los recursos de red de acceso en sentido ascendente. Además, las codificaciones TLV relacionadas con la BPI se han dejado fuera de los mensajes DOCSIS, para mayor claridad asimismo.

1) El cliente inicializa la sesión consultando a un gestor de aplicación sobre los recursos necesarios para utilizar la aplicación. Un ejemplo al respecto sería el caso de un videojuego basado en un programa informático, en el que se pidieran recursos para jugar en línea. Esta señalización queda fuera del alcance de la presente Recomendación.

2) Tras recibir la señalización de la aplicación procedente del cliente, el gestor de aplicación envía un Gate-Set al servidor de política, pidiendo los recursos que se necesitan para la sesión.

0		**1**	**2**	**3**
Encabezamiento COPS				
Versión 0x1	Banderas 0x0	Op-Code 0x02	Client-Type 0x800A	
Longitud del mensaje 0x00000088				
Objeto Asa COPS				
Longitud 0x0008			C-Num 0x01	C-Type 0x01
Asa 0x00001234				
Objeto Contexto COPS				
Longitud 0x0008			C-Num 0x02	C-Type 0x01
Tipo de petición (R-Type) 0x0008 (Petición de configuración)			Tipo de mensaje (M-Type) 0x0000	
Objeto Banderas de decisión COPS				
Longitud 0x0008			C-Num 0x06	C-Type 0x01
Código de instrucción 0x0001 (Instalar configuración)			Banderas 0x0000	
Encabezamiento de objeto Datos de decisión específicos del cliente COPS				
Longitud 0x00A0			C-Num 0x06	C-Type 0x04
Objeto ID de transacción de multimedia				
Longitud 0x0008			S-Num 0x01	S-Type 0x01
ID de transacción 0x9999			Instrucción de puerta 0x0004 (Gate-Set)	
Objeto AMID de multimedia				
Longitud 0x0008			S-Num 0x02	S-Type 0x01
AMID 0x00005678				
Objeto ID de abonado de multimedia				
Longitud 0x0008			S-Num 0x03	S-Type 0x01
ID de abonado 0x01010101				
Objeto GateSpec de multimedia				
Longitud 0x0010			S-Num 0x05	S-Type 0x01
Banderas 0x01		Campo DSCP/TOS 0x00	Máscara DSCP/TOS 0x00	ID de clase de sesión 0x00

0	1	2	3
Temporizador T1 0x00C8 (200 segundos)		Temporizador T2 0x012C (300 segundos)	
Temporizador T3 0x003C (60 segundos)		Temporizador T4 0x001E (30 segundos)	
Objeto FlowSpec de multimedia			
Longitud 0x0024		S-Num 0x07	S-Type 0x01
Capacidad máxima 0x07	Número de servicio 0x02	Reservado	Reservado
Capacidad máxima autorizada, reservada y comprometida en conjunto			
Velocidad de colector testigo [r] (codificado en coma flotante IEEE) 0x461C4000 (10 000 bit/s)			
Tamaño de colector testigo [b] (codificado en coma flotante IEEE) 0x43480000 (200 bytes)			
Velocidad de datos de cresta [p] (codificado en coma flotante IEEE) 0x461C4000 (10 000 bit/s)			
Unidad mínima sujeta a aplicación de política [m] 0x000000C8 (200 bytes)			
Tamaño de paquete máximo [M] 0x000000C8 (200 bytes)			
Velocidad [R] (codificado en coma flotante IEEE) 0x461C4000 (10 000 bit/s)			
Término suelto [S] 0x00000320 (800 µs)			
⋮			⋮
Objeto Clasificador de multimedia			
Longitud 0x0018		S-Num 0x06	S-Type 0x01
Reservado	ID de Protocolo 0x11 (17 UDP)	Campo DSCP/TOS 0x00	Máscara DSCP/TOS 0x00
Dirección IP de origen 0x01010101			
Dirección IP de destino 0x02020202			
Puerto de origen 0x1234		Puerto de destino 0x9876	
Prioridad 0x0040 (64)		Reservado	

3) Después de que el PS recibe el Gate-Set procedente del gestor de aplicación, comprueba si la petición está autorizada y, en caso afirmativo, envía un Gate-Set al CMTS.

0		1	2	3
Encabezamiento COPS				
Versión 0x1	Banderas 0x0	Op-Code 0x02	Client-Type 0x800A	
Longitud del mensaje 0x000000B4				
Objeto Asa COPS				
Longitud 0x0008			C-Num 0x01	C-Type 0x01
Asa 0x00005678				

0	1	2	3
Objeto Contexto COPS			
Longitud 0x0008		C-Num 0x02	C-Type 0x01
Tipo de petición (R-Type) 0x0008 (Petición de configuración)		Tipo de mensaje (M-Type) 0x0000	
Objeto Banderas de decisión COPS			
Longitud 0x0008		C-Num 0x06	C-Type 0x01
Código de instrucción 0x0001 (Instalar configuración)		Banderas 0x0000	
Encabezamiento de objeto Datos de decisión específicos del cliente COPS			
Longitud 0x00CC		C-Num 0x06	C-Type 0x04
Objeto ID de transacción de multimedia			
Longitud 0x0008		S-Num 0x01	S-Type 0x01
ID de transacción 0x0001		Instrucción de puerta 0x0004 (Gate-Set)	
Objeto AMID de multimedia			
Longitud 0x0008		S-Num 0x02	S-Type 0x01
AMID 0x00005678			
Objeto ID de abonado de multimedia			
Longitud 0x0008		S-Num 0x03	S-Type 0x01
ID de abonado 0x01010101			
Objeto GateSpec de multimedia			
Longitud 0x0010		S-Num 0x05	S-Type 0x01
Sentido 0x01	Campo DSCP/TOS 0x00	Máscara DSCP/TOS 0x00	ID de clase de sesión 0x00
Temporizador T1 0x00C8 (200 segundos)		Temporizador T2 0x012C (300 segundos)	
Temporizador T3 0x003C (60 segundos)		Temporizador T4 0x001E (30 segundos)	
Objeto FlowSpec de multimedia			
Longitud 0x0024		S-Num 0x07	S-Type 0x01
Capacidad máxima 0x07	Número de servicio 0x02	Reservado	Reservado
Capacidad máxima autorizada, reservada y comprometida en conjunto			
Velocidad de colector testigo [r] (codificado en coma flotante IEEE) 0x461C4000 (10 000 bit/s)			
Tamaño de colector testigo [b] (codificado en coma flotante IEEE) 0x43480000 (200 bytes)			
Velocidad de datos de cresta [p] (codificado en coma flotante IEEE) 0x461C4000 (10 000 bit/s)			
Unidad mínima sujeta a control de política [m] 0x000000C8 (200 bytes)			

0	1	2	3
Tamaño de paquete máximo [M] 0x000000C8 (200 bytes)			
Velocidad [R] (codificado en coma flotante IEEE) 0x461C4000 (10 000 bit/s)			
Término suelto [S] 0x00000320 (800 µs)			
⋮			⋮
Objeto Clasificador de multimedia			
Longitud 0x0018		S-Num 0x06	S-Type 0x01
Reservado	ProtocolID 0x11	Campo DSCP/TOS 0x00	Máscara DSCP/TOS 0x00
Dirección IP de origen 0x01010101			
Dirección IP de destino 0x02020202			
Puerto de origen 0x1234		Puerto de destino 0x9876	
Prioridad 0x0040 (64)		Reservado	
Objeto Información de generación de evento de multimedia			
Longitud 0x002C		S-Num 0x08	S-Type 0x01
Dirección de RKS primario 0x03030303			
Puerto de RKS primario 0x1111		Reservado	
Dirección de RKS secundario 0x04040404			
Puerto de RKS secundario 0x1111		Reservado	
BCID 0x3e4812082020202020313436302d3035303030300003db77			

4) Si el control de admisión del CMTS tiene éxito, el CMTS iniciará la reserva y el compromiso de los recursos de red de acceso enviando un DSA al módem de cable.

0	1	2	3
Encabezamiento de gestión MAC			
ID de transacción 0x0007		Flujo de servicio US 0x18	Longitud 0x29
ID de flujo de servicio 0x02	Longitud 0x04	Valor 0x0000	
Valor (cont.) 0001		ID de servicio 0x03	Longitud 0x02
Valor 0x0001		Conjunto de parámetros de QoS 0x06	Longitud 0x01
Valor 0x06 (ad.+act.)	Tipo de calendarización 0x0F	Longitud 0x01	Valor 0x06
Tamaño de UGS 0x13	Longitud 0x02	Valor 0x00E8 (232 bytes)	
Intervalo de concesión nominal 0x14	Longitud 0x04	Valor 0x0000	
Valor (cont.) 4E20 (20 000 µs)		Concesiones por intervalo 0x16	Longitud 0x01
Valor 0x01	Política de petición/ transmisión 0x10	Longitud 0x04	Valor 0x00
Valor (cont.) 00017F			Fluctuación de concesión tolerada 0x15
Longitud 0x04	Valor 0x000003		
Valor (cont.) 20 (800 µs)	Clasificador de paquetes US 0x16	Longitud 0x2B	ID de clasificador 0x02
Longitud 0x02	Valor 0x0001		ID de flujo de servicio 0x04
Longitud 0x04	Valor 0x000000		
Valor (cont.) 01	Prioridad de regla 0x05	Longitud 0x01	Valor 0x40
Estado de activación del clasificador 0x06	Longitud 0x01	Valor 0x01 (Activo)	IP Pkt Clfr0x09
Longitud 0x001A	Protocolo IP 0x02	Longitud 0x02	Valor 0x00

0	1	2	3
Value (cont.) 11 (17 UDP)	Dirección IP de origen 0x03	Longitud 0x04	Valor 0x01
Valor (cont.) 010101			Comienzo de puerto IP de origen 0x07
Longitud 0x02	Valor 0x1234		Final de puerto IP de origen 0x08
Longitud 0x02	Valor 0x1234		Comienzo de puerto IP de destino 0x09
Longitud 0x02	Valor 0x9876		Final de puerto IP de destino 0x0A
Longitud 0x02	Valor 0x9876		

5) El CM responde al CMTS con un DSA-RSP.

0	1	2	3
Encabezamiento de gestión MAC			
ID de transacción 0x0007		Código de confirmación 0x00	

6a) El CMTS completa la transacción con un DSA-ACK.

0	1	2	3
Encabezamiento de gestión MAC			
ID de transacción 0x0007		Código de confirmación 0x00	

6b) Una vez que el CMTS reciba un DSA-REP procedente de un CM confirmando una transacción exitosa, enviará un Gate-Set-Ack al servidor de política.

0		1	2	3
Encabezamiento COPS				
Versión 0x1	Banderas 0x1	Op-Code 0x03	Client-Type 0x800A	
Longitud del mensaje 0x0000003C				
Objeto Asa COPS				
Longitud 0x0008			C-Num 0x01	C-Type 0x01
Asa 0x00005678				

0	1	2	3
Objeto Tipo de informe COPS			
Longitud 0x0008		C-Num 0x12	C-Type 0x01
Tipo de informe (R-Type) 0x0001 (éxito)		Reservado	
Encabezamiento de objeto ClientSI COPS			
Longitud 0x0024		C-Num 0x09	C-Type 0x01
Objeto ID de transacción de multimedia			
Longitud 0x0008		S-Num 0x01	S-Type 0x01
ID de transacción 0x0001		Instrucción de puerta 0x0005 (Gate-Set-Ack)	
Objeto AMID de multimedia			
Longitud 0x0008		S-Num 0x02	S-Type 0x01
AMID 0x00005678			
Objeto ID de abonado de multimedia			
Longitud 0x0008		S-Num 0x03	S-Type 0x01
ID de abonado 0x01010101			
Objeto ID de puerta de multimedia			
Longitud 0x0008		S-Num 0x04	S-Type 0x01
ID de puerta 0x12345678			

6c) El CMTS enviará también un mensaje de evento QoS_Reserve para indicar al RKS que los recursos de red de acceso han sido reservados.

0	1	2	3
Encabezamiento de petición de contabilidad RADIUS			
Específico del vendedor RADIUS 0x1A	Longitud 0x54	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo (Encabezamiento de EM) 0x01	Longitud 0x4E
Versión 0x0003		BCID 0x3D48	
BCID (cont.) 120820202020203134363 02D3035303030300003DB77			
		Tipo de mensaje de evento 0x0007 (QoS_Reserve)	

0	1	2	3
Tipo de elemento 0x0002 (CMTS)		ID de elemento 0x2020202031323334	
		Huso horario 0x302D303530303030	
		Número de secuencia 0x0000	
Número de secuencia (cont.) 0001		Hora de evento 0x3230	
Hora de evento (cont.) 3033313230363030303030302E303030			
Estatus 0x00000000			
Prioridad 0x80 (128)	Cuenta de atributos 0x0004		Objeto Evento 0x00
Específico del vendedor RADIUS 0x1A	Longitud 0x5C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x20	Longitud 0x56
QoS_Descriptor 0x0003FFFD0000000000000000000000000000000000000000600004e2000000320000000001000000e8			
00000000000000000000BE40000004000000000000005F20000017F000186A0000007D000FF0000			
00000000			

0	1	2	3
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x1E	Longitud 0x06
ID de campo estatus 0x00000001			
Específico del vendedor RADIUS 0x1A	Longitud 0x0A	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x32	Longitud 0x04
Sentido del flujo 0x0001 (ascendente)		Específico del vendedor RADIUS 0x1A	Longitud 0x0A
ID de vendedor 0x0000118B			
Tipo 0x37	Longitud 0x04	Element_Requesting_QoS 0x0001 (Servidor de política)	

6d) Inmediatamente después de enviar el mensaje de evento QoS_Reserve al RKS, el CMTS enviará el mensaje de evento QoS_Commit al RKS. Esto se debe a que los recursos de red de acceso se reservan y comprometen en un paso.

0	1	2	3
Encabezamiento de petición de contabilidad RADIUS			
Específico del vendedor RADIUS 0x1A	Longitud 0x54	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo (Encabezamiento de EM) 0x01	Longitud 0x4E
Versión 0x0003		BCID 0x3E48	
BCID (cont.) 120820202020203134363 02D3035303030300003DB77			
		Tipo de mensaje de evento 0x0013 (QoS_Commit)	
Tipo de elemento 0x0002 (CMTS)		ID de elemento 0x2020202031323334	
		Huso horario 0x302d303530303030	
		Número de secuencia 0x0000	

0	1	2	3
Número de secuencia (cont.) 0002		Hora de evento 0x3230	
Número de secuencia (cont.) 3033313230363030303030302E303030			
Estatus 0x00000000			
Prioridad 0x80 (128)	Cuenta de atributos 0x0003		Objeto Evento 0x00
Específico del vendedor RADIUS 0x1A	Longitud 0x5C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x20	Longitud 0x56
QoS_Descriptor 0x0003FFFD0000000000000000000000000000000000000000600004e2000000320000000001000000e8			
00000000000000000000BE40000004000000000000005F20000017F000186A0000007D000FF0000			
00000000			
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x1E	Longitud 0x06

0	1	2	3
ID de campo estatus 0x00000001			
Específico del vendedor RADIUS 0x1A	Longitud 0x0A	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x32	Longitud 0x04
Sentido del flujo 0x0001 (ascendente)			

7a) Después de recibir y registrar el mensaje de evento QoS_Reserve, el RKS acusa recibo del mismo.

0	1	2	3
Encabezamiento de respuesta de contabilidad RADIUS			

7b) Después de recibir y registrar el mensaje de evento QoS_Commit, el RKS acusa recibo del mismo.

0	1	2	3
Encabezamiento de respuesta de contabilidad RADIUS			

7c) Como resultado de la recepción de un Gate-Set-Ack procedente del CMTS, el servidor de política enviará un Gate-Set-Ack al gestor de aplicación para completar la transacción.

0		1	2	3
Encabezamiento COPS				
Versión 0x1	Banderas 0x1	Op-Code 0x03	Client-Type 0x800A	
Longitud del mensaje 0x0000003C				
Objeto Asa COPS				
Longitud 0x0008			C-Num 0x01	C-Type 0x01
Asa 0x00001234				
Objeto Tipo de informe COPS				
Longitud 0x0008			C-Num 0x12	C-Type 0x01
Tipo de informe (R-Type) 0x0001 (éxito)			Reservado	
Encabezamiento de objeto ClientSI COPS				
Longitud 0x0024			C-Num 0x09	C-Type 0x01

0	1	2	3
Objeto ID de transacción de multimedia			
Longitud 0x0008		S-Num 0x01	S-Type 0x01
ID de transacción 0x9999		Instrucción de puerta 0x0005	
Objeto AMID de multimedia			
Longitud 0x0008		S-Num 0x02	S-Type 0x01
AMID 0x00005678			
Objeto ID de abonado de multimedia			
Longitud 0x0008		S-Num 0x03	S-Type 0x01
ID de abonado 0x01010101			
Objeto ID de puerta de multimedia			
Longitud 0x0008		S-Num 0x04	S-Type 0x01
ID de puerta 0x12345678			

7d) El servidor de política enviará también un mensaje de evento Policy_Request al RKS para el seguimiento de la petición de política y el resultado correspondiente.

0	1	2	3
Encabezamiento de petición de contabilidad RADIUS			
Específico del vendedor RADIUS 0x1A	Longitud 0x54	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo (Encabezamiento de EM) 0x01	Longitud 0x4E
Versión 0x0001		BCID 0x3E48	
BCID (cont.) 120820202020203134363 02D3035303030300003DB77			
		Tipo de mensaje de evento 0x0015 (Policy_Request)	

0	1	2	3
Tipo de elemento 0x0004 (Servidor de política)		ID de elemento 0x2020202035363738	
		Huso horario 0x302E303530303030	
		Número de secuencia 0x0000	
Número de secuencia (cont.) 0001		Hora de evento 0x3230	
Hora de enveto (cont.) 3033313230363030303030302E323130			
Estatus 0x00000000			
Prioridad 0x80 (128)	Cuenta de atributos 0x0004		Objeto Evento 0x00
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x3D	Longitud 0x06
ID de gestor de aplicación 0x00005678			
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x34	Longitud 0x06
ID de abonado 0x01010101			
Específico del vendedor RADIUS 0x1A	Longitud 0x0A	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x3C	Longitud 0x04
Estatus de decisión de tipo político 0x0001 (Política aprobada)		Específico del vendedor RADIUS 0x1A	Longitud 0x1C
ID de vendedor 0x0000118B			
Tipo 0x31	Longitud 0x16	FEID 0x0000	
FEID (cont.) 00000000000000005061636B65744361626C65			

8) Después de recibir y registrar el mensaje de evento Policy_Request, el RKS acusa recibo del mensaje.

0	1	2	3
Encabezamiento de respuesta de contabilidad RADIUS			

9) El gestor de aplicación responderá al cliente para informarle de que ya puede jugar. Esta señalización queda fuera del alcance de la presente Recomendación.

10) Cuando el cliente haya terminado con la aplicación, se lo notificará al gestor de aplicación. Esta señalización queda fuera del alcance de la presente Recomendación.

11) El gestor de aplicación terminará la sesión enviando un Gate-Delete al servidor de política.

0		1	2	3
Encabezamiento COPS				
Versión 0x1	Banderas 0x0	Op-Code 0x02	Client-Type 0x800A	
Longitud del mensaje 0x00000044				
Objeto Asa COPS				
Longitud 0x0008			C-Num 0x01	C-Type 0x01
Asa 0x00001234				
Objeto Contexto COPS				
Longitud 0x0008			C-Num 0x02	C-Type 0x01
Tipo de petición (R-Type) 0x0008 (Petición de configuración)			Tipo de mensaje (M-Type) 0x0000	
Objeto Banderas de decisión COPS				
Longitud 0x0008			C-Num 0x06	C-Type 0x01
Código de instrucción 0x0001 (Instalar configuración)			Banderas 0x0000	
Encabezamiento de objeto Datos de decisión específica del cliente COPS				
Longitud 0x0014			C-Num 0x09	C-Type 0x04
Objeto ID de transacción de multimedia				
Longitud 0x0008			S-Num 0x01	S-Type 0x01
ID de transacción 0x9998			Instrucción de puerta 0x000A (Gate-Delete)	
Objeto AMID de multimedia				
Longitud 0x0008			S-Num 0x02	S-Type 0x01
AMID 0x00005678				
Objeto ID de abonado de multimedia				
Longitud 0x0008			S-Num 0x03	S-Type 0x01

0	1	2	3
ID de abonado 0x01010101			
Objeto ID de puerta de multimedia			
Longitud 0x0008		S-Num 0x04	S-Type 0x01
ID de puerta 0x12345678			

12) El servidor de política ordenará al CMTS que elimine la sesión enviando un mensaje Gate-Delete.

0		1	2	3
Encabezamiento COPS				
Versión 0x1	Banderas 0x0	Op-Code 0x02	Client-Type 0x800A	
Longitud del mensaje 0x00000044				
Objeto Asa COPS				
Longitud 0x0008			C-Num 0x01	C-Type 0x01
Asa 0x00005678				
Objeto Contexto COPS				
Longitud 0x0008			C-Num 0x02	C-Type 0x01
Tipo de petición (R-Type) 0x0008 (Petición de configuración)			Tipo de mensaje (M-Type) 0x0000	
Objeto Banderas de decisión COPS				
Longitud 0x0008			C-Num 0x06	C-Type 0x01
Código de instrucción 0x0001 (Instalar configuración)			Banderas 0x0000	
Encabezamiento de objeto Datos de decisión específicos del cliente COPS				
Longitud 0x0014			C-Num 0x09	C-Type 0x01
Objeto ID de transacción de multimedia				
Longitud 0x0008			S-Num 0x01	S-Type 0x01
ID de transacción 0x0002			Instrucción de puerta 0x000A (Gate-Delete)	
Objeto AMID de multimedia				
Longitud 0x0008			S-Num 0x02	S-Type 0x01
AMID 0x00005678				
Objeto ID de abonado de multimedia				
Longitud 0x0008			S-Num 0x03	S-Type 0x01

0	1	2	3
ID de abonado 0x01010101			
Objeto ID de puerta de multimedia			
Longitud 0x0008		S-Num 0x04	S-Type 0x01
ID de puerta 0x12345678			

13) El CMTS eliminará los recursos de red de acceso enviando un DSD-REQ al CM.

0	1	2	3
Encabezamiento de gestión MAC			
ID de transacción 0x0008		Reservado	
ID de campo estatus 0x00000001			

14) El CM confirmará su conocimiento de la eliminación de la sesión con un DSD-RSP.

0	1	2	3
Encabezamiento de gestión MAC			
ID de transacción 0x0008		Código de confirmación 0x00	Reservado

15a) El CMTS completará la transacción Gate-Control con un mensaje Gate-Delete-Ack.

0	1	2	3
Encabezamiento COPS			
Versión 0x1	Banderas 0x1	Op-Code 0x03	Client-Type 0x800A
Longitud del mensaje 0x00000034			
Objeto Asa COPS			
Longitud 0x0008		C-Num 0x01	C-Type 0x01
Asa 0x00005678			
Objeto Tipo de informe COPS			
Longitud 0x0008		C-Num 0x12	C-Type 0x01
Tipo de informe (R-Type) 0x0001		Reservado	

0	1	2	3
Encabezamiento de objeto ClientSI COPS			
Longitud 0x001C		C-Num 0x09	C-Type 0x01
Objeto ID de transacción de multimedia			
Longitud 0x0008		S-Num 0x01	S-Type 0x01
ID de transacción 0x0002		Instrucción de puerta 0x000B (Gate-Delete-Ack)	
Objeto AMID de multimedia			
Longitud 0x0008		S-Num 0x02	S-Type 0x01
AMID 0x00005678			
Objeto ID de puerta de multimedia			
Longitud 0x0008		S-Num 0x04	S-Type 0x01
ID de puerta 0x12345678			

15b) Además, tras la recepción del DSD-RSP, el CMTS informará al RKS de que se han liberado los recursos de acceso de red enviando un QoS_Release.

0	1	2	3
Encabezamiento de petición de contabilidad RADIUS			
Específico del vendedor RADIUS 0x1A	Longitud 0x54	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo (encabezamiento de EM) 0x01	Longitud 0x4E
Versión 0x0001		BCID 0x3E48	
BCID (cont.) 120820202020203134363 02D3035303030300003DB77			
		Tipo de mensaje de evento 0x0008 (QoS_Release)	
Tipo de elemento 0x0002 (CMTS)		ID de elemento 0x2020202031323334	
		Huso horario 0x302D303530303030	
		Número de secuencia 0x0000	

0	1	2	3
Número de secuencia (cont.) 0003		Hora de evento 0x3230	
Hora de evento (cont.) 3032313230363030303030302E333030			
Estatus 0x00000000			
Prioridad 0x80 (128)	Cuenta de atributos 0x0005		Objeto Evento 0x00
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x1E	Longitud 0x06
ID de campo estatus 0x00000001			
Específico del vendedor RADIUS 0x1A	Longitud 0x0A	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x32	Longitud 0x04
Sentido del flujo 0x0001 (ascendente)		Específico del vendedor RADIUS 0x1A	Longitud 0x0A
ID de vendedor 0x0000118B			
Tipo 0x38	Longitud 0x04	QoS_Release_Reason 0x0001 (Puerta cerrada por PS)	
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x36	Longitud 0x06
Información de utilización de QoS 0x77777777 (bytes)			
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x3F	Longitud 0x06
Información de tiempo de QoS 0x77777777 (segundos)			

16a) Después de recibir y registrar el mensaje de evento QoS_Release, el RKS acusa recibo del mismo.

0	1	2	3
Encabezamiento de respuesta de contabilidad RADIUS			

16b) Después de recibir el Gate-Delete-Ack procedente del CMTS, el servidor de política enviará un Gate-Delete-Ack para completar la transacción Gate-Control.

0		1	2	3
Encabezamiento COPS				
Versión 0x1	Banderas 0x1	Op-Code 0x03	Client-Type 0x800A	
Longitud del mensaje 0x00000034				
Objeto Asa COPS				
Longitud 0x0008			C-Num 0x01	C-Type 0x01
Asa 0x00001234				
Objeto Tipo de informe COPS				
Longitud 0x0008			C-Num 0x12	C-Type 0x01
Tipo de informe (R-Type) 0x0001 (éxito)			Reservado	
Encabezamiento de objeto ClientSI COPS				
Longitud 0x001C			C-Num 0x09	C-Type 0x01
Objeto ID de transacción de multimedia				
Longitud 0x0008			S-Num 0x01	S-Type 0x01
ID de transacción 0x9998			Instrucción de puerta 0x000B (Gate-Delete-Ack)	
Objeto AMID de multimedia				
Longitud 0x0008			S-Num 0x02	S-Type 0x01
AMID 0x00005678				
Objeto ID de puerta de multimedia				
Longitud 0x0008			S-Num 0x04	S-Type 0x01
ID de puerta 0x12345678				

16c) El servidor de política envía un mensaje de evento Policy_Delete al RKS para completar todo el proceso.

0	1	2	3
Encabezamiento de petición de contabilidad RADIUS			
Específico del vendedor RADIUS 0x1A	Longitud 0x54	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo (Encabezamiento de EM) 0x01	Longitud 0x4E

0	1	2	3
Versión 0x0001		BCID 0x3E48	
BCID (cont.) 120820202020203134363 02D303530303030003DB77			
		Tipo de mensaje de evento 0x0016 (Policy_Delete)	
Tipo de elemento 0x0004 (Servidor de política)		ID de elemento 0x2020202035363738	
		Huso horario 0x302D303530303030	
		Número de secuencia 0x0000	
Número de secuencia (cont.) 0002		Hora de evento 0x3230	
Hora de evento (cont.) 303231323036303030303030 2E343030			
Estatus 0x00000000			
Prioridad 0x80	Cuenta de atributos 0x0004		Objeto Evento 0x00
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x3D	Longitud 0x06
ID de gestor de aplicación 0x00005678			
Específico del vendedor RADIUS 0x1A	Longitud 0x0C	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x34	Longitud 0x06
ID de abonado 0x01010101			
Específico del vendedor RADIUS 0x1A	Longitud 0x0A	ID de vendedor 0x0000	
ID de vendedor (cont.) 118B		Tipo 0x3A	Longitud 0x04
Motivo de política denegada 0x0001 (Petición de gestor de aplicación)		Específico del vendedor RADIUS 0x1A	Longitud 0x1C

0	1	2	3
ID de vendedor 0x0000118B			
Tipo 0x31	Longitud 0x16	FEID 0x0000	
FEID (cont.) 00000000000000005061636B65744361626C65			

17) Después de recibir y registrar el mensaje de evento Policy_Delete, el RKS acusa recibo del mensaje.

0	1	2	3
Encabezamiento de respuesta de contabilidad RADIUS			

11 Cuestiones que quedan en estudio

Se han identificado como cuestiones que deben ser objeto de un estudio ulterior las siguientes.

- Requisitos del tratamiento de errores (es decir, obligación de códigos de error específicos para condiciones específicas).
- Encaminamiento de mensajes Control por puerta dentro del marco de multimedia.
- Requisitos de la sincronización de estados (es decir, granularidad, alcance, frecuencia, etc.) y mecanismo de protocolo.
- Soporte del protocolo para estrategias de cambio por fallo y redundancia. Además, manipulación de las puertas en el caso de una conexión COPS fallida.
- Formato de las reglas del servidor de política y mecanismo de provisionamiento: provisión de XML DTD específico de multimedia al CMS.
- Soporte de la supresión del encabezamiento de cabida útil (PHS, *payload header suppression*).
- Entrega del mensaje Control por puerta en caso de conexiones fallidas (en la actualidad, estos mensajes son suprimidos).

Apéndice I

Información básica

I.1 Introducción

El presente apéndice describe la arquitectura que proporciona una plataforma basada en IP para el soporte de diversas aplicaciones y diversos servicios multimedia que requieren tratamiento de QoS por redes de acceso al módem de cable de la tecnología CableModem. Dicha arquitectura define los componentes funcionales y las interfaces de protocolo que permitirán a cada operador de cable entregar los servicios multimedia con QoS mejorada que satisfagan sus requisitos comerciales particulares.

Puesto que la arquitectura es agnóstica respecto a los detalles a nivel de aplicación de ofertas concretas de multimedia, la provisión específica, la señalización y las funciones del sistema de soporte de operaciones (OSS, *operations support system*) requeridos para proporcionar un determinado servicio quedan fuera del alcance de la misma. La atención de los multimedia IPCablecom se centra más bien en la entrega de una QoS fiable por la red de acceso, teniendo en cuenta de manera específica las cuestiones técnicas relativas a la autorización de políticas, señalización de QoS, contabilidad de recursos y seguridad.

I.1.1 Visión de conjunto de IPCablecom

El proyecto IPCablecom tiene por objeto definir especificaciones de interfaces utilizadas por la comunidad de vendedores para el desarrollo de equipos interoperables capaces de proporcionar servicios multimedia de voz, vídeo y otros de alta velocidad basados en IP por sistemas de cable híbridos de fibra y coaxiales (HFC) que se atengan a las Recomendaciones sobre redes de acceso de banda ancha de CableModem.

El servicio de voz por IP (VoIP) fue el primero de esos servicios identificados para su entrega por la plataforma IPCablecom. El conjunto actual de Recomendaciones sobre IPCablecom, al que se hace referencia de forma colectiva como IPCablecom-T, define una arquitectura IPCablecom optimizada para la entrega de servicios VoIP residenciales. Véase la Rec. UIT-T J.160.

I.1.2 Motivación de los multimedia IPCablecom

Al igual que la VoIP, las aplicaciones multimedia más populares (por ejemplo, juegos en línea, medios de flujo continuo y comunicación vídeo en tiempo real) son sensibles al retardo de la transmisión por la red. Además, a medida que surjan aplicaciones nuevas diseñadas para aprovechar las ventajas de las redes de banda ancha, dichas aplicaciones presentarán también requisitos de latencia y anchura de banda exclusiva.

En la actualidad, los clientes de banda ancha reciben servicios multimedia vía entrega de datos de mejor esfuerzo. Esto da lugar en la práctica a una situación en línea incoherente con una calidad que varía dependiendo de la disponibilidad de banda ancha y de la congestión que se produzca en la red. Una red capaz de reservar recursos y entregar anchura de banda a la demanda según impongan los requisitos de los servicios estará en condiciones de proporcionar a sus clientes una amplia gama de servicios nuevos.

Para abordar estas necesidades en el caso de los servicios VoIP, IPCablecom define actualmente mecanismos de señalización de calidad de servicio dinámica (DQoS) que permiten a las aplicaciones de voz pedir y obtener anchura de banda de la capa enlace de datos de CableModem. El presente marco DQoS soporta además el establecimiento seguro de sesiones mediante la autenticación y la autorización del punto de extremo y un modelo de seguimiento de la utilización basado en QoS. Teniendo en cuenta estas capacidades medulares, se puede afirmar que la arquitectura IPCablecom está bien situada por lo que se refiere al soporte de aplicaciones y servicios con QoS mejorada existentes y futuros, más allá de la telefonía.

El objetivo principal de los multimedia IPCablecom es definir el marco arquitectural fundamental requerido para el soporte de aplicaciones multimedia basadas en QoS. La parte nuclear de este marco son los mecanismos de calidad de servicio definidos en las especificaciones relativas a la DQoS de CableModem e IPCablecom. La compleción exitosa de esta iniciativa proporcionará un fundamento técnico sólido que permitiría avanzar en el soporte de servicios multimedia específicos.

I.2 Objetivos y alcance de los multimedia IPCablecom

El objetivo principal de los multimedia IPCablecom es el desarrollo de una arquitectura polivalente que:

- Dé soporte a una amplia gama de servicios con QoS habilitada, más allá del servicio de voz.
- Se base en los mecanismos existentes definidos en las Recomendaciones IPCablecom-T y sobre la tecnología CableModem.
- Requiera un conjunto mínimo de extensiones con relación a IPCablecom.
- Reduzca la complejidad del desarrollo eliminando requisitos específicos de la telefonía donde no sean aplicables (por ejemplo, interconexión con la RTPC, vigilancia electrónica, modelos de facturación de telefonía, etc.)
- Coexista con la arquitectura IPCablecom-T de tal manera que:
  - los requisitos de los multimedia IPCablecom sean suficientes para soportar una plataforma de entrega de servicios multimedia basados en QoS;
  - se puedan añadir requisitos de los multimedia IPCablecom a componentes funcionales de IPCablecom pertinentes ya existentes;
  - se puedan añadir requisitos de IPCablecom-T a componentes funcionales de los multimedia IPCablecom pertinentes.
- Dé soporte a los MTA IPCablecom como dispositivos "Client Type 2" de (definidos en) la arquitectura de multimedia IPCablecom.
- Interactúe con las arquitecturas IPCable2Home (Rec. UIT-T J.191) y CableModem (Recs. UIT-T J.112 y J.122).

En esta cláusula se describen los requisitos identificados, cuyo cumplimiento es preciso para alcanzar los objetivos anteriores, y se expone a grandes rasgos el alcance del trabajo que tendrá que abordar la arquitectura.

I.2.1 Requisitos

Esta arquitectura describe la interacción de diversos elementos de red, incluidos los dispositivos de cliente, gestores de aplicación, servidores de política, CMTS y módems de cable. Esos elementos de red se definen formalmente en la cláusula relativa al marco multimedia de este apéndice. No obstante, se han establecido hipótesis específicas a propósito de la autoridad de gestión y las relaciones fiduciarias en las que intervienen algunos de esos elementos de red, y esas hipótesis se presentan más adelante como requisitos de multimedia IPCablecom. En esta cláusula se incluyen además los requisitos de alto nivel relativos a la señalización de QoS, gestión de recursos, mensajería de eventos y seguridad.

Los multimedia IPCablecom son agnósticos a propósito del protocolo de señalización de aplicación, en lo que se refiere a la interacción entre dispositivo de cliente y gestor de aplicación. Se entiende que el dispositivo de cliente y el gestor de aplicación pueden soportar diversos protocolos de aplicación y señalización (por ejemplo, HTTP, SIP, H.323, señalización de llamada distribuida (DCS, *distributed call signalling*), establecimiento de comunicación normal (NCS, *normal call setup*), etc.).

Los dispositivos de cliente de la arquitectura de multimedia IPCablecom:

1) residen directamente en la red de acceso del operador, o en el hogar;
2) pueden ser autónomos o contener un módem de cable incorporado; y
3) se consideran elementos de red no fiduciarios y, por tal motivo, es posible que el operador requiera alguna forma de autenticación del usuario, la aplicación o la mensajería de la aplicación.

Los gestores de aplicación de la arquitectura de multimedia IPCablecom:

1) residen en la red gestionada por el operador;
2) son gestionados por el operador; y
3) se encargan de asegurar que los clientes que piden un servicio de la red del operador están autorizados para recibir ese servicio.

Los servidores de política de la arquitectura de multimedia IPCablecom:

1) residen en la red gestionada por el operador;
2) son gestionados por el operador; y
3) se encargan de hacer que las decisiones de tipo político relacionadas con la QoS se basen en reglas de política definidas por el operador.

Los CMTS de la arquitectura de multimedia IPCablecom son responsables de la aplicación de las decisiones de tipo político relacionadas con la QoS.

Requisitos de señalización de QoS y gestión de recursos

- Se deben definir mecanismos de petición de recurso dinámicos, incluyendo:
  - el acceso a todos los modelos de calendarización de la QoS de la tecnología CableModem;
  - las peticiones de recurso con limitación de tiempo;
  - las peticiones de recurso con limitación de volumen.
- Se deben soportar los modelos de reserva de recurso monofásicos y bifásicos.
- Se deben soportar reservas unidireccionales; se deberían soportar reservas bidireccionales.
- Los gestores de aplicación pueden iniciar peticiones de reserva de QoS en nombre de dispositivos de cliente.
- La arquitectura debe proporcionar una manera de detectar fallos de cliente y/o servidor y de recuperar los recursos asociados.

Requisitos de recogida de información de mensajes de evento

- Se debe definir un amplio conjunto de mensajes de evento para el seguimiento de la utilización de los recursos flujo por flujo, incluyendo:
  - eventos de política que indiquen una petición de recurso de red de acceso, sujetos a reglas de política definidas por el operador;
  - eventos de política que indiquen la liberación de recursos de red de acceso;
  - eventos de QoS que indiquen la reserva, el compromiso y la liberación de recursos QoS;
  - eventos(s) que soporta(n) la utilización de recursos, flujo por flujo, basándose en el volumen (conteo de paquetes con medición).
- Los mensajes deberán contener la información siguiente:
  - origen de la petición (por ejemplo, abonado o proveedor de servicio);
  - características de los recursos pedidos;

– decisión sobre la autorización de la política.

Requisitos de seguridad

- Es preciso contar con seguridad, que debe ser definida para las interfaces pertinentes.
- Es posible que los clientes que inicien la señalización de QoS requieran alguna forma de autenticación del usuario o la aplicación.

I.2.2 Alcance

Los elementos que siguen definen el alcance de la presente fase inicial de la iniciativa multimedia IPCablecom:

- La arquitectura deberá abordar el tema de los elementos de red que residen:
  1) en la red de acceso; o
  2) en una red IP gestionada por un solo operador.
- La arquitectura deberá definir los protocolos y las interfaces que se necesitan para soportar la autorización de políticas, el control de admisión de QoS, la contabilidad de recursos y los mecanismos de seguridad.
- La arquitectura no deberá referirse a temas específicos de la aplicación (por ejemplo, prestación de servicios, señalización, facturación, etc.).
- La arquitectura no se ocupará de la provisión ni de los requisitos OSS de los elementos de red multimedia IPCablecom.
- La arquitectura centrará su atención en la gestión de QoS entre el CMTS y el CM.
- La arquitectura no impedirá la entrega de servicios de multidifusión, incluso aunque no haya de manera explícita consideraciones relativas a la multidifusión.
- La arquitectura no se ocupará por ahora de los requisitos relativos al tránsito de la traducción de dirección de red (NAT, *network address translation*) ni a la interoperabilidad.
- La arquitectura no deberá definir en la fase actual requisitos de QoS de extremo a extremo.
- La arquitectura proporcionará soporte para el "cliente de tipo 1" y el "escenario 1" (definidos) en la fase actual. A efectos de integridad y en previsión de una futura elaboración, el presente apéndice describe los tres tipos de cliente y los tres escenarios de servicio.
- La arquitectura no proporcionará en la fase actual ningún descubrimiento de topología dinámica (es decir, la revelación dinámica de las relaciones entre gestores de aplicación, servidores de política, CMTS, RKS, etc.).
- La arquitectura no deberá referirse a la autenticación del cliente por el gestor de aplicación.
- La arquitectura no se ocupará de los mecanismos específicos mediante los cuales el servidor de política obtiene y gestiona reglas de política.
- La arquitectura no soportará la recogida de eventos de aplicación o específicos del servicio que se vayan a incorporar en la pista de auditoría de la utilización de recursos.

I.3 Marco de los multimedia IPCablecom

Para facilitar la entrega de aplicaciones multimedia de banda ancha de calidad que requieren garantías de QoS, el marco de los multimedia ofrece una funcionalidad QoS polivalente basada en mecanismos definidos en las especificaciones de IPCablecom-T medulares. En apoyo de este objetivo, se han identificado y perfilado varios elementos clave de red. La figura I.1 presenta los componentes de los multimedia IPCablecom que se hallan en la red IP gestionada por el operador.

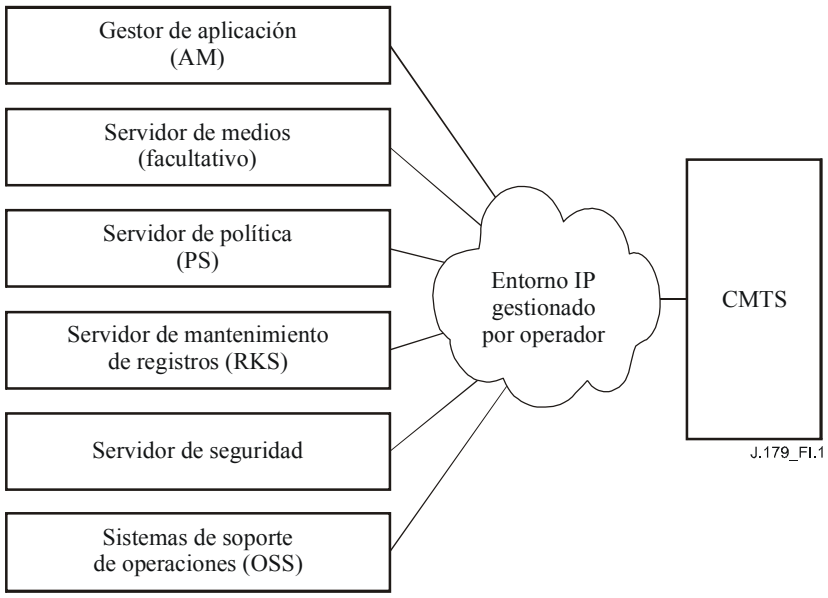


Figura I.1/J.179 – Elementos de red multimedia de operador

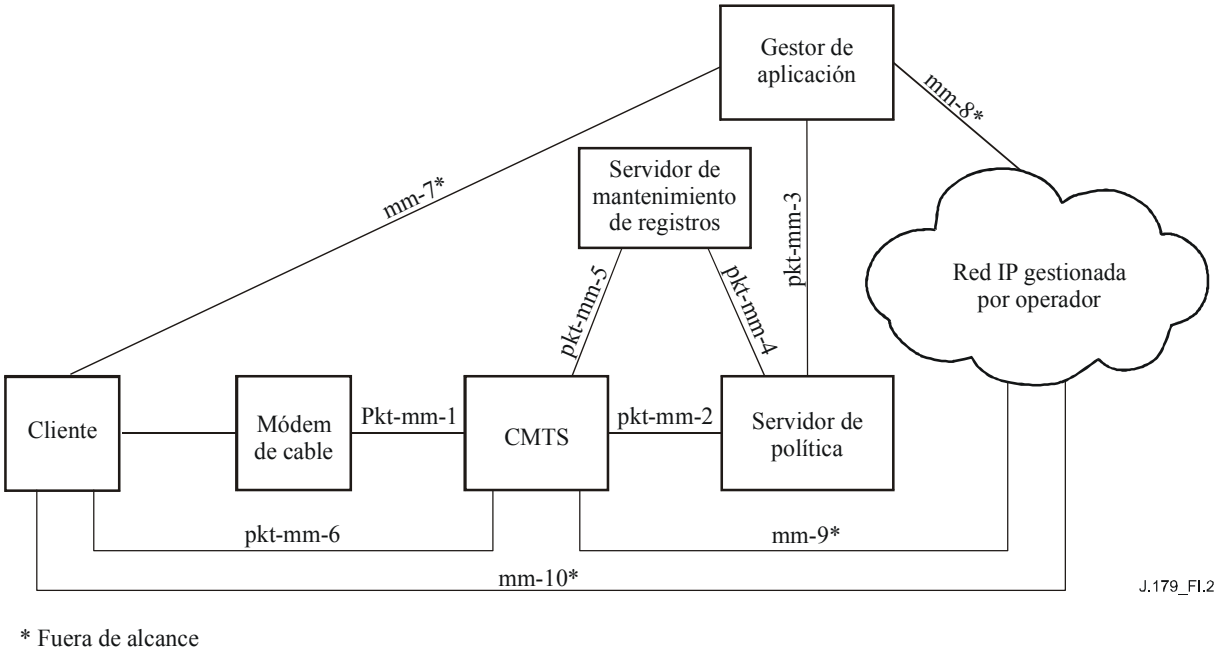
Además de disponer de un CMTS que facilita capacidades QoS basadas en parámetros, la arquitectura de red multimedia de operador consta de un conjunto de computadores (conocido como finca de computadores o rancho de computadores (*server farm*)) que puede dividirse en las áreas siguientes:

- Un gestor de aplicación y un servidor de medios (facultativo) que alojan una aplicación con QoS habilitada.
- Un marco de aplicación de políticas que proporciona control de autorización y admisión de QoS como soporte de la gestión de recursos de la red flujo por flujo.
- Un subsistema de mensajería de eventos utilizado para supervisar y registrar la información relativa a la utilización de los recursos.

También se pueden incluir en la configuración de la red multimedia de operador sistemas de soporte de operaciones para efectuar funciones de configuración, gestión de red y supervisión técnica, si bien estos elementos quedan fuera del alcance de la arquitectura actual.

I.3.1 Modelo de referencia de la arquitectura de multimedia IPCablecom

Además de los elementos que se hallan en la red del extremo de cabecera del operador, se ha definido un cierto número de dispositivos de cliente situados en las instalaciones del cliente para completar el modelo. La figura I.2 muestra el marco arquitectural de multimedia IPCablecom e identifica interfaces clave entre los componentes. Esas interfaces se han rotulado con identificadores a los que se hará referencia en el análisis posterior.



* Fuera de alcance

Figura I.2/J.179 – Marco arquitectural de multimedia IPCablecom

En esta arquitectura, los clientes pueden soportar o no el marco de los multimedia IPCablecom. Los clientes que soportan el marco y sus mecanismos de señalización de QoS explícitamente emiten peticiones de recurso de red en su propio nombre, que son autorizadas en los extremos de cabecera por el servidor de política. Las peticiones de recurso de red de los clientes que no soportan los mecanismos de señalización de QoS son formuladas en su nombre, mediante apoderado, por un gestor de aplicación con el que interactúan.

Con independencia del método de señalización de QoS, las peticiones de recurso de red de acceso están siempre sujetas al control de política, aplicado por el sistema de terminación de módem de cable (CMTS, *cable modem termination system*) que sirve a modo de punto de imposición de la política (PEP) y se define en el servidor de política (PS), que actúa como un punto de decisión de la política (PDP).

- Las decisiones de tipo político pueden ser extraídas (*pulled*) del servidor de política por el CMTS. En este caso, el CMTS formula normalmente una petición de política como resultado de una petición no autorizada entonces, aunque conforme, de recursos QoS. Dependiendo de la decisión resultante, la petición de QoS original es atendida o rechazada.
- Alternativamente, las decisiones de tipo político pueden ser empujadas (*pushed*) hacia el CMTS por el servidor de política. En este caso, el servidor de política instalará una decisión de tipo político antes que una petición de recurso QoS basada en una petición de política procedente de un gestor de aplicación. El gestor de aplicación genera esa petición en base a la interacción del cliente (mediante algún mecanismo de señalización no especificado).

Tanto el servidor de política como el CMTS generan mensajes de evento para el seguimiento de las peticiones y la utilización de QoS. Dichos mensajes son enviados al servidor de mantenimiento de servicios (RKS), en donde se utilizan a efectos de facturación o de otras aplicaciones de contabilidad.

El cuadro I.1 presenta de forma resumida las interfaces expuestas en la figura I.2. Las interfaces definidas por la presente Recomendación se etiquetan con "pkt-mm-x", mientras que las otras interfaces, que se incluyen a efectos de integridad, se etiquetan con "mm-x".

Cuadro I.1/J.179 – Interfaces de multimedia IPCablecom

Interfaz	Descripción	Notas
pkt-mm-1	CMTS – CM	El CM puede pedir QoS del CMTS vía señalización DSx de CableModem. Alternativamente, el CMTS puede indicar al módem de cable (CM) que establezca, deshaga o cambie un flujo de servicio CableModem para cumplimentar una petición de QoS, de nuevo vía señalización DSx.
pkt-mm-2	PS – CMTS	Esta interfaz es fundamental en el marco de gestión de políticas. Controla las decisiones de tipo político, que pueden ser: a) empujadas por el servidor de política (PS) hacia el CMTS; o b) extraídas del PS por el CMTS. La interfaz permite además formular peticiones de QoS, mediante apoderado, en nombre de un cliente. En algunos escenarios, esta interfaz puede ser utilizada también para informar al PS cuando los recursos de QoS se queden inactivos.
pkt-mm-3	AM – PS	El gestor de aplicación (AM) puede pedir que el PS instale una decisión de tipo político en el CMTS. Además, el AM puede pedir también que el PS formule peticiones de QoS, mediante apoderado, al CMTS en nombre de un cliente. Esta interfaz puede ser utilizada además para informar al AM de los cambios en el estatus de los recursos QoS.
pkt-mm-4	PS – RKS	El PS envía mensajes de evento al servidor de mantenimiento de registros (RKS) para el seguimiento de las decisiones de tipo político relacionadas con la QoS.
pkt-mm-5	CMTS – RKS	El CMTS envía al RKS mensajes de evento para el seguimiento de peticiones y la utilización de QoS (por ejemplo, adiciones, cambios, supresiones y medidas de volumen del flujo de servicio).
pkt-mm-6	Cliente – CMTS	El cliente puede utilizar esta interfaz para pedir y gestionar directamente recursos de red de QoS. Si se autorizan, estos recursos son proporcionados por el CMTS.
mm-7	Cliente – AM	Esta interfaz puede ser utilizada por el cliente para interactuar con el AM e, indirectamente, pedir y gestionar recursos QoS. Esta interfaz queda fuera del alcance de este apéndice.
mm-8	AM – Par	El AM puede utilizar esta interfaz para interactuar con alguna otra entidad que forme parte de la aplicación en cuestión. Esta interfaz queda fuera del alcance de este apéndice.
mm-9	CMTS – Red IP gestionada por operador	Esta interfaz del CMTS puede ser utilizada en soporte de peticiones de QoS de extremo a extremo más allá de la red de acceso. Esta interfaz queda fuera del alcance de este apéndice.
mm-10	Cliente – Par	El cliente puede utilizar esta interfaz para interactuar con alguna otra entidad que forma parte de la aplicación en cuestión. Esta interfaz queda fuera del alcance de este apéndice.

I.3.2 Componentes de multimedia

En esta cláusula se amplía el análisis previo del marco arquitectural proporcionando detalles adicionales de cada uno de los elementos de red.

I.3.2.1 Cliente

Un cliente de multimedia es una entidad lógica que puede enviar o recibir datos. Los multimedia IPCablecom definen tres tipos de cliente diferentes, que difieren en la manera en que el cliente señala QoS y la manera en que las decisiones de tipo político asociadas a la QoS se instalan en el CMTS.

El cliente de tipo 1 representa puntos de extremo "herederos" (por ejemplo, aplicaciones de PC, consolas de juegos) que carecen de información relativa a la QoS o capacidades de señalización. Este cliente no sabe nada sobre mensajería de CableModem, IPCable2Home o IPCablecom y, por tanto, no cabe imponerle requisitos relativos a la misma. Clientes de tipo 1 pueden ser desde dispositivos sencillos de presentación analógica audio y vídeo hasta periféricos en red complejos y electrónica de consumidor, tales como unidades de adaptación multimedia o consolas de juegos. Estos clientes se comunican con un gestor de aplicación para pedirle servicio y no piden recursos QoS directamente de la red de acceso del operador.

El cliente de tipo 2 es similar a un MTA de telefonía IPCablecom-T en el sentido de que soporta la señalización de QoS basada en DQoS de IPCablecom. Este cliente está al corriente de la QoS de multimedia IPCablecom y se comunica con un gestor de aplicación para pedirle servicio y obtener un testigo para recursos de red de acceso. El cliente presenta luego ese testigo, cuando pide recursos QoS de la red de acceso (pkt-mm-1, pkt-mm-6).

El cliente de tipo 3 pide QoS en base al RSVP sin la interacción del gestor de aplicación. Este cliente está al corriente del RSVP basado en las normas IETF y utiliza dicho protocolo para pedir recursos QoS de la red de acceso directamente del CMTS.

I.3.2.2 Servidor de política

El marco de gestión de políticas para la iniciativa sobre multimedia IPCablecom se basa en la labor del grupo de trabajo sobre el protocolo de asignación de recursos (RAP) del IETF. Como se define y describe en RFC 2753, el elemento de red servidor de política (PS), implementa procedimientos de gestión de recursos y autorización definidos por el operador. Además de los parámetros de los recursos pedidos y el estatus de los recursos disponibles, las decisiones de tipo político pueden requerir la identidad del cliente e información sobre el perfil asociado, parámetros de la aplicación, consideraciones relativas a la seguridad, hora del día, etc. Operadores particulares pueden optar también por desplegar múltiples servidores de política y delegar determinadas decisiones de tipo político entre esos servidores para satisfacer los requisitos relativos a la escalabilidad y la tolerancia frente a averías.

Entre las funciones principales del servidor de política figuran:

- Un mecanismo de petición de decisiones de tipo político, invocado por los gestores de aplicación (pkt-mm-3, modelo empuje) o los CMTS (pkt-mm-2, modelo extracción).
- Un mecanismo de entrega de decisiones de tipo político, utilizado para instalar decisiones de tipo político en el CMTS (pkt-mm-2).
- Un mecanismo que permita la transmisión al CMTS mediante apoderado de mensajes de gestión de QoS en nombre del gestor de aplicación (para clientes que no tienen capacidades de señalización de QoS inherentes).
- Una interfaz de registro de eventos con un servidor de mantenimiento de registros (pkt-mm-4) utilizada para el registro cronológico de peticiones de política, que pueden también ser correlacionadas con registros de utilización de recursos de red.

El servidor de política soporta dos modelos diferentes de instalación de decisiones de tipo político en el CMTS:

- El servidor de política puede instalar en (empujar hacia) el CMTS una decisión de tipo político antes de que la petición de reserva de QoS llegue al CMTS.

- El CMTS puede pedir al (extraer del) servidor de política una decisión de tipo político cuando una petición de reserva de QoS llega al CMTS.

Las reglas de política pueden contener la información siguiente:

- Reglas que definen recursos autorizados por el servidor de política:
  - por servicio;
  - por abonado;
  - de anchura de banda (especificada utilizando parámetros de colector testigo);
  - garantías de latencia;
  - horas de expiración de política;
  - límites de volumen de política.
- Reglas que definen la escasez/el valor de la anchura de banda en base a la hora del día.
- Reglas de apropiación con prioridad.

En el escenario "empujar hacia", el servidor de política debe llevar a cabo como mínimo las funciones siguientes:

- Autenticar y verificar mensajes de política procedentes de gestores de aplicación.
- Procesar mensajes de política basados en reglas definidas por un operador.
- Resolver la identidad correcta del CMTS hacia el que se ha de empujar la política.
- Comunicar decisiones de tipo político y otros mensajes de manera segura al CMTS.
- Enviar mensajes de evento para el seguimiento de estas peticiones al RKS.

En el escenario "extraer de", el servidor de política debe llevar a cabo como mínimo las funciones siguientes:

- Si en el servicio está involucrado un gestor de aplicación, autenticar y verificar los mensajes de política procedentes del gestor de aplicación.
- Comunicar decisiones de tipo político y otros mensajes de manera segura al CMTS.
- Procesar mensajes de política basados en reglas definidas por un operador.
- Enviar mensajes de evento para el seguimiento de estas peticiones al RKS.

El servidor de política debe llevar a cabo las funciones adicionales siguientes:

- Seguir la utilización de los recursos en base a la información sobre estados mantenida internamente (por ejemplo, temporizadores).
- Seguir los recursos autorizados usuario por usuario, servicio por servicio o de forma combinada.

I.3.2.3 Sistema de terminación de módem de cable

Los multimedia IPCablecom permite el acceso al conjunto completo de algoritmos de calendarización en sentido ascendente del CMTS que se definen en las Recomendaciones relativas a la tecnología CableModem. La arquitectura define, en concreto, un "perfil de tráfico" de multimedia IPCablecom que proporciona una capa de abstracción a partir de los tipos asociados de calendarización de CableModem (UGS, UGS/AD, etc.). Además, las características específicas de la telefonía y las hipótesis que se establecen en la especificación de DQoS de IPCablecom-T se generalizarán para facilitar una infraestructura de QoS que pueda ser utilizada por múltiples tipos de clientes y aplicaciones.

El CMTS soporta modelos de reserva tanto monofásicos como bifásicos para gestionar recursos de red de acceso. En el modelo bifásico, los recursos de red de acceso se reservan inicialmente y luego se compromete su utilización según se requiera en un momento posterior. El CMTS soporta

también un modelo de reserva monofásico en el que los recursos de red de acceso son reservados y comprometidos simultáneamente para su utilización inmediata.

El CMTS fija el o los flujos de servicio pertinentes en la red de acceso de CableModem vía pkt-mm-1. El CMTS envía mensajes de evento para la reserva y utilización de recursos QoS a un servidor de mantenimiento de registros vía identificador de la interfaz pkt-mm-5. Por último, el CMTS supervisa los flujos de servicio basados en QoS y los contabiliza según se define en el subsistema de gestión de contabilidad (facultativo) de las Recomendaciones relativas a la tecnología CableModem.

I.3.2.4 Gestor de aplicación

El gestor de aplicación desempeña una función de coordinación en la que intervienen la señalización y la semántica de la aplicación así como la interacción con el marco de política de los multimedia IPCablecom, según lo expuesto durante el análisis anterior del elemento servidor de política. Se señala que un gestor de aplicación puede estar alojado junto con un servidor de medios o bien, en un modelo dividido, los dos elementos pueden existir por separado.

El gestor de aplicación hace interfaz con un cliente vía mm-7. En base a su conocimiento de las ofertas de servicio particulares, el gestor de aplicación debe deducir o definir los parámetros de QoS que, en concreto, se necesitan para entregar el servicio al cliente de tipo 1. Una vez que esta información ha sido confirmada, el gestor de aplicación envía una petición de política al servidor de política vía pkt-mm-3. Si es necesario, el gestor de aplicación puede utilizar mm-8 para sincronizar con un servidor de medios.

El cliente de tipo 2 interactúa también con el gestor de aplicación y comunica información sobre petición de servicio vía mm-7. De nuevo, el gestor de aplicación debe deducir los parámetros de QoS que se necesitan para entregar el servicio al cliente de tipo 2. El gestor de aplicación envía una petición de política al servidor de política vía pkt-mm-3. Una vez conseguida la autorización, el gestor de aplicación recibe un testigo procedente del servidor de política y lo envía al cliente vía mm-7. Si hace falta, el gestor de aplicación puede utilizar el mm-8 para sincronizar con un servidor de medios.

El cliente de tipo 3 no requiere un gestor de aplicación, aunque es muy probable la presencia de un servidor de aplicación en escenarios de entrega de servicio complejos.

I.3.2.5 Servidor de mantenimiento de registros

El servidor de mantenimiento de registros (RKS) recibe mensajes de evento que indican la utilización de recursos QoS de red de acceso. El RKS hace interfaz con el servidor de política (pkt-mm-4) y el CMTS (pkt-mm-5). El RKS no recibe información específica de la aplicación directamente del gestor de aplicación. En cambio, información específica de la aplicación puede estar incluida en un mensaje de evento en forma de datos opacos enviados del gestor de aplicación al servidor de política e incorporados en el mensaje de evento de petición de política enviado al RKS.

I.4 QoS proporcionada mediante apoderado con empuje de la política (escenario 1)

Como se ha indicado más arriba, se han identificado tres escenarios arquitecturales con los que se da soporte a los tres tipos de cliente. El modelo de autorización "QoS proporcionada mediante apoderado con empuje de la política" (escenario 1) soporta al cliente de tipo 1, que no soporta por sí mismo mecanismos de señalización de QoS inherentes. En la figura I.3 se presenta una visión general de alto nivel de la interacción entre elementos que se produce en este escenario.

El cliente pide un servicio específico de la aplicación enviando un mensaje "Petición de servicio" al gestor de aplicación. Tras recibir esa petición, el gestor de aplicación determina cuáles son las necesidades de QoS y envía un mensaje "Petición de política" al servidor de política. El servidor de política a su vez valida la "petición de política" cotejándola con las reglas de política definidas por

el operador y, si la decisión es afirmativa, envía un mensaje "Fijación de política" al CMTS. El CMTS lleva a cabo el control de admisión en la capacidad máxima de QoS pedida (verificando si se dispone de los recursos adecuados para cumplimentar esa petición), instala la decisión de tipo político y establece (eventualmente) el flujo o los flujos de servicio con los niveles de QoS pedidos.

Hay que señalar que la gestión efectiva del flujo o los flujos de servicio (es decir, peticiones de adición, cambio o supresión) puede ser controlada y supervisada estrechamente por el gestor de aplicación mediante ampliaciones de los mecanismos de señalización básicos que se describen aquí para la instalación de la decisión de tipo político. En el escenario 1, no hay comunicación directa entre el cliente y el CMTS.

Se señala que la interfaz entre el cliente y el gestor de aplicación, incluidos los detalles de la "petición de servicio", queda fuera del alcance de la presente Recomendación. Es posible que el cliente no tenga conocimiento de la QoS y pida simplemente un servicio (por ejemplo, el usuario desea jugar con un amigo un juego de múltiples participantes) del gestor de aplicación en el mensaje "Petición de servicio". También es posible que el cliente tenga pleno conocimiento de sus necesidades de QoS (por ejemplo, el usuario pide un servicio garantizado a 128 kbit/s para acceder a su red privada virtual (RPV) colectiva, asegurada por IPSec) y comunica esta información adicional en la "petición de servicio". El mecanismo mediante el cual el gestor de aplicación determina los requisitos de QoS del servicio pedido queda fuera del ámbito de la presente arquitectura.

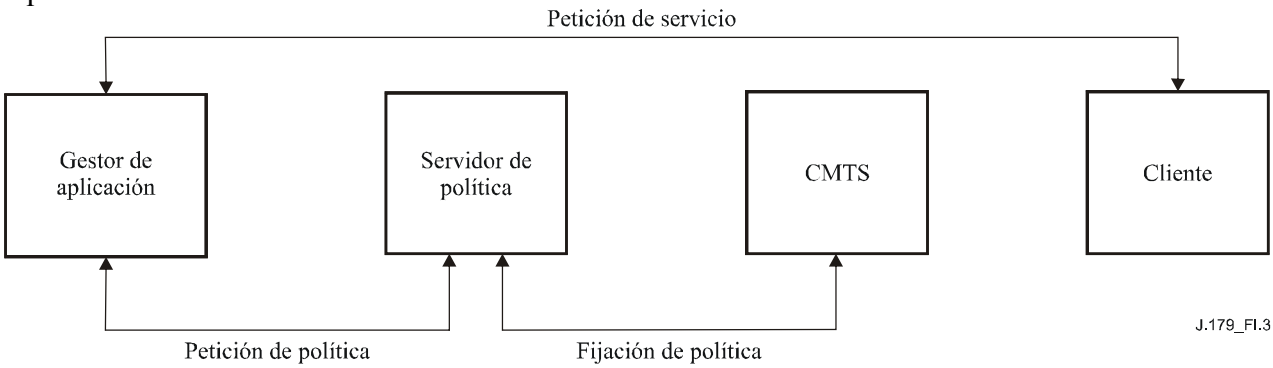


Figura I.3/J.179 – Marco de autorización del escenario 1

En el escenario 1, el CMTS soporta un modelo de reserva de recurso monofásico, mostrado a continuación en la figura I.4, para habilitar la activación inmediata y la utilización de recursos de red de acceso por el cliente. (En este escenario se soporta también un modelo de reserva de recurso bifásico, como se expone más adelante en esta misma cláusula.)

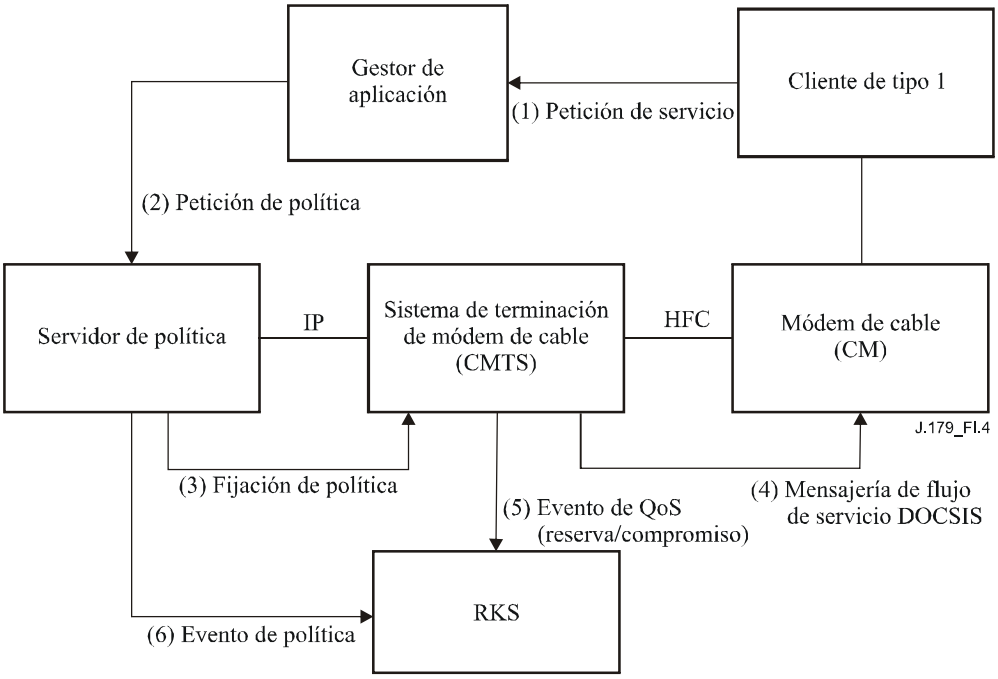


Figura I.4/J.179 – Modelo de reserva de recurso monofásico del escenario 1

En base a esa secuencia de mensajería monofásica, el cuadro I.2 presenta un resumen de alto nivel de cada uno de los mensajes. Los detalles específicos de los mensajes y objetos de protocolo se han trasladado a las especificaciones respectivas de los multimedia IPCablecom.

Cuadro I.2/J.179 – Detalles de los mensajes de reserva de recurso monofásicos del escenario 1

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(1) Petición de servicio	El cliente pide servicio del gestor de aplicación.	<none>	Fuera del alcance de multimedia IPCablecom	Este protocolo deberá soportar la autenticación del cliente y del gestor de aplicación. Además, el protocolo deberá proporcionar información suficiente para que el gestor de aplicación lleve las necesidades de QoS del servicio pedido.
(2) Petición de política	El gestor de aplicación pide fijación de QoS en nombre del cliente.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca.	Gate-Control (COPS)	El servidor de política utiliza reglas de política gestionadas por el operador para admitir o rechazar la petición.

Cuadro I.2/J.179 – Detalles de los mensajes de reserva de recurso monofásicos del escenario 1

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(3) Fijación de política	El servidor de política envía un mensaje al CMTS, instalando su decisión de tipo político y pidiendo el establecimiento de flujos de servicio.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS).	Gate-Control (COPS)	En el modelo monofásico, esta petición es para autorización, reserva y compromiso de recursos QoS.
(4) Mensajería de CableModem	El CMTS establece flujos de servicio con QoS mejorada.	Tipo de calendarización de CableModem, parámetros de anchura de banda y latencia, clasificador de tráfico.	Mensajería DSx de CableModem	Las funciones de QoS se basan aquí en los mecanismos definidos en la especificación RFI de CableModem.
(5) Evento de QoS	El CMTS genera el mensaje de evento adecuado, indicando la utilización de QoS y otros parámetros de facturación.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político, datos de utilización del servicio, hora del día.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.
(6) Evento de política	El servidor de política genera el mensaje de evento adecuado, indicando la petición de política y la acción efectuada.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.

La información resumida en la columna Campos del cuadro I.2 tiene por objeto dar un ejemplo del tipo de información que lleva cada mensaje. Los detalles de cada mensaje de protocolo se han trasladado a los documentos de especificación apropiados.

El escenario 1 soporta también un modelo de reserva de recurso bifásico, mostrado a continuación en la figura I.5. Aquí, el gestor de aplicación pide primero que se autoricen y reserven recursos QoS de red de acceso. Una vez reservados esos recursos, el gestor de aplicación puede continuar su diálogo con el cliente a propósito del servicio. Cuando proceda, el gestor de aplicación pedirá que se comprometan recursos QoS de red de acceso. Este modelo de reserva/compromiso bifásico garantiza el que los recursos de red de acceso estén disponibles antes de ofrecer el servicio al cliente.

Se señala que no se incluyen explícitamente los acuses de recibo de cada uno de los mensajes mostrados, pero están implícitos. Cada mensaje de acuse de recibo sólo se puede enviar una vez que se conoce el resultado final de la petición correspondiente. Esto es particularmente importante en la secuenciación de acuses de recibo de los mensajes 4 (Reserva DOCSIS), 3 (Fijación de política) y 2 (Petición de política) ya que el gestor de aplicación esperará probablemente la confirmación exitosa de la fase de reserva antes de continuar su diálogo con el cliente y, eventualmente, comprometer los recursos.

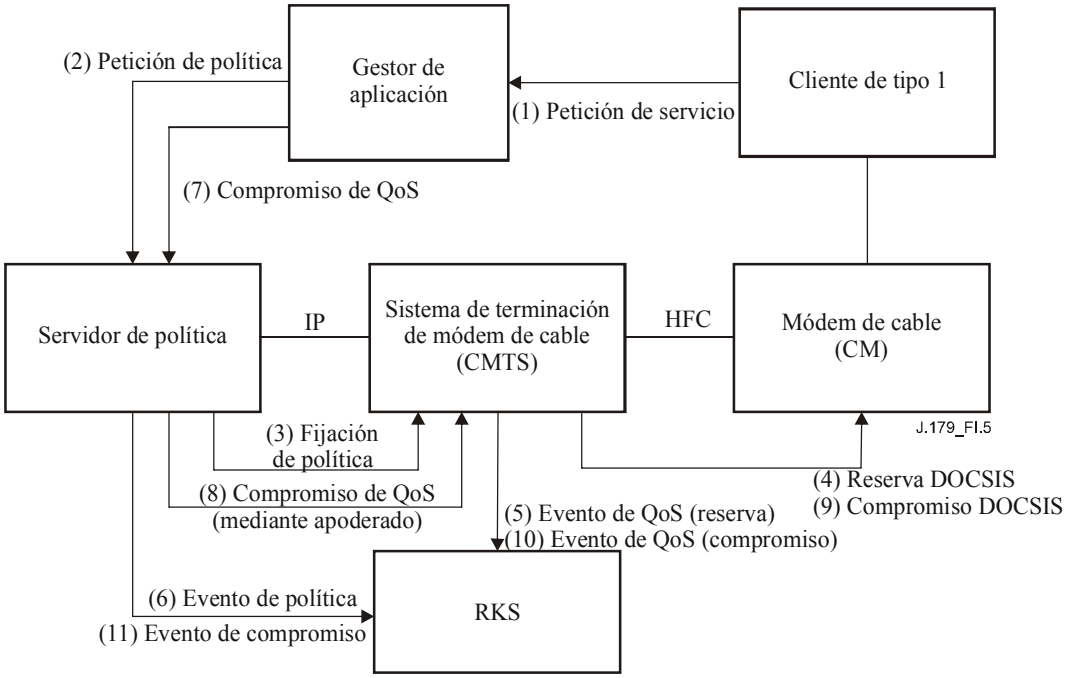


Figura I.5/J.179 – Modelo de reserva de recurso bifásico del escenario 1

En el cuadro I.3 se da un resumen de los mensajes indicados en la figura I.5. Se señala que se han añadido mensajes (7 a 10) como soporte de la fase señalización de compromiso.

Cuadro I.3/J.179 – Detalles de los mensajes de reserva de recurso bifásicos del escenario 1

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(1) Petición de servicio	El cliente pide servicio del gestor de aplicación.	<none>	Fuera del alcance de multimedia IPCablecom	Este protocolo deberá soportar la autenticación del cliente y del gestor de aplicación. Además, el protocolo deberá proporcionar información suficiente para que el gestor de aplicación lleve las necesidades de QoS del servicio pedido.
(2) Petición de política	El gestor de aplicación pide fijación de QoS en nombre del cliente.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca.	Gate-Control (COPS)	El servidor de política utiliza reglas de política gestionadas por el operador para admitir o rechazar la petición.
(3) Fijación de política	El servidor de política envía un mensaje al CMTS, instalando su decisión de tipo político y pidiendo la reserva de flujos de servicio.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS).	Gate-Control (COPS)	En el modelo bifásico, esta petición es para autorización, reserva y compromiso de recursos QoS.
(4) Reserva DOCSIS	El CMTS establece flujos de servicio con QoS mejorada y los pone en un estado "admitido".	Tipo de calendarización de CableModem, parámetros de anchura de banda y latencia, clasificador de tráfico.	Mensajería DSx de CableModem	Las funciones de QoS se basan aquí en los mecanismos definidos en la especificación RFI de CableModem. Los recursos reservados permanecen inactivos y pueden ser utilizados por el tráfico de mejor esfuerzo en otros flujos hasta que sean comprometidos.

Cuadro I.3/J.179 – Detalles de los mensajes de reserva de recurso bifásicos del escenario 1

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(5) Evento de QoS	El CMTS genera el mensaje de evento adecuado, indicando la reserva de QoS y otros parámetros de facturación.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político, datos de utilización del servicio, hora del día.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.
(6) Evento de política	El servidor de política genera el mensaje de evento adecuado, indicando la petición de política y la acción efectuada.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.
(7) Compromiso de QoS	El AM señala para comprometer los recursos QoS.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, identificador de política.	Gate-Control (COPS)	El compromiso de AM puede depender de la mensajería ulterior con el cliente.

Cuadro I.3/J.179 – Detalles de los mensajes de reserva de recurso bifásicos del escenario 1

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(8) Compromiso de QoS (mediante apoderado)	El servidor de política recibe la petición de AM y actúa mediante apoderado con el CMTS.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, identificador de política.	Gate-Control (COPS)	Aunque el PS puede aplicar reglas de política durante la fase compromiso, por lo general se supone que la anchura de banda reservada puede ser comprometida por el AM en cualquier momento.
(9) Compromiso DOCSIS	El CMTS pone el flujo de servicio en el estado "activo".	Tipo de calendarización de IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, ID de flujo de servicio.	Mensajería DSx de CableModem	Las funciones de QoS se basan aquí en la especificación RFI de CableModem.
(10) Evento de QoS (compromiso)	El CMTS genera el mensaje de evento adecuado, indicando la utilización de QoS y otros parámetros de facturación.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político, datos de utilización del servicio, hora del día.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.
(11) Evento de compromiso	El servidor de política genera el mensaje de evento adecuado, indicando el compromiso de QoS y la acción efectuada.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, identificador de política.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.

Una vez que los recursos QoS han sido autorizados, reservados y comprometidos de manera satisfactoria sobre la red de acceso, en el CMTS se supervisa la actividad de los mismos. En general, se utiliza un modelo de estados flexible en el que se requieren mensajes de reiniciación periódicos durante los periodos de inactividad en los flujos de servicio reservados y comprometidos. Si los temporizadores de actividad expiran sin ser reiniciados, los recursos asociados pueden ser recuperados por el CMTS. Así se facilita la adaptabilidad de la red en caso de que falle un punto de extremo.

En este escenario se proporciona también una secuencia de recuperación de recursos más normalizada, en la que el gestor de aplicación señala al servidor de política cuándo ha terminado la sesión del servicio. El servidor de política responde generando un mensaje de evento, que es enviado al RKS, y emitiendo una directiva dirigida al CMTS para que elimine el flujo o los flujos de servicio correspondientes y recupere los recursos asociados. Con independencia de si un flujo de servicio expira por inactividad o es suprimido de forma explícita, se mantiene una pista de auditoría sólida, con la que se sigue la utilización efectiva de los recursos vía mensajes de evento producidos en el CMTS y enviados al RKS.

I.4.1 Ejemplo: Anchura de banda basada en la web a la demanda

Un ejemplo de cómo los mecanismos del escenario 1 pueden ser aplicados en un contexto de entrega de servicio es el caso de un sitio web seguro cuyo anfitrión es el operador, que permitiría a los abonados disponer de reservas de anchura de banda a la demanda.

Supóngase, por ejemplo, que el servicio normal de un abonado tiene la velocidad limitada a 128 kbit/s en sentido descendente y a 128 kbit/s en sentido ascendente. Aunque este nivel de servicio puede ser el adecuado en la mayoría de las utilizaciones, es posible que haya ocasiones en las que la aplicación que utiliza el abonado requiera más anchura de banda o tenga necesidades de QoS diferentes. Si el usuario decidiera utilizar el servicio de anchura de banda a la demanda para introducir cambios temporales en su nivel de servicio normal, se conectaría simplemente al sitio web del operador (gestor de aplicación) y pediría un aumento temporal del nivel de servicio.

Un posible motivo de esa petición sería el deseo de transmitir los ficheros de medios en flujo continuo de alta velocidad binaria desde un proveedor de contenidos. En este caso, el abonado podría pedir explícitamente un servicio a velocidad reservada mínima descendente de 512 kbit/s durante las tres horas siguientes. De manera alternativa, podría ocurrir que las necesidades exactas de QoS de la aplicación fuesen opacas al abonado, que pediría simplemente un determinado vídeo clip de tres horas (el cual, sin que lo sepa el abonado, resulta que está codificado a 512 kbit/s). De un modo u otro, este intercambio representa la "petición de servicio" del abonado al gestor de aplicación.

El gestor de aplicación presentaría, en cualquiera de los dos casos, una "petición de política" del servicio a velocidad mínima reservada de 512 kbit/s durante tres horas al servidor de política en nombre del abonado. El servidor de política aplicaría entonces su propio criterio de autorización y, si la petición se aprobara, pediría al CMTS (mediante un mensaje "Fijación de política") que proporcionara la anchura de banda para el abonado. El CMTS efectuaría, a su vez, un control de admisión interno y establecería la QoS utilizando la mensajería de CableModem, con seguimiento de este proceso mediante un mensaje de evento de QoS.

I.4.2 Ejemplo: Juegos en línea vía consolas configuradas en red

De manera alternativa, considérese el caso en que dos consolas de juegos desean vincularse la una con la otra a través de un túnel de red. En este ejemplo, normalmente dos usuarios sólo pueden configurar en red sus consolas si están coubicadas. Sin embargo, un programa informático especial instalado en los ordenadores personales de los usuarios, situados en una red local y que actúan como apoderados de las consolas distantes, permite el funcionamiento en red de tal manera que ya no es preciso que las dos consolas de juegos estén coubicadas. El único problema de este

planteamiento novedoso es que el túnel resultante requiere QoS suficiente de forma que se pueda jugar con las consolas de juegos como si estuvieran coubicadas en una red de alta velocidad.

En este escenario, el o los usuarios se conectarían al gestor de aplicación vía el o los PC que tunelizan sus paquetes. Mediante mensajería específica de la aplicación, se autentican a sí mismos e indican su deseo jugar una partida el uno con el otro. El gestor de aplicación concede la petición y genera la o las "petición(es) de política" en nombre del o de los usuarios. El servidor de política toma su decisión y reenvía el mensaje como una "fijación de política" al CMTS. El CMTS lleva a cabo el control de admisión y habilita la QoS de red de acceso entre los PC del túnel de juegos utilizando mensajería de CableModem. Desde ese momento en adelante, las consolas de juegos pueden intercambiar paquetes sin saber que no están coubicadas. Se señala que en este ejemplo se ha omitido la mensajería de eventos para simplificar.

En un caso hipotético como este, si los usuarios residen en nodos HFC separados, corresponde al operador asegurar que la QoS medular hacia y desde el CMTS es manipulada adecuadamente al nivel que requieren sus acuerdos sobre políticas y servicios. La figura I.6 presenta una ilustración gráfica de este ejemplo para el caso simplificado en que ambos usuarios reciben servicio desde un único CMTS.

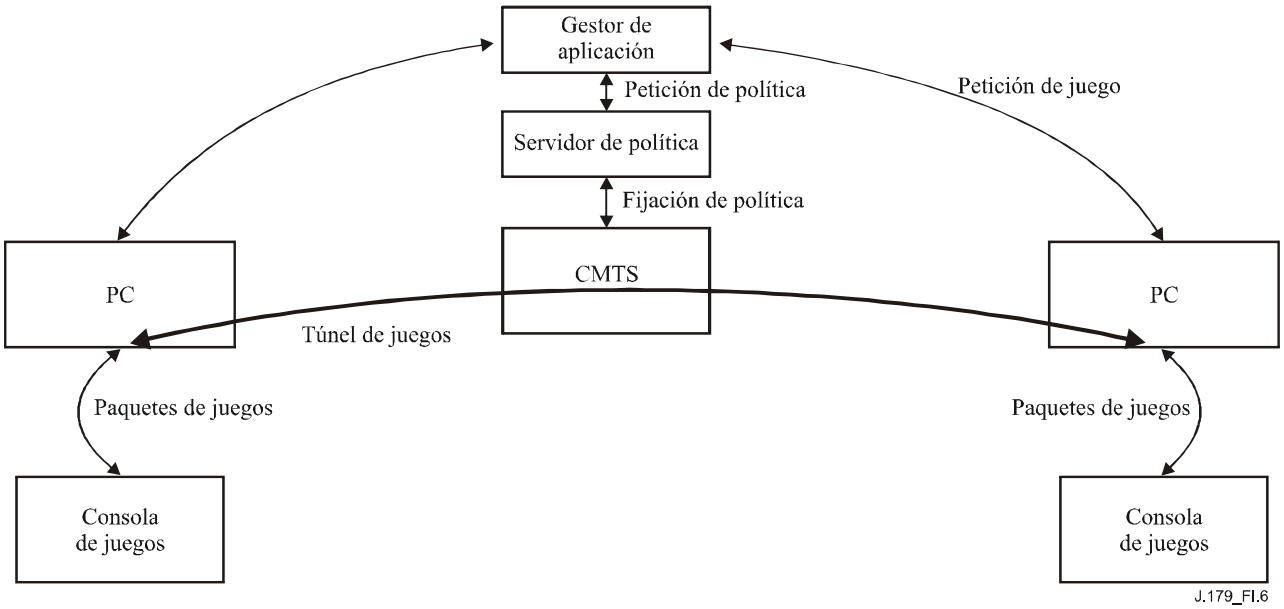


Figura I.6/J.179 – Consolas de juegos configuradas en red vía un túnel IP de QoS mejorada

I.5 QoS pedida por el cliente con empuje de la política (escenario 2)

El modelo "QoS pedida por el cliente con empuje de la política" del escenario 2 soporta al cliente de tipo 2, que es capaz de señalizar y gestionar sus propios recursos QoS pero requiere la autorización previa de las peticiones vía un gestor de aplicación. En este escenario, el modelo de autorización de política y reserva de QoS se parece mucho al modelo de telefonía de IPCablecom-T definido en la especificación de DQoS. El servidor de política empuja la política hacia el CMTS de forma parecida a como hace el controlador de puerta para enviar la política al CMTS vía el COPS. El cliente de tipo 2 utiliza mensajería DSx de CableModem o RSVP+ similar a la de los dispositivos MTA de IPCablecom-T.

En la figura I.7 se da una visión general de alto nivel del escenario 2. Se señalan las semejanzas con el marco de autorización expuesto para el escenario 1. De nuevo aquí, el cliente pide un servicio específico de la aplicación enviando un mensaje "Petición de servicio" al gestor de aplicación. El gestor de aplicación determina a continuación cuáles son las necesidades de QoS del servicio

pedido y envía un mensaje "Petición de política" al servidor de política. El mensaje "Petición de política" contiene la "capacidad máxima autorizada" o QoS máxima permitida para el cliente. El servidor de política valida entonces el mensaje "Petición de política" cotejándolo con las reglas de política definidas por el operador y, si la decisión es afirmativa, envía un mensaje "Fijación de política" al CMTS. El CMTS efectúa el control de admisión en la QoS pedida e instala la autorización de política. Como en el escenario 1, mensajes de evento son generados por el servidor de política y el CMTS y enviados al RKS. El servidor de política registra un evento cada vez que toma una decisión, o actualiza su estado, y el CMTS lleva a cabo el seguimiento del mantenimiento y la utilización de los recursos QoS.

En el escenario 2, y a diferencia del escenario 1, hay una comunicación directa entre el cliente y el CMTS para añadir, cambiar y suprimir reservas de recurso. Una vez que el CMTS reciba el mensaje "Fijación de política" procedente del servidor de política, el cliente puede pedir QoS directamente del CMTS utilizando el mecanismo de señalización de QoS indicado anteriormente. El cliente puede también cambiar la QoS dinámicamente en tanto en cuanto la QoS pedida esté dentro de la "capacidad máxima autorizado" aprobado por el servidor de política. La ventaja de este método consiste en que el gestor de aplicación no tiene que negociar la utilización de la anchura de banda por el cliente, lo que constituye un factor muy útil cuando las necesidades de QoS del cliente cambian dinámicamente.

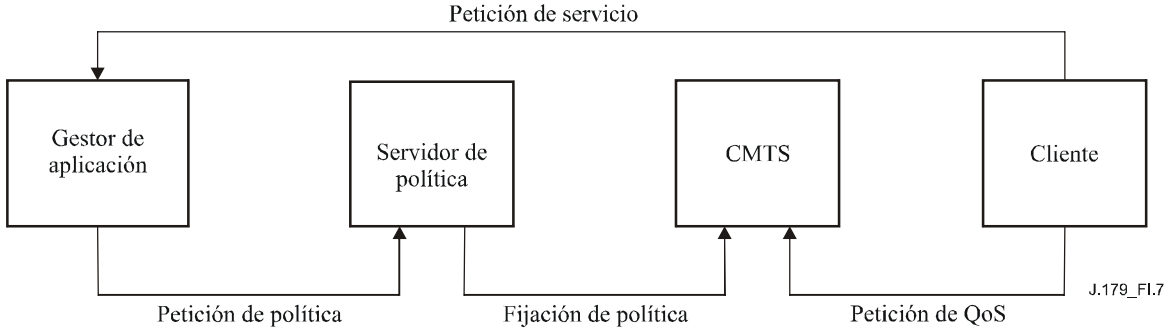


Figura I.7/J.179 – Marco de autorización del escenario 2

Al igual que en el escenario anterior, el escenario 2 (mostrado en la figura I.8) soporta un modelo de reserva de recurso monofásico para habilitar la activación y la utilización inmediatas de recursos de red de acceso por el cliente.

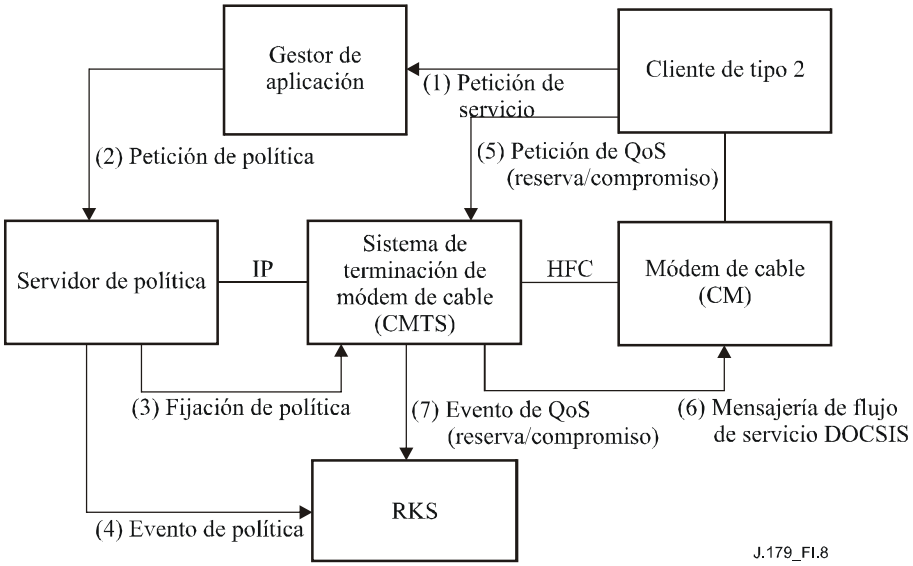


Figura I.8/J.179 – Modelo de reserva de recurso monofásico del escenario 2

En base a esa secuencia de mensajería monofásica, el cuadro I.4 presenta un resumen de alto nivel de cada uno de los mensajes.

Cuadro I.4/J.179 – Detalles de los mensajes de reserva de recurso monofásicos del escenario 2

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(1) Petición de servicio	El cliente pide servicio del gestor de aplicación.	<none>	Fuera del alcance de multimedia IPCablecom	Este protocolo deberá soportar la autenticación del cliente y del gestor de aplicación. Además, el protocolo deberá proporcionar información suficiente para que el gestor de aplicación lleve las necesidades de QoS del servicio pedido.
(2) Petición de política	El gestor de aplicación pide autorización de QoS en nombre del cliente.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca.	Gate-Control (COPS)	El servidor de política utiliza reglas de política gestionadas por el operador para admitir o rechazar la petición.

Cuadro I.4/J.179 – Detalles de los mensajes de reserva de recurso monofásicos del escenario 2

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(3) Fijación de política	El servidor de política envía un mensaje al CMTS, instalando su decisión de tipo político.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS).	Gate-Control (COPS)	En este escenario, esta petición es para autorización solamente.
(4) Evento de política	El servidor de política genera el mensaje de evento adecuado, indicando la petición de política y la acción efectuada.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político.	Event-Messaging RADIUS	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.
(5) Petición de QoS (reserva/ compromiso)	El cliente pide que se reserven recursos QoS y se comprometan inmediatamente para su utilización.	Parámetros de anchura de banda y latencia, clasificador de tráfico.	DSx o RSVP+ de CableModem	El cliente puede establecer directamente flujos de servicio CableModem vía mensajería DSx o puede emitir mensajes RSVP+ para establecer estos flujos.

Cuadro I.4/J.179 – Detalles de los mensajes de reserva de recurso monofásicos del escenario 2

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(6) Mensajería DOCSIS	El CMTS establece flujos de servicio con QoS mejorada y los pone en un estado "activo".	Tipo de calendarización de CableModem, parámetros de anchura de banda y latencia, clasificador de tráfico.	Mensajería DSx de CableModem	Este paso sólo es necesario si se ha proporcionado señalización de RSVP+ al CMTS en el mensaje previo; de no ser así, los flujos de servicio ya han sido establecidos y activados vía mensajería DSx de CableModem. Las funciones de QoS se basan aquí en los mecanismos definidos en las Recomendaciones sobre CableModem.
(7) Evento de QoS	El CMTS genera el mensaje de evento adecuado, indicando la utilización de QoS y otros parámetros de facturación.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político, datos de utilización del servicio, hora del día.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.

El CMTS soporta también un modelo de reserva de recurso bifásico, según se muestra en la figura I.9. En este modelo, el cliente pide primero que se reserven recursos QoS de red de acceso. Una vez que estos recursos han sido reservados, el cliente indica que dichos recursos sean comprometidos. El modelo de reserva/compromiso bifásico garantiza el que los recursos de red de acceso estén disponibles antes de ofrecer servicios al cliente.

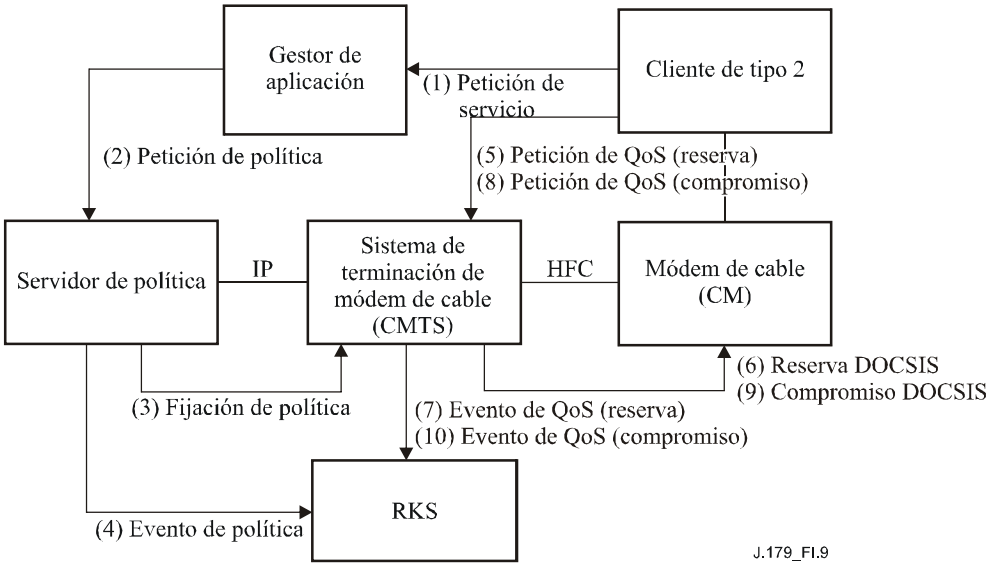


Figura I.9/J.179 – Modelo de reserva de recurso bifásico del escenario 2

Cuadro I.5/J.179 – Detalles de los mensajes de reserva de recurso bifásicos del escenario 2

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(1) Petición de servicio	El cliente pide servicio del gestor de aplicación.	<none>	Fuera del alcance de multimedia IPCablecom	Este protocolo deberá soportar la autenticación del cliente y del gestor de aplicación. Además, el protocolo deberá proporcionar información suficiente para que el gestor de aplicación lleve las necesidades de QoS del servicio pedido.
(2) Petición de política	El gestor de aplicación pide la autorización de QoS en nombre del cliente.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca.	Gate-Control (COPS)	El servidor de política utiliza reglas de política gestionadas por el operador para admitir o rechazar la petición.

Cuadro I.5/J.179 – Detalles de los mensajes de reserva de recurso bifásicos del escenario 2

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(3) Fijación de política	El servidor de política envía un mensaje al CMTS, instalando su decisión de tipo político.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS).	Gate-Control (COPS)	En este escenario, esta petición es para autorización solamente.
(4) Evento de política	El servidor de política genera el mensaje de evento adecuado, indicando la petición de política y la acción efectuada.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.
(5) Petición de QoS (reserva)	El cliente pide que se reserven recursos QoS.	Parámetros de anchura de banda y latencia, clasificador de tráfico.	DSx o RSVP+ de CableModem	El cliente puede establecer directamente flujos de servicio CableModem vía mensajería DSx o puede emitir mensajes RSVP+ para establecer estos flujos.
(6) Reserva DOCSIS	El CMTS establece flujos de servicio con QoS mejorada y los pone en un estado "admitido".	Tipo de calendarización de CableModem, parámetros de anchura de banda y latencia, clasificador de tráfico.	Mensajería DSx de CableModem	Este paso sólo es necesario si se ha proporcionado señalización de RSVP+ al CMTS en el mensaje previo; de no ser así, los flujos de servicio ya han sido establecidos y activados vía mensajería DSx de CableModem. Las funciones de QoS se basan aquí en los mecanismos definidos en las Recomendaciones sobre CableModem.

Cuadro I.5/J.179 – Detalles de los mensajes de reserva de recurso bifásicos del escenario 2

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(7) Evento de QoS (reserva)	El CMTS genera el mensaje de evento adecuado, indicando la utilización de QoS y otros parámetros de facturación.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político, datos de utilización del servicio, hora del día.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.
(8) Petición de QoS (compromiso)	El cliente pide que se comprometan recursos QoS.	Parámetros de anchura de banda y latencia, clasificador de tráfico.	DSx o RSVP+ de CableModem	El cliente puede establecer directamente flujos de servicio CableModem vía mensajería DSx o puede emitir mensajes RSVP+ para establecer estos flujos.
(9) Compromiso DOCSIS	El CMTS pone los flujos de servicio en un estado "activo".	Tipo de calendarización de CableModem, parámetros de anchura de banda y latencia, clasificador de tráfico, ID de flujos de servicio.	Mensajería DSx de CableModem	Este paso sólo es necesario si se ha proporcionado señalización de RSVP+ al CMTS en el mensaje previo; de no ser así, los flujos de servicio ya han sido establecidos y activados vía mensajería DSx de CableModem. Las funciones de QoS se basan aquí en los mecanismos definidos en las Recomendaciones sobre CableModem.

Cuadro I.5/J.179 – Detalles de los mensajes de reserva de recurso bifásicos del escenario 2

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(10) Evento de QoS (compromiso)	El CMTS genera el mensaje de evento adecuado, indicando la utilización de QoS y otros parámetros de facturación.	Tipo de QoS de MM IPCablecom, clase de sesión de MM IPCablecom, parámetros de anchura de banda y latencia, clasificador de tráfico, indicación de facturación opaca (para AM y PS), decisión de tipo político, datos de utilización del servicio, hora del día.	Event-Messaging (RADIUS)	Este mensaje deberá contener constructivos suficientes como para permitir una reconstrucción del evento o los eventos y de la o las decisiones tomadas con respecto a un servicio determinado a efectos de soporte y/o conciliación.

Al igual que en el escenario anterior, son posibles dos alternativas con respecto a la eliminación y recuperación de recursos QoS. Los recursos pueden caducar (se detecta en el CMTS) por inactividad sin que se reinicie un temporizador señalado o pueden ser eliminados explícitamente por el cliente cuando concluya una sesión de servicio. El mecanismo proporcionado para señalar explícitamente la eliminación de un flujo de servicio es un componente del protocolo de QoS definido en el dispositivo de cliente 2. La única variación entre la secuencia de recuperación de recursos definida para el escenario 1 y la del escenario 2 es que la eliminación de un flujo de servicio es señalada directamente vía el cliente en vez de serlo mediante apoderado a través del gestor de aplicación en el segundo escenario.

I.5.1 Ejemplo: Juegos en línea vía consolas configuradas en red

El ejemplo de las consolas de juegos configuradas en red expuesto para el escenario 1 en I.4.2 puede ser alterado fácilmente para atenerse al modelo de gestión de recursos QoS presentado en el escenario 2. En este caso, las consolas se seguirían coordinando con un gestor de aplicación para localizarse mutuamente y establecer la señalización específica de la aplicación. Además, el gestor de aplicación presentaría una petición de recurso al servidor de política solicitando la autorización para los recursos QoS necesarios. Sin embargo, tras la instalación exitosa de esta decisión de autorización en el CMTS, el gestor de aplicación devolvería simplemente un acuse de recibo afirmativo conteniendo un testigo de autorización a cada PC apoderado. El testigo podría ser utilizado entonces por los PC en su señalización de QoS a los CMTS para reservar, comprometer y suprimir los flujos de servicio requeridos por el túnel de juegos.

I.6 QoS pedida por el cliente con extracción de la política (escenario 3)

El tercer escenario, con su modelo de autorización "QoS pedida por el cliente con extracción de la política", soporta al cliente de tipo 3. El escenario 3 define un modelo en el que las decisiones de autorización de política no están preestablecidas ni son empujadas hacia el CMTS vía el gestor de aplicación y los mecanismos del servidor de política expuestos en los escenarios previos, sino que son pedidas por el CMTS del servidor de política a la demanda según impongan las peticiones de reserva entrantes. De esta manera es posible un modelo de reserva de recurso muy flexible y dinámico estimulado por el cliente, mientras se mantiene un control autoritario por parte del operador sobre todas las peticiones de recurso en el extremo de cabecera.

En este escenario, el CMTS recibe una petición de QoS procedente del cliente antes de que el servidor de política instale una decisión de tipo político. Incluidas en la petición de QoS figuran las credenciales que habilitan al cliente que ha de ser autenticado. El CMTS elabora una petición de política que envía al servidor de política. En el servidor de política, la petición es autenticada y se toma una decisión respecto a la autorización de la petición en base a criterios especificados por el operador (por ejemplo, disponibilidad de recursos, perfil del cliente, grado de solvencia, clase de servicio, interacción con otros elementos de red, etc.). Si la autorización de la política tiene éxito, se permite que la reserva de recurso en el CMTS siga su curso y se establece el flujo de servicio CableModem en base a la QoS pedida. Las interfaces de multimedia IPCablecom (definidas en I.3.1) que intervienen en esta interacción son: pkt-mm-1, pkt-mm-2, pkt-mm-4, pkt-mm-5, pkt-mm-6 y mm-9. También se puede utilizar la interfaz pkt-mm-3, según impongan los requisitos específicos de señalización de la aplicación, pero no se supone que esté en uso.

La figura I.10 ilustra el flujo de información entre los elementos medulares de la red de acceso del escenario 3. El cuadro I.6 que sigue a la figura I.10 contiene otra descripción de los mensajes. En el ejemplo que se muestra a continuación, la QoS sólo se establece en sentido ascendente entre el CM y el CMTS. Para establecer la QoS simétrica en sentido descendente se requeriría un flujo similar.

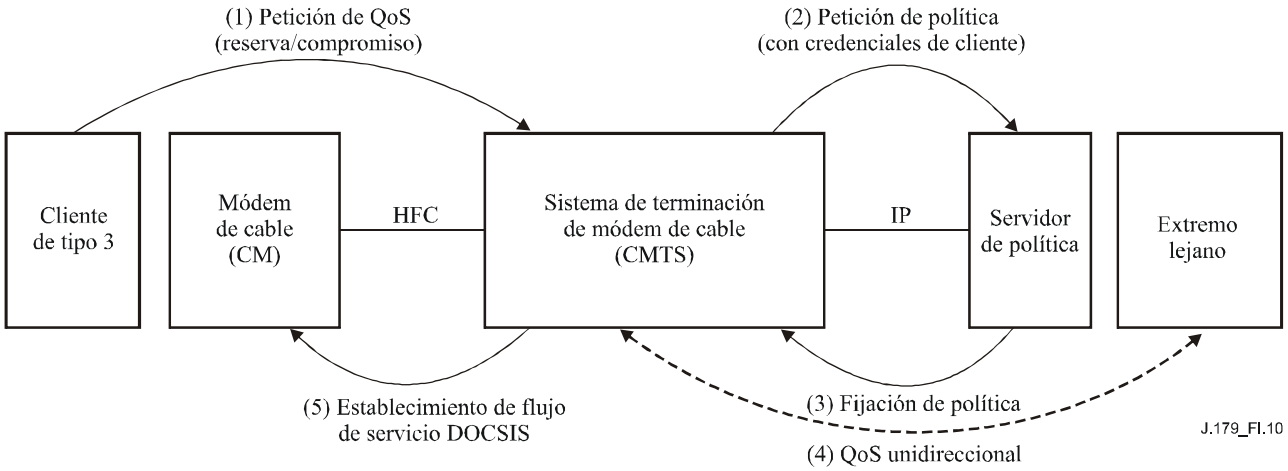


Figura I.10/J.179 – Marco de autorización del escenario 3

Cuadro I.6/J.179 – Detalles de los mensajes del escenario 3

Mensaje	Función	Campos	Protocolo candidato	Comentarios
(1) Petición de QoS (reserva/ compromiso)	El cliente pide reserva de recurso del CMTS.	Parámetros de anchura de banda y latencia, clasificador de tráfico, credenciales de autenticación.	RSVP	Este escenario supone que en el cliente existen capacidades de RFC 2205.
(2) Petición de política	El CMTS solicita decisión de autorización de política del servidor de política.	Parámetros de anchura de banda y latencia, clasificador de tráfico, credenciales de autenticación.	COPS	RFC 2748
(3) Fijación de política	El servidor de política instala la autorización en el CMTS.	Parámetros de anchura de banda y latencia, clasificador de tráfico.	COPS	RFC 2748
(4) QoS unidireccional	El CMTS reenvía señalización de RSVP de extremo lejano.	Parámetros de anchura de banda y latencia, clasificador de tráfico, credenciales de autenticación.	RSVP	RFC 2205
(5) Establecimiento de flujo de servicio CableModem	El CMTS negocia el establecimiento de un flujo de servicio programado de CableModem con el CM.	Tipo de calendarización de CableModem, parámetros de anchura de banda y latencia, clasificador de tráfico, ID de flujo de servicio.	Mensajería DSx de CableModem	Las funciones de QoS se basan aquí en los mecanismos definidos en las Recomendaciones sobre CableModem.

Una de las principales características distintivas de este escenario es su soporte del RSVP, un mecanismo de señalización de QoS basado en normas. Mientras que el escenario 1 se refiere a clientes sin capacidades de señalización de QoS inherentes y el escenario 2 define un mecanismo de señalización de QoS específico de IPCablecom (basado en el RSVP, pero con ampliaciones patentadas), este escenario se basa exclusivamente en una norma IETF. De este modo es posible la interoperabilidad con clientes basados en normas que se hayan abonado a servicios con QoS de operador y dispongan de algún medio para autenticarse a sí mismos de forma segura en la red de acceso. Tampoco se requieren aplicaciones que empujen las decisiones de tipo político hacia adelante en el tiempo y, por ello, no se imponen restricciones arquitecturales a la señalización de la aplicación.

El escenario 3 supone que se intercambian mensajes RSVP entre el cliente y el extremo lejano. Se señala, no obstante, que esto no exige que todos los elementos de red entre el cliente y el extremo lejano tengan que soportar el RSVP, ni implica el empleo de una estrategia de QoS de extremo a extremo de servicios integrados (IntServ [13]). Se pueden utilizar, por ejemplo, servicios diferenciados (DiffServ [16] u otros esquemas de QoS más allá del CMTS. Además, los encaminadores intermedios que no deseen soportar el RSVP pueden pasar los mensajes RSVP simplemente sin procesamiento. Otro es el caso cuando se pueden obtener garantías de QoS por

otros medios; en tal situación, esos encaminadores pueden definirse como regiones de agregación y por tanto pasar mensajes RSVP transparentemente como se define en RFC 3175 [20].

NOTA – RFC 3175 requiere la implementación de esta función de agregación tanto en el encaminador de borde del extremo cercano como en el del extremo lejano.

Cabe observar, además, que la utilización de RSVP en este escenario se atiene de manera muy estricta al funcionamiento normalizado de RSVP (es decir, la norma RFC 2205) y, por tanto, las reservas de recurso en la red de acceso son unidireccionales. Así pues, el cliente reserva recursos en sentido ascendente y el extremo lejano es responsable de la reserva de recurso en sentido descendente.

Las reservas de recurso exitosas se mantienen de manera similar a las reservas en los demás escenarios vía renovaciones de estados flexibles. Los clientes RSVP deben enviar mensajes periódicamente para mantener sus reservas o dichas reservas caducarán y serán recuperadas en el CMTS.

Por último, en el protocolo RSVP se incluyen mecanismos específicos que permiten que el punto de extremo transmisor o el punto de extremo receptor señalen la terminación y eliminación de un flujo de servicio. En base a la naturaleza unidireccional de las reservas RSVP, un punto de extremo que mantenga múltiples flujos de servicio es responsable de la supresión explícita de cada uno de esos flujos al concluir una sesión de servicio.

Teniendo en cuenta este modelo, la autenticación de una petición de extremo lejano de habilitación de la reserva de recurso en sentido descendente requiere una consideración especial. Una solución consiste en exigir que el servidor de política pueda autenticar tanto a los clientes del extremo cercano como a los del extremo lejano. Son posibles también otras soluciones, pero deben ser analizados cuidadosamente los aspectos relativos a la seguridad y, en particular, la posibilidad de que el servicio sea objeto de hurto.

I.6.1 Ejemplo: Juegos en línea vía señalización de QoS inherente

Un posible servicio, que puede aprovechar el escenario 3, es el de los juegos en línea. En este ejemplo, todo lo que se necesitaría es el soporte integrado del RSVP basado en normas por parte del cliente. Es decir, los juegos en línea podrían diseñarse para funcionar con o sin un servidor de aplicación.

Cuando un cliente deseara participar en un juego, sólo tendría que enviar un mensaje específico de la aplicación al extremo lejano y pedir, a continuación, la QoS de red enviando un mensaje RSVP, dirigido de nuevo al punto de extremo lejano. Cuando el CMTS recibiera este mensaje, enviaría una petición al servidor de política para autenticar al cliente y decidir si debe concederse o no la QoS. Una autorización exitosa daría lugar a una reserva de QoS unidireccional.

De manera similar, el extremo lejano enviaría un mensaje RSVP dirigido al cliente. Una vez más, cuando se recibiera en el CMTS, ese mensaje sería enviado al servidor de política para determinar si debe concederse la QoS. Tras la debida autorización y el ofrecimiento del servicio al cliente, éste tendría QoS en ambos sentidos de transmisión y podría proseguir con el juego en línea.

I.7 Comparación entre IPCablecom-T y multimedia IPCablecom

En esta cláusula se hace una descripción de alto nivel de las diferencias principales entre la arquitectura IPCablecom-T y la arquitectura de multimedia IPCablecom. Hay que tener en cuenta que la mayoría de las características del protocolo específico y los detalles funcionales de los multimedia IPCablecom están pendientes de definición cuando se escribe la presente Recomendación. Véase el cuadro I.7 en el que se presentan las diferencias conocidas de forma resumida para una referencia rápida.

Cuadro I.7/J.179 – Comparación entre IPCablecom-T y multimedia IPCablecom

	IPCablecom-T	Multimedia IPCablecom
Servicios soportados	Telefonía residencial Características de la telefonía residencial básico Características de la telefonía ampliada	Servicios multimedia Basados en el cliente (par a par) Basados en el servidor
Mensajería de eventos	Pista de auditoría sólida para todos los eventos de política y QoS Soporta el modelo de facturación RTPC	Pista de auditoría sólida para todos los eventos de política y QoS Soporta la contabilidad basada en QoS Soporta la contabilidad basada en el tiempo y el volumen
Capacidades QoS	Algoritmos de calendarización de QoS de CableModem Servicio de concesión no solicitada Servicio de concesión no solicitada con detección de actividad Características de anchura de banda Velocidad binaria constante. Sentidos ascendente/ descendente simétricos. Nivel de QoS garantizado Cliente a cliente (es decir, extremo a extremo vía modelo segmentado)	Algoritmos de calendarización de QoS de CableModem Servicio de concesión no solicitada Servicio de concesión no solicitada con detección de actividad • Interrogación secuencial en tiempo real • Interrogación secuencial no en tiempo real • Mejor esfuerzo con o sin prioridad Características de anchura de banda: • Velocidad binaria constante • Velocidad binaria variable • Sentidos ascendente/descendente simétricos • Sentidos ascendente/descendente asimétricos Nivel de QoS garantizado: • CMTS a CM (es decir, red de acceso)
Seguridad	Señalización y medios seguros Provisión de dispositivos y gestión de configuración seguras	COPS y RADIUS asegurados vía IPsec; gestión de claves mediante IKE con autenticación de claves precompartidas (IKE con certificados o gestión de claves kerberizadas son facultativos). La señalización de cliente queda fuera del alcance de este apéndice, por lo que no hay seguridad definida para la interfaz de señalización del cliente.

I.7.1 DQoS

El interés de IPCablecom-T se centra fundamentalmente en los servicios de telefonía residencial. Como parte del presente esfuerzo, se elaboró la especificación de la calidad de servicio dinámica (DQoS), definiendo los mecanismos necesarios para entregar QoS en la porción de acceso basado en la tecnología CableModem de la red IP. Es decir, IPCablecom-T adopta un planteamiento segmentado (dividiendo los medios y el trayecto de señalización de extremo a extremo en redes de acceso cercano y lejano unidas por una red medular) en el que la DQoS se refiere de manera específica a las reservas de recurso en el segmento de acceso, no se trata de la QoS medular o de extremo a extremo.

Los multimedia IPCablecom están orientados hacia aplicaciones multimedia más generales, que trascienden el soporte de la voz. Sin embargo, se basan en algunos mecanismos fundamentales de DQoS de IPCablecom-T para proporcionar a esas aplicaciones servicios con QoS mejorada.

I.7.1.1 Elementos de red de acceso

IPCablecom-T soporta los elementos de red siguientes: MTA, CM, CMTS, CMS (compuestos lógicamente por un agente de llamada y un controlador de puerta) y RKS. En la arquitectura de multimedia IPCablecom se puede establecer funcionalmente la correspondencia entre el agente de llamada y un gestor de aplicación, y se puede establecer funcionalmente la correspondencia entre el controlador de puerta y el servidor de política. En la arquitectura de multimedia IPCablecom, se pueden introducir elementos de red adicionales, incluyendo, por ejemplo, un servidor de medios. El gestor de aplicación y el servidor de medios pueden estar ubicados físicamente en el mismo equipo o pueden estar instalados por separado.

I.7.1.2 Arquitectura de DQoS

La arquitectura de DQoS de IPCablecom [9] se basa en políticas de CableModem, RSVP+ y QoS instaladas en el CMTS por el CMS (controlador de puerta).

Como se ha descrito a lo largo del presente apéndice, la arquitectura de multimedia IPCablecom se basa también en esas tecnologías. Además, el esfuerzo multimedia tiene como objetivo soportar un modelo de señalización RSVP más normalizado (escenario 3) para que esa aptitud haga que los servicios con QoS mejorada estén a disposición de un colectivo mayor de consumidores.

El CMTS de la arquitectura de DQoS de IPCablecom-T sirve como punto de puesta en vigor de las políticas de QoS. El CMTS llevará a cabo una función similar en la arquitectura de multimedia IPCablecom. Además de atender las peticiones de QoS procedentes de los clientes, el CMTS puede también recibir peticiones de QoS formuladas mediante apoderado y procedentes del servidor de política (escenario 1). Esto difiere de la arquitectura de DQoS de IPCablecom-T, en donde sólo el MTA autónomo o el MTA incorporado pueden iniciar la activación de QoS.

I.7.1.3 Interfaces de QoS

En la arquitectura IPCablecom-T se han definido interfaces de señalización entre todos los elementos de red, así como también entre los CMTS en el caso de llamadas en red a llamadas en red que soportan la coordinación de puertas. En resumen, el protocolo de señalización principal entre el MTA y el agente de llamada es NCS, entre el MTA incorporado y el CMTS es CableModem y entre un MTA autónomo y el CMTS es RSVP+. La señalización del controlador de puerta al CMTS es mensajería de control por puerta basada en el COPS.

Los multimedia IPCablecom se basan en estas interfaces de señalización y soportan adicionalmente interfaces de señalización entre el gestor de aplicación y el servidor de política. Hay que recordar que toda señalización específica de la aplicación que se produzca entre el gestor de aplicación y sus clientes está fuera del ámbito de la presente arquitectura.

I.7.1.4 Marco de QoS de IPCablecom

En la arquitectura de QoS de IPCablecom-T, "un constructivo definido por la QoS llamado puerta proporciona el punto de control para la conexión de redes de acceso a un servicio medular de alta calidad". (Véase la especificación de DQoS [14].) La puerta representa una autorización de QoS que se instala en el CMTS a efectos de aplicación de políticas. Los multimedia IPCablecom definen un constructivo de política de QoS similar y se prevé que el constructivo de puerta DQoS de IPCablecom-T será perfeccionado para que proporcione la función de política en multimedia IPCablecom. Quizá se requiera introducir cambios en los mecanismos de control por puerta de IPCablecom-T existentes para proporcionar un control de QoS atenuado (por ejemplo, en soporte del escenario 1).

I.7.1.5 Requisitos de la gestión de recursos de red de acceso

La arquitectura IPCablecom-T "pretende proporcionar un alto grado de generalización con miras a habilitar nuevos servicios y la evolución futura de las arquitecturas de red". Este objetivo plantea varios requisitos para que una arquitectura de QoS sea viable en las áreas siguientes (se señala que cada una de estas capacidades relacionadas con la QoS se analiza y define de manera precisa en la especificación de DQoS de IPCablecom):

- Cambios de recurso durante una sesión.
- Vinculación dinámica de recursos.
- Clase de sesión (designación de prioridad).
- Compromiso de recurso bifásico.
- Asignación de recurso segmentada.
- Soporte de QoS medular.
- Prevención del hurto de un servicio.

La arquitectura de multimedia IPCablecom debe soportar también un modelo de reserva de recurso monofásico. Inicialmente, la arquitectura de multimedia no se referirá al soporte de QoS medular, aunque esta funcionalidad puede ser tratada formalmente según lo que impongan las necesidades del operador. Para más información sobre los requisitos de DQoS de IPCablecom-T, véase la especificación de DQoS de IPCablecom-T [14].

I.7.1.6 Teoría del funcionamiento

La DQoS de IPCablecom-T implica fases de reserva y compromiso distintas para obtener recursos de red de acceso. Al final de la fase de reserva, los recursos han quedado reservados pero todavía no están activos ni a disposición del MTA. Al final de la segunda fase, los recursos están comprometidos y disponibles para su utilización. En el modelo de telefonía tradicional, la facturación comienza en la fase de compromiso.

En el modelo de MTA incorporado, no se requiere RSVP+ entre el MTA y el CMTS. El E-MTA puede, en cambio, señalar reserva y compromiso de recursos vía mensajería DSx de CableModem. En el modelo de MTA autónomo, se utiliza mensajería de RSVP+ para llevar a cabo esos pasos. El CM y el CMTS se coordinan a continuación mediante mensajería DSx de CableModem para programar los flujos de servicio requeridos en la red de acceso.

Como se ha indicado en el presente apéndice, los multimedia IPCablecom soportan un modelo similar al de IPCablecom-T y admiten además una utilización más normalizada del RSVP. Además, proporcionan un modelo de petición de QoS mediante apoderado, en el que el gestor de aplicación gestiona la QoS en nombre del cliente. Estos modelos se detallan en la cláusula relativa a escenarios del presente apéndice. El modelo IPCablecom-T existente se corresponde con el escenario 2. Los otros dos modelos se soportan en la arquitectura de multimedia IPCablecom para una mayor flexibilidad de la manera en que se pueden desplegar los servicios multimedia en la red del operador.

I.7.2 Mensajes de evento para la facturación

Los mensajes de evento de IPCablecom están concebidos de modo que sean flexibles y ampliables para llevar información sobre la utilización de la red por parte de una gran variedad de servicios entregados por la arquitectura IPCablecom. La especificación de los mensajes de evento de IPCablecom-T define la arquitectura general del mensaje de evento así como los requisitos específicos para el soporte de un servicio de voz de los IPCablecom-T. La especificación de los mensajes de evento de IPCablecom (Rec. UIT-T J.164) da los detalles de una codificación TLV de mensaje de evento independiente del protocolo de transporte, un formato de fichero de mensajes de evento y protocolos de transporte obligatorios y facultativos.

Estos mensajes contienen información suficiente de cada sesión como para soportar la facturación del servicio al cliente. La información contenida en los mensajes de evento soporta una amplia gama de modelos de facturación y liquidación. IPCablecom no impone la utilización de modelos de facturación o liquidación específicos ya que esos modelos son definidos por, y se fundamentan en, los requisitos comerciales básicos del operador de cable de que se trate. IPCablecom tampoco impone ni excluye la utilización de una oficina de compensación para efectuar las liquidaciones.

Los mensajes de evento de IPCablecom se basan en un modelo en el que una sesión o servicio se divide en una mitad origen y una mitad terminación. El CMS o MGC de origen debe generar un ID de correlación de facturación (BCID) único para identificar todos los mensajes de evento asociados a la mitad origen de la sesión. El CMS o MGC de terminación debe generar un BCID único para identificar todos los mensajes de evento asociados a la mitad terminación de la sesión. Para cada mitad de la sesión o servicio, el conjunto de elementos de red IPCablecom que generan mensajes de evento (CMS, MGC, CMTS) debe proporcionar toda la información que se requiera a efectos de facturación y/o liquidaciones según proceda, dependiendo del servicio. La información generada por la mitad origen debe ser enviada al RKS que soporta la mitad origen. La información generada por la mitad terminación debe ser enviada al RKS que soporta la mitad terminación.

Los servicios multimedia IPCablecom requieren un conjunto limitado de mensajes de evento. Entre esos mensajes figuran los siguientes:

- Signal_Start para "servicio con QoS mejorada" generado por el servidor de política, que indica el momento en que el servidor de política recibe una petición de QoS de red de acceso.
- Signal_Stop para "servicio con QoS mejorada" generado por el servidor de política, que indica el momento en que el servidor de política recibe la notificación de que la utilización de QoS de la red ha terminado.
- QoS_Reserve, QoS_Commit y QoS_Stop generados por el CMTS. Estos mensajes indican el momento en que el CMTS reserva, compromete o libera QoS de la red de acceso.

I.7.3 Seguridad

La arquitectura de seguridad IPCablecom-T define los mecanismos, algoritmos y protocolos que cumplen los requisitos del servicio de seguridad. Las interfaces de multimedia IPCablecom se aseguran utilizando mecanismos idénticos para las interfaces correspondientes.

Apéndice II

Directrices para la asignación del número de versión

La interoperabilidad entre diferentes versiones del protocolo se basa en los siguientes principios:

Principio de robustez:

La RFC 791 define el "principio de robustez" para el protocolo Internet como sigue:

– "Una implementación debe ser conservadora en su comportamiento en emisión y liberal en su comportamiento en recepción."

– Siguiendo este principio de robustez, es posible permitir pequeños cambios en el protocolo pero manteniendo la compatibilidad con versiones anteriores.

La regla general de numeración de las versiones del protocolo en el marco del protocolo de control de puerta multimedia PacketCable, es la siguiente:

– Las versiones del protocolo que tienen el mismo número de versión principal DEBEN ser compatibles con las anteriores. Las versiones que tienen el número de versión principal diferente no se cree que sean compatibles.

– Es crucial que el equipo encargado de la especificación multimedia PacketCable examine todos los cambios del protocolo que vayan a incluirse en una nueva versión del mismo y seleccione un número de versión del protocolo basado en el cambio de mayor repercusión. Si alguno de los cambios satisface los criterios para cambiar el número de una versión principal del protocolo, éste debe incrementarse.

Ejemplos de cambios del protocolo que darían lugar a un cambio en el número de versión secundaria:

– La introducción de un nuevo objeto opcional, siempre que la inclusión del nuevo objeto en un mensaje no introduzca nuevos requisitos funcionales obligatorios en el elemento de red que recibe el mensaje, de modo que el objeto pueda ser ignorado sin problemas.

– La desaprobación de un objeto opcional.

Ejemplos de cambios del protocolo que darían lugar a un cambio en el número de versión principal:

– La introducción de un nuevo mensaje.

– Un cambio en el formato de un determinado objeto.

– Un cambio gramatical que prohibió la inclusión de un determinado objeto en un mensaje dado.

– Un cambio gramatical que hizo un objeto obligatorio en un determinado mensaje.

– Un cambio gramatical que hizo un objeto opcional en un mensaje en el que anteriormente, era obligatorio.

– La introducción de un nuevo objeto opcional que cuando se incluyó en un mensaje introdujo nuevos requisitos funcionales obligatorios en el elemento de red que recibe el mensaje, de modo que el objeto pueda ser ignorado sin problemas.

– Un cambio semántico en los algoritmos del protocolo o los estados (por ejemplo, en la máquina de estados de una puerta) que pudiera dar lugar a una incoherencia de estados entre dispositivos que aplican la versión nueva y la antigua del protocolo.

Algunos cambios, tales como los que introducen nueva funcionalidad, son difíciles de clasificar. Por ejemplo, podría imaginarse un cambio que introduzca un nuevo objeto y requisitos funcionales para el elemento de red que recibe el objeto en un mensaje. Si dicho elemento estaba operando con una versión inferior del protocolo en la que el nuevo objeto no estaba definido, el comportamiento por

defecto sería ignorar ese objeto y, por consiguiente, no se produciría el comportamiento implicado por el nuevo objeto. Si el nuevo comportamiento que no se produce debido a que el objeto que se ignora era local para el elemento de red receptor, podría argumentarse que en este caso los dos elementos de red están interoperando correctamente en la versión inferior del protocolo. En cambio, si la presencia del nuevo objeto en un mensaje exige que el elemento de red receptor envíe una nueva respuesta o modifique una respuesta existente, ignorar el nuevo objeto podría entonces impedir la interoperabilidad. En este último caso se requeriría un cambio de la versión principal.

Otros cambios, tales como los que cambian el estatus de un objeto en un mensaje de obligatorio a opcional, o viceversa, podrían dar lugar a implementaciones interoperables, dependiendo del comportamiento del emisor. No obstante, dado que el comportamiento del emisor en lo que respecta a parámetros opcionales no puede garantizarse, esos cambios deben considerarse principales.

Dado que existen muchos tipos de modificación del protocolo que requerirían un cambio de versión de protocolo principal, es razonable agrupar los cambios del protocolo para que los cambios de versión principal se produzcan con poca frecuencia y las nuevas versiones aporten un valor considerable que justifique su implementación.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2006