Unión Internacional de Telecomunicaciones

# UIT-T J.163

(11/2005)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

IPCablecom

## Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable

Recomendación UIT-T J.163

UIT-T

Unión Internacional de Telecomunicaciones

# Recomendación UIT-T J.163

## Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable


**Resumen**

Esta Recomendación trata de los requisitos que debe cumplir un dispositivo de cliente para acceder a los recursos de la red. En particular, se especifica un mecanismo completo para que el dispositivo de cliente solicite una calidad de servicio específica de la red DOCSIS. Numerosos ejemplos ilustran la utilización de esta Recomendación, cuya finalidad es definir una arquitectura de calidad de servicio (QoS) para la sección de "acceso" de una red de comunicaciones por cable que el protocolo IP (IPCablecom), que se pone a disposición de cada uno de los flujos de las aplicaciones que la solicitan. La sección de acceso de la red se define como la parte entre el adaptador del terminal de medios (MTA) y el sistema de terminación del módem de cable (CMTS), incluida la red DOCSIS. En esta Recomendación no se especifica el método de atribución de QoS a través de la red troncal. La interfaz con la red troncal IP gestionada y las cuestiones relacionadas con la multidifusión IP quedan fueran del alcance de la presente Recomendación. Esta Recomendación también tiene en cuenta que puede ser necesario efectuar reservas para cada flujo en las instalaciones del cliente, y el protocolo desarrollado trata esta posible necesidad.



**Orígenes**

La Recomendación UIT-T J.163 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

# Recomendación UIT-T J.163

## Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable

### 1 Alcance

Esta Recomendación trata de los requisitos que debe cumplir un dispositivo de cliente para acceder a los recursos de la red. En particular, se especifica un mecanismo completo para que el dispositivo de cliente solicite una calidad de servicio específica de la red DOCSIS. Numerosos ejemplos ilustran la utilización de esta Recomendación, cuya finalidad es definir una arquitectura de calidad de servicio (QoS, *quality of service*) para la sección de "acceso" de una red de comunicaciones por cable que el protocolo IP (IPCablecom), que se pone a disposición de cada uno de los flujos de las aplicaciones que la solicitan. La sección de acceso de la red se define como la parte entre el adaptador del terminal de medios (MTA, *media terminal adapter*) y el sistema de terminación del módem de cable (CMTS, *cable modem termination system*), incluida la red DOCSIS. En esta Recomendación no se especifica el método de atribución de QoS a través de la red troncal. La interfaz con la red troncal IP gestionada y las cuestiones relacionadas con la multidifusión IP quedan fueran del alcance de la presente Recomendación. Esta Recomendación también tiene en cuenta que puede ser necesario efectuar reservas para cada flujo en las instalaciones del cliente, y el protocolo desarrollado trata esta posible necesidad.

### 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.

- Recomendación UIT-T J.83 (1997), *Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable*.
- Recomendación UIT-T J.112 (1998), *Sistemas de transmisión para servicios interactivos de televisión por cable*.
- Recomendación UIT-T J.112 anexo A (2001), *Difusión de vídeo digital: Canal de interacción para sistemas de distribución de televisión por cable en difusión de vídeo digital*.
- Recomendación UIT-T J.112 anexo B (2004), *Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia*.
- Recomendación UIT-T J.160 (2005), *Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable*.
- Recomendación UIT-T J.161 (2001), *Requisitos de los códecs de audio para la prestación de servicios de audio bidireccionales por redes de televisión por cable que utilizan módems de cable*.

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

## 2.2 Referencias informativas

– Recomendación UIT-T G.114 (2003), *Tiempo de transmisión en un sentido*.

– Recomendación UIT-T G.711 (1988), *Modulación por impulsos codificados (MIC) de frecuencias vocales*.

– Recomendación UIT-T G.726 (1990), *Modulación por impulsos codificados diferencial adaptativa (MICDA) a 40, 32, 24, 16 kbit/s*.

– Recomendación UIT-T G.728 (1992), *Codificación de señales vocales a 16 kbit/s utilizando predicción lineal con excitación por código de bajo retardo*.

– Recomendación UIT-T G.729 anexo E (1998), *Algoritmo de codificación de la voz a 11,8 kbit/s mediante predicción lineal con excitación por código algebraico de estructura conjugada*.

– Recomendación UIT-T J.162 (2005), *Protocolo de señalización de llamada de red para la prestación de servicios dependientes del tiempo de redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.164 (2005), *Requisitos de los mensajes de eventos para el soporte de servicios en tiempo real transmitidos mediante redes de televisión por cable que utilizan módems de cable*.

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

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program – Protocol specification*.

– IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal control*.

– IETF RFC 2327 (1998), *SDP: Session Description Protocol*.

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

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

# 3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

**3.1 módem de cable**: Un módem de cable es un dispositivo de terminación de capa dos en el que termina el extremo de cliente de una conexión J.112 (o J.122).

**3.2 flujo DOCSIS**: Flujo unidireccional o bidireccional de paquetes de datos que está sujeto a señalización de capa MAC y a la asignación de calidad de servicio conforme con lo establecido en la Rec. UIT-T J.112 (o Rec. UIT-T J.122).

**3.3 IPCablecom**: Proyecto del UIT-T que incluye una arquitectura y una serie de Recomendaciones que permiten la distribución de servicios en tiempo real sobre redes de televisión por cable utilizando módems de cable.

## 4 Abreviaturas y convenios

### 4.1 Abreviaturas, siglas o acrónimos

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

CM Módem de cable (*cable modem*)

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

COPS Servicio de política común abierta (*common open policy service*)

CPE Equipo en las instalaciones del cliente (*customer premises equipment*)

DCS Señalización de llamada distribuida (*distributed call signalling*)

DSA Adición de servicio dinámica (*dynamic service addition*)

DSC Cambio de servicio dinámico (*dynamic service change*)

INA Adaptador de red interactivo (*interactive network adapter*)

IP Protocolo Internet (*Internet protocol*)

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

NCS Señalización de llamada de red (*network-based call signalling*)

PHS Supresión de encabezamiento de cabida útil (*payload header suppression*)

QoS Calidad de servicio (*quality of service*)

RAP Protocolo de asignación de recursos (*resource allocation protocol*)

RSVP Protocolo de reserva de recursos (*Resource reSerVation Protocol*)

RTPC Red telefónica pública conmutada

TLV Tipo-Longitud-Valor (*type-length-value*)

VAD Detección de actividad vocal (*voice activity detection*)

### 4.2 Convenios

Las palabras utilizadas para indicar determinadas condiciones se escriben en mayúsculas en toda la Recomendación:

"DEBE(N)" Esta palabra, o el adjetivo "REQUERIDO", significa que el elemento en cuestión 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 decidir 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 "OPCIONAL"o "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 Presentación técnica general

La calidad de servicio mejorada es necesaria para poder ofrecer aplicaciones multimedia interactiva. Es necesaria una asignación de recursos en la red debido a la posible limitación de recursos disponibles en determinados segmentos. El alcance de esta Recomendación es definir la arquitectura de calidad de servicio para la sección de "acceso" de la red IPCablecom. La sección de acceso es la parte de la red comprendida entre el adaptador de terminal multimedia (MTA, *multimedia terminal adapter*) y el sistema de terminación de módem de cable (CMTS, *cable modem termination system*), incluyendo la red DOCSIS. En esta Recomendación también se reconoce que puede ser necesario realizar reservas para cada flujo en las instalaciones del cliente, y se definen unos protocolos adaptados. Aunque algunos segmentos de la red troncal pueden necesitar la reserva de recursos para proporcionar una calidad de servicio adecuada, se considera que los protocolos de red troncal para la gestión de recursos quedan fuera del ámbito de esta Recomendación.

En una red DOCSIS se atribuyen recursos a flujos individuales asociados a cada una de las sesiones de una aplicación, para cada abonado y aplicando reglas de autorización y autenticación. En el contexto de esta Recomendación, una sesión con calidad de servicio dinámica (DQoS), o simplemente una sesión, es un flujo de datos bidireccional entre dos clientes. Cuando una aplicación multimedia necesita múltiples flujos de datos bidireccionales (por ejemplo, uno para voz y otro separado para vídeo), se establecen sesiones separadas con una determinada QoS dinámica para cada uno de ellos. Algunas aplicaciones utilizan sólo la mitad del flujo de datos bidireccional de la sesión, proporcionando servicios de sólo transmisión o de sólo recepción. Por ejemplo, en una aplicación de comunicación vocal típica, la comunicación simple entre dos partes se implementa mediante una única sesión, mientras que las comunicaciones complejas multipartitas (por ejemplo, "teleconferencias") se implementan mediante múltiples sesiones simultáneas.

El protocolo de señalización de llamadas IPCablecom definido es la señalización de llamada basada en la red (Rec. UIT-T J.162). Esta especificación de QoS dinámica es la referencia de calidad de servicio para ambos protocolos de señalización de llamada. La QoS se asigna a flujos asociados a una sesión de forma coordinada con el protocolo de señalización.

En esta Recomendación se introduce el concepto de marco de referencia de QoS segmento a segmento. La información disponible en los protocolos de señalización se utiliza para realizar asignaciones de QoS en el segmento "local" (la red DOCSIS cercana a la parte iniciadora) y en el segmento "distante" (la red DOCSIS cercana a la parte de terminación). Por lo tanto, esta Recomendación permite que distintos proveedores utilicen los mecanismos más apropiados para el segmento que están gestionando. La concatenación de segmentos con QoS permite proporcionar una garantía de QoS extremo a extremo para la sesión.

La especificación de QoS dinámica incorpora protocolos que permiten a los proveedores de comunicaciones de paquetes en el marco de IPCablecom utilizar distintos modelos de tasación, tanto tarifa plana como tasación en función del tiempo. Esta Recomendación pretende garantizar que la QoS mejorada sólo se proporcione a usuarios autorizados y autenticados. Las técnicas específicas utilizadas para autorizar y autenticar a un usuario quedan fuera del campo de aplicación de esta Recomendación.

Una de las hipótesis de la especificación de QoS dinámica es que un servicio de comunicaciones vocales no será comercialmente viable si no responde a los mismos requisitos de la red telefónica pública conmutada. Es importante garantizar que los recursos están disponibles antes de dar paso a la comunicación de las dos partes de una sesión. Por lo tanto, los recursos se reservan antes de que se notifique al receptor de la comunicación que alguien está intentando iniciar una comunicación. La sesión se bloquea si los recursos disponibles son insuficientes.

Los protocolos definidos en esta Recomendación reconocen explícitamente la necesidad de garantizar que no hay riesgos de fraude ni de robo del servicio por parte de puntos extremos que no aplican los protocolos de señalización de llamada y señalización de QoS, para no pagar por la utilización. Esta Recomendación introduce el concepto de reserva de recursos en dos fases (reserva y compromiso). Este principio permite al proveedor asignar recursos sólo cuando éstos han sido solicitados (cuando el trayecto vocal está establecido), lo cual puede utilizarse con fines de facturación, y también evitar el fraude y el robo del servicio, porque la segunda fase de compromiso de recursos necesita una petición explícita del MTA.

Esta Recomendación es compatible con el correspondiente documento PacketCable de CableLabs en sus aspectos técnicos: *PacketCable Dynamic Quality-of-Service Specification* PKT-SP-DQOS1.5 I01.

## 5.1 Requisitos de la arquitectura de calidad de servicio IPCablecom

A continuación se enumeran los requisitos de QoS para soportar aplicaciones multimedia sobre redes IPCablecom.

1) *Conocer los recursos de QoS de cada sesión para IPCablecom*

   En lo referente a la facturación, se considera que uno de los recursos que deberá tenerse en cuenta será la utilización de facilidades de QoS en una red DOCSIS. Por lo tanto, es necesario identificar información que permita asociar la utilización de recursos de QoS DOCSIS con la actividad de sesión IPCablecom.

2) *Modelos de activación de los criterios de QoS en dos fases (reserva-compromiso) y en una fase (compromiso)*

   Bajo el control de la aplicación, se deberá poder utilizar el modelo de activación de la QoS en dos fases o en una. En el modelo de dos fases, la aplicación reserva el recurso y ulteriormente lo compromete. En el modelo de una fase, la reserva y el compromiso se realizan mediante una única operación autónoma. Al igual que en el modelo DOCSIS, los recursos que están reservados pero no comprometidos están disponibles para su asignación temporal a otros flujos DOCSIS del servicio (por ejemplo, servicios "de mejor esfuerzo"). La presente Recomendación ofrece los mecanismos necesarios para la activación en dos fases y en una fase en el caso de MTA integrados.

3) *Proporcionar políticas definidas de IPCablecom destinadas a controlar la QoS en la red DOCSIS y en la red troncal IP*

   Es conveniente que distintos tipos de sesiones tengan distintas características de QoS. Por ejemplo, la QoS de sesiones en el dominio de un determinado proveedor operador de cable puede ser diferente de la QoS de las sesiones externas a dicho dominio (por ejemplo, sesiones internacionales que incluyan enlaces con la RTPC). Esta especificación de QoS dinámica permite que un operador de cable proporcione diferentes niveles de QoS para distintos tipos de clientes (por ejemplo, una QoS superior para abonados a un servicio comercial durante ciertas horas del día, en comparación con la ofrecida a los particulares) o para distintos tipos de aplicaciones de un mismo cliente.

4) *Prevenir (minimizar) la utilización abusiva de la QoS*

Se han identificado dos tipos de utilizaciones abusivas de la QoS: aquella que se factura correctamente, pero que provoca la denegación de servicio a otros, y aquélla que no se factura correctamente y supone un robo del servicio. Las aplicaciones de abonado y las aplicaciones IPCablecom (ya sean integradas o basadas en PC) pueden utilizar abusivamente, voluntaria o involuntariamente, sus privilegios de QoS (por ejemplo, utilizar para aplicaciones de tipo FTP una QoS que el proveedor desea limitar a aplicaciones vocales). Aunque la red DOCSIS regulará normalmente el acceso de los usuarios a la QoS, debe disponerse de una gran variedad de mecanismos de clasificación de paquetes y de control de señalización para impedir que el abonado (y los dispositivos del abonado) haga un uso fraudulento de la QoS. Deben utilizarse procedimientos de control de admisión a fin de reducir el número de ataques de denegación de servicio.

5) *Proporcionar mecanismos de control en los sentidos ascendente y descendente de las redes DOCSIS*

La QoS en los sentidos ascendente y descendente debe estar sujeta a un control de admisión para cada sesión.

6) *QoS DOCSIS*

Debe ser posible vigilar (marcar, descartar o retardar paquetes) todos los aspectos de la QoS definidos para el servicio en el CMTS mediante los mecanismos de QoS de DOCSIS. Además, se deben soportar varios modelos de correspondencia de flujos (asociar una sesión IPCablecom o múltiples sesiones IPCablecom a un único flujo del servicio).

7) *El CMTS aplica las políticas*

En última instancia, es prerrogativa del CMTS controlar las políticas. Cualquier cliente puede hacer una petición de QoS, pero el CMTS (o una entidad que actúa tras el CMTS) es la única entidad capacitada para conceder o denegar peticiones de QoS.

8) *Las entidades IPCablecom deben ignorar en la mayor medida posible las primitivas y parámetros específicos de QoS DOCSIS*

Para IPCablecom, como para cualquier aplicación que utilice una red IP, el objetivo de diseño es minimizar la cantidad de conocimiento específico del enlace de acceso que se incluye en la capa de aplicación. Cuanto menor conocimiento del enlace de acceso exista en la capa de aplicación, mayor será el número de aplicaciones disponibles para desarrollo y despliegue, y se encontrarán menos problemas en el ámbito de las pruebas y el soporte.

9) *Recuperación de recursos de QoS de sesiones inactivas/interrumpidas*

En el caso de sesiones inactivas que no se hubiesen cerrado adecuadamente, es necesario recuperar y atribuir los valiosos recursos de QoS. No debería haber "pérdidas" de recursos en el enlace DOCSIS Por ejemplo, si un módulo de cliente IPCablecom falla durante una sesión IPCablecom, deberían liberarse todos los recursos de QoS DOCSIS utilizados en dicha sesión tras un plazo razonable.

10) *Adaptar dinámicamente la política de QoS*

Conviene adaptar de forma dinámica las políticas de QoS de los abonados. Este requisito permite, por ejemplo, cambiar el nivel de servicio de un cliente (por ejemplo, pasar de un servicio "bronce" a un servicio "oro") mientras el mismo está activo sin tener que reinicializar el módem de cable.

11) *Tiempo mínimo absoluto de retardo para el establecimiento de una sesión y del retardo de posselección*

La red IPCablecom debe permitir emular y mejorar la experiencia del cliente en la RTPC, debiendo ser igualmente buena o mejor en lo que se refiere al tiempo de establecimiento y a la métrica del retardo de posselección.

12) *Gestionar múltiples sesiones concurrentes*

Conviene que se puedan asignar recursos de QoS (por ejemplo, anchura de banda) no sólo para sesiones individuales punto a punto, sino también para múltiples sesiones punto a punto (por ejemplo, teleconferencias, llamadas combinadas de audio/vídeo).

13) *Ajustar dinámicamente parámetros de QoS durante una sesión IPCablecom*

El servicio IPCablecom debe poder modificar la QoS en plena sesión, por ejemplo, para el ajuste de los recursos en todo el ámbito de la red o para la creación de parámetros compatibles del CÓDEC (que necesitan cambios de QoS), una característica definida por el usuario con distintos niveles de QoS o la detección de flujos de facsímil o de módem (que necesitan cambiar de un CÓDEC con compresión a la Rec. UIT-T G.711).

14) *Soportar múltiples modelos de control de QoS*

Puede considerarse que es importante iniciar la señalización de QoS desde el lado del abonado y también desde el lado de red. Desde el lado del abonado, una aplicación puede iniciar inmediatamente su petición cuando considere que necesita una determinada QoS. Asimismo, la señalización del lado de abonado soporta modelos de aplicaciones realizadas entre pares. En la señalización del lado de red, la implementación de una aplicación de punto extremo puede desconocer completamente la QoS (especialmente en la red DOCSIS). La señalización del lado de red soporta modelos de aplicación cliente-servidor (con un servidor fiable). Es previsible que ambos modelos coexistan en las redes IPCablecom (y en otras aplicaciones). La presente Recomendación sólo incluye la señalización del lado de abonado.

15) *Soportar señalización de QoS de un MTA integrado y un MTA autónomo*

Es conveniente que se puedan enviar mensajes de QoS tanto desde un adaptador de terminal de medios (MTA) integrado como desde un MTA autónomo. En esta Recomendación sólo se describen los MTA integrados que utilizan acceso directo a la señalización MAC DOCSIS.

## 5.2 Elementos de la red de acceso que intervienen en la calidad de servicio IP

Los siguientes elementos de red se utilizan para soportar la QoS en redes IPCablecom.

### 5.2.1 Adaptador de terminal multimedia (MTA)

Las características de los dispositivos de cliente de una red IPCablecom (es decir, MTA) pueden ser diferentes. Se encuentran en la instalación del usuario y están conectados a la red a través del canal DOCSIS. Se supone que todos los MTA implementan algún protocolo de señalización multimedia, tal como el J.162. Un MTA puede ser un dispositivo con un terminal telefónico a dos hilos en la configuración MTA-1, o incluir capacidades de entrada/salida de vídeo en la configuración MTA-2. Puede tener capacidades mínimas o bien implementar esta funcionalidad en una computadora personal multimedia, teniendo a su disposición todas las capacidades de la misma.

Desde el punto de vista de la QoS existen dos tipos de MTA.

1) **MTA integrado**: Es un terminal multimedia de cliente que incluye una interfaz de capa MAC DOCSIS con la red DOCSIS.

2) **MTA autónomo**: Es un dispositivo de cliente que implementa la funcionalidad multimedia sin incorporar una interfaz de capa MAC DOCSIS. El MTA autónomo utiliza típicamente Ethernet, USB o IEEE 1394 como modo de conexión física a un módem de cable. El MTA autónomo puede estar conectado a una red de cliente y utilizar facilidades de transporte de dicha red de cliente (posiblemente incluyendo encaminadores IP intermedios) para establecer sesiones sobre la red DOCSIS.

### 5.2.2 Módem de cable (CM)

El módem de cable (CM, *cable modem*) es un elemento de la red IPCablecom definido en la Rec. UIT-T J.112 o J.122. Su función es clasificar, vigilar y marcar los paquetes una vez que los protocolos de señalización definidos aquí han establecido los flujos de tráfico.

### 5.2.3 Sistema de terminación de módem de cable (CMTS)

El sistema de terminación de módem de cable (CMTS) se encarga de atribuir y programar la anchura de banda ascendente y descendente de conformidad con las peticiones del MTA y las autorizaciones de QoS establecidas por el administrador de red. El CMTS corresponde al punto de imposición de políticas (PEP, *policy enforcement point*) definido en el protocolo de asignación de recursos (RAP, *resource allocation protocol*) del IETF (RFC 2753).

El CMTS implementa una "puerta de QoS dinámica IPCablecom" (denominada simplemente "puerta" en esta Recomendación) entre la red DOCSIS y una red troncal IP. En la implementación de esta puerta se utilizan las funciones de clasificación y filtración de paquetes definidas en las Recs. UIT-T J.112 y J.122.

El CMTS se puede o no configurar como entidad "frontera IS-DS". Una entidad frontera IS-DS es una interfaz para funcionamiento combinado de redes, con el modelo de control de QoS de servicios integrados (IntServ) y otro modelo, por ejemplo el de servicios diferenciados (DiffServ).

### 5.2.4 Servidor de gestión de llamadas (CMS, *call management server*) y controlador de puerta (GC, *gate controller*)

La entidad servidor de gestión de llamadas (CMS) de IPCablecom realiza servicios que permiten al MTA establecer sesiones multimedia [incluyendo aplicaciones de comunicaciones vocales tales como "telefonía IP" o "voz sobre IP" (VoIP, *voice over IP*)]. El controlador de puerta (GC) es una sección del CMS (cualquiera de los dos tipos) que realiza funciones relacionadas con la calidad de servicio.

En el modelo de QoS dinámica de IPCablecom, el controlador de puerta (GC) controla el funcionamiento de las puertas implementadas en un CMTS. El GC corresponde al punto de decisión de políticas (PDP, *policy decision point*) del sistema de protocolo de asignación de recursos (RAP) del IETF (RFC 2753).

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

El servidor de mantenimiento de registros (RKS) es un elemento de red IPCablecom que sólo recibe información de elementos IPCablecom descritos en esta Recomendación. El RKS puede utilizarse como un servidor de facturación, herramienta de diagnóstico, etc.

## 5.3 Arquitectura de calidad de servicio dinámica de IPCablecom

La arquitectura de calidad de servicio (QoS) de IPCablecom se basa en la Rec. UIT-T J.112, en el RSVP del IETF y en el sistema de QoS garantizada de servicios integrados del IETF.

Específicamente, la arquitectura de QoS IPCablecom utiliza el protocolo definido en la Rec. UIT-T J.112 para la red de televisión por cable. Estos mensajes soportan la instalación estática y dinámica de clasificadores de paquetes (especificaciones de filtro) y mecanismos de planificación de flujos (especificaciones de flujos) destinados a proporcionar una calidad de servicio mejorada. La QoS DOCSIS se basa en objetos que describen el tráfico y las especificaciones de flujos, similares a los objetos TSpec y RSpec definidos en el protocolo de reserva de recursos (RSVP, *resource reservation protocol*) del IETF. Esta opción permite reservar recursos de QoS para cada flujo.

En la arquitectura de QoS DOCSIS se considera que los flujos de tráfico son unidireccionales y por consiguiente una sesión interactiva consta de dos flujos, cada uno de ellos sujeto a las operaciones que se indican a continuación. Para cada flujo (unidireccional):

Funciones del módem de cable (CM) a través del cual el tráfico accede a la red de cable con capacidad de QoS:

- Clasificar el tráfico IP en flujos de QoS IP conforme a determinadas especificaciones de filtro.
- Estructurar y vigilar el tráfico conforme a lo requerido por la especificación de flujo.
- Mantener el estado de los flujos activos.
- Modificar el campo tipo de servicio (TOS, *type of service*) en los encabezamientos de los paquetes IP ascendentes conforme a la política del operador de red.
- Obtener del CMTS la QoS requerida.
- Aplicar adecuadamente los mecanismos de QoS DOCSIS.

Funciones del CMTS:

- Proporcionar al CM la QoS requerida conforme a las políticas.
- Atribuir la anchura de banda en sentido ascendente de conformidad con las peticiones del CM y las políticas de QoS de la red.
- Clasificar cada paquete entrante desde la interfaz del lado de red y asignarlo a un nivel de QoS basado en determinadas especificaciones de filtro.
- Vigilar el campo TOS de los paquetes procedentes de la red de cable para garantizar la aplicación de los valores definidos en las políticas del operador de red.
- Modificar el campo TOS de los encabezamientos de paquetes IP descendentes conforme a la política del operador de red.
- Estructurar y vigilar el tráfico conforme a la especificación de flujo.
- Reenviar los paquetes descendentes hacia la red DOCSIS utilizando la QoS asignada.
- Reenviar los paquetes ascendentes a los dispositivos de red troncal utilizando la QoS asignada.
- Mantener el estado de los flujos activos.

La red troncal puede utilizar mecanismos de servicios integrados (Intserv) o de servicios diferenciados (DiffServ) del IETF. En el caso de una red troncal DiffServ, los encaminadores de la red reenvían un paquete aplicando la QoS IP adecuada en función de los valores del campo TOS. Los dispositivos de una red troncal DiffServ no tienen que mantener el estado de cada flujo.

### 5.4 Interfaces de calidad de servicio

Tal como se muestra en la figura 1, se definen interfaces de señalización de la calidad de servicio entre muchos de los componentes de la red IPCablecom. La señalización implica la comunicación de los requisitos de QoS en la capa de aplicación (por ejemplo, parámetros SDP), en la capa de red (por ejemplo, RSVP) y en la capa del enlace de datos (por ejemplo, QoS DOCSIS). Se necesitan otras interfaces entre componentes de la red IPCablecom para satisfacer los requisitos de aplicación de políticas y de enlaces entre los sistemas configuración de abonado en soporte de operaciones (OSS, *operation support systems*), de control de admisión en la red troncal IP y de control de admisión en la red DOCSIS.

En la Rec. UIT-T J.160, Arquitectura de IPCablecom se hace una descripción detallada de la arquitectura de QoS representada en la figura 1.

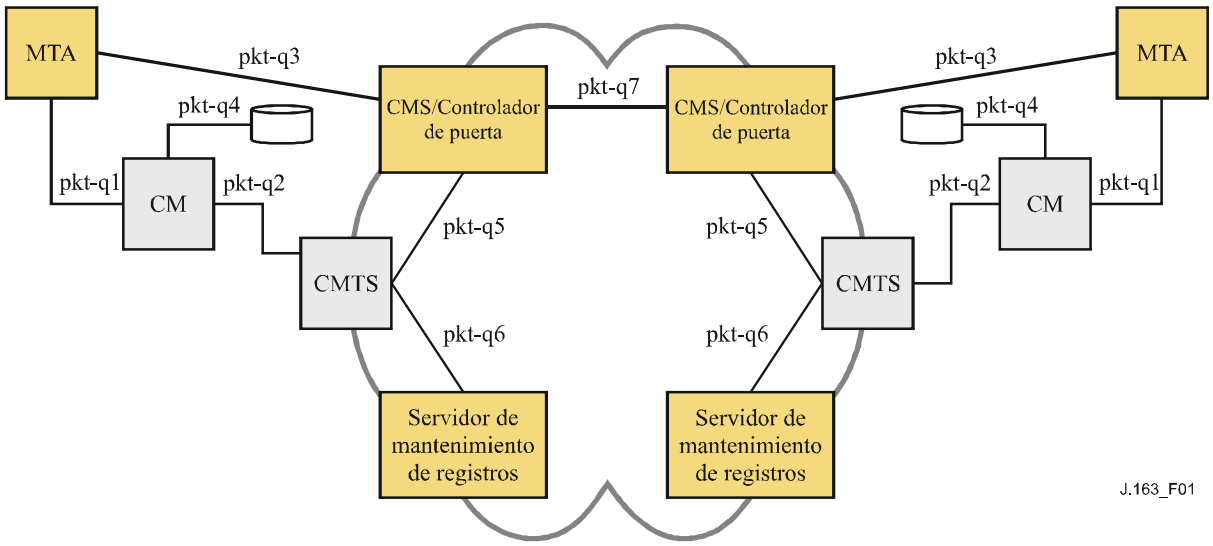



**Figura 1/J.163 – Interfaces de señalización de QoS en una red IPCablecom**

Las interfaces pkt-q1 a pkt-q7 están dedicadas al control y procesamiento de la QoS. No todas las interfaces se utilizan en todas las configuraciones y variantes de protocolos. Todas las interfaces, excepto la pkt-q5, se utilizan para la especificación de QoS dinámica (DQoS, *dynamic QoS specification*). En el cuadro 1 se identifica someramente cada interfaz y cómo se utilizan en la especificación de QoS dinámica.

**Cuadro 1/J.163 – Interfaces DQoS**

| Interfaz | Descripción | DQoS dinámica de MTA integrado (optional) |
|---|---|---|
| pkt-q1 | MTA-CM | Interfaz de capa MAC E-MTA |
| pkt-q2 | CM-CMTS | QoS DOCSIS, iniciada por el CM |
| pkt-q3 | MTA-GC/CMS | NCS |
| pkt-q4 | CM- Servidor de configuración | No disponible |
| pkt-q5 | GC-CMTS | Gestión de puerta |
| pkt-q6 | CMTS-RKS | Facturación |
| pkt-q7 | CMS-CMS | Señalización CMS a CMS |

### pkt-q1: Interfaz entre MTA y CM

Esta interfaz sólo se define para el MTA integrado. La interfaz se descompone en tres subinterfaces:

- Control: utilizada para gestionar flujos de servicio DOCSIS así como los parámetros de tráfico y las reglas de clasificación asociados (QoS).
- Sincronización: utilizada para sincronizar la paquetización y la planificación al objeto de minimizar el retardo y la fluctuación.
- Transporte: utilizada para procesar paquetes en el tren de medios y realizar el adecuado procesamiento de QoS de cada paquete.

El principio de esta interfaz está definido en la Rec. UIT-T J.112. No se ha definido ninguna configuración de esta interfaz para MTA autónomos.

**pkt-q2: Interfaz de QoS DOCSIS entre CM y CMTS**

Es la interfaz de QoS DOCSIS (control, planificación y transporte). Las funciones de control pueden ser iniciadas desde el CM o el CMTS. Sin embargo, el CMTS es el árbitro de políticas en última instancia y el asignador de recursos, controlando la admisión a la red DOCSIS. Esta interfaz se define en la Rec. UIT-T J.112.

**pkt-q3: Señalización de la capa de aplicación entre GC/CMS y MTA**

A través de esta interfaz se transmiten mensajes de señalización de muchos parámetros: el tren de medios, las direcciones IP, los números de puertos, la selección del códec y las características de paquetización. Los sistemas DCS y NCS son dos ejemplos de señalización de capa de aplicación.

**pkt-q4: Señalización entre el sistema de configuración DOCSIS/IPCablecom y el CM**

Esta interfaz no se utiliza para señalización de QoS en caso de QoS dinámica.

**pkt-q5: Interfaz entre GC/CMS y CMTS**

Esta interfaz se utiliza para gestionar las puertas dinámicas en sesiones de trenes de medios. Permite a la red IPCablecom solicitar y autorizar una QoS.

**pkt-q6: Interfaz entre CMTS y el servidor de mantenimiento de registros**

El CMTS utiliza esta interfaz para señalar al servidor de mantenimiento de registros (RKS) todos los cambios relativos a la autorización y utilización de la sesión.

**pkt-q7: Interfaz entre CMS y CMS**

Esta interfaz se utiliza para la gestión de la sesión y la coordinación de recursos entre un par de CMS.

## 5.5 Marco de referencia para la QoS de IPCablecom

Para que el usuario final considere justificados los costes de un servicio multimedia comercial (por ejemplo, capacidad de comunicaciones vocales) posiblemente habrá que ofrecer una elevada calidad de funcionamiento tanto en el transporte como en la señalización, incluyendo:

- Bajo retardo: el retardo de paquetes extremo a extremo debe ser suficientemente reducido para no afectar las interacciones multimedia normales. Para el servicio de telefonía normal en la RTPC, el UIT-T recomienda un retardo de ida y vuelta no superior a 300 ms[1]. Dado que el retardo de propagación extremo a extremo de la red troncal puede representar una parte significativa de este retardo total, es importante controlar el retardo en el canal de acceso, al menos para las llamadas de larga distancia.
- Baja pérdida de paquetes: la pérdida de paquetes debe ser suficientemente pequeña para que la calidad de la voz o la calidad de funcionamiento del fax o del módem de datos en banda vocal no se vea degradada de forma perceptible. Aunque se pueden utilizar algoritmos de compensación de pérdidas para reproducir la señal vocal de forma inteligible incluso con una elevada tasa de pérdidas, la calidad de funcionamiento resultante no permitirá considerar que el servicio es equivalente al servicio telefónico con conmutación de circuitos existente. Los requisitos para una calidad de funcionamiento aceptable de los módem en banda vocal son aún más exigentes que los aplicables a la señal vocal.

---

[1] En la Rec. UIT-T G.114 se establece que un retardo unidireccional de 150 ms es aceptable para la mayoría de las aplicaciones de usuario. Sin embargo, las aplicaciones muy interactivas de voz y datos pueden resultar degradadas por un retardo incluso inferior a 150 ms. Por lo tanto, conviene evitar siempre alargar el retardo de procesamiento (incluso en conexiones con tiempos de transmisión bastante inferiores a 150 ms), a no ser que haya claras ventajas para el servicio y la aplicación.

- Bajo retardo posterior a la marcación: es preciso que el retardo entre la petición de conexión de un usuario y la recepción de una confirmación de la red sea suficientemente reducido como para que el usuario no perciba un retardo postmarcación distinto al que está acostumbrado en la red con conmutación de circuitos, o que le haga pensar que la red ha tenido un fallo. Dicho retardo es de aproximadamente un segundo.
- Bajo retardo posterior al descuelgue: es preciso que el retardo entre el instante en que el usuario descuelga para atender una llamada y el establecimiento del trayecto vocal sea lo suficientemente corto para que no se recorte el "hola" inicial. Es del orden de unos pocos cientos de milisegundos (idealmente menos de 100 ms).

Una contribución clave del marco de la QoS dinámica es que se ha determinado la necesidad de coordinación entre la señalización, que controla el acceso a los servicios específicos de la aplicación, y la gestión de los recursos, que controla el acceso a los recursos de la capa de red. Esta coordinación proporciona varias funciones críticas. Garantiza que los usuarios serán autenticados y autorizados antes de acceder a la QoS mejorada asociada al servicio. Garantiza que los recursos de red estarán disponibles extremo a extremo antes de avisar al MTA de destino. Finalmente, garantiza que la utilización de recursos será contabilizada adecuadamente y a imagen de los convenios del servicio telefónico tradicional de calidad vocal (con el que se comparan algunos servicios IPCablecom, desde la perspectiva del cliente), en el cual la tasación sólo se inicia después de que la parte receptora de la comunicación haya descolgado.

Con objeto de soportar estos requisitos, los protocolos de QoS garantizan que todos los recursos están comprometidos en todos los segmentos de transporte antes de que los protocolos de señalización avisen al destino. Igualmente, cuando se deshace una sesión, los protocolos de QoS toman medidas para asegurar que todos los recursos dedicados exclusivamente a dicha sesión son liberados. Sin esta coordinación entre ambos sentidos del flujo de datos, los usuarios podrían burlar los controles de QoS y disponer de un servicio gratuito. Por ejemplo, si el cliente que paga da por terminada la sesión, y no así el que no paga, se mantiene disponible "medio canal" que puede ser utilizado de forma ilícita para transferir datos en un sentido. La semántica de transacciones de los protocolos de QoS es del tipo "todo o nada" para los aspectos de creación y destrucción de sesión.

Es conveniente que los mecanismos utilizados para implementar la sesión estén basados en normas y prácticas existentes y, asimismo, que el resultado de este trabajo pueda ser utilizado para soportar modelos de llamada alternativos. Esto ha llevado a la utilización del protocolo en tiempo real (RTP, *real time protocol*) del IETF para el transporte de datos multimedia, transportados sobre el protocolo de datagramas de usuario (UDP, *user datagram protocol*) del IETF. La señalización dentro de banda necesaria para establecer la QoS se transporta utilizando mensajes QoS dinámicos DOCSIS.

La arquitectura de QoS debe soportar nuevas aplicaciones emergentes que dependen de la distribución de datos en multidifusión. Aunque ello no constituye un requisito estricto en la arquitectura de QoS, el hecho de soportar la multidifusión, permitirá el futuro desarrollo de un amplio conjunto de aplicaciones multimedia. Aún no se ha analizado si las mejoras en la gestión de recursos que presenta esta Recomendación soportarán la multidifusión sin discontinuidad.

Para gestionar la calidad de servicio, el canal portador de una sesión se gestiona como si se tratara de tres segmentos distintos: la red de acceso para el lado origen de la sesión, una red troncal y la red de acceso para el lado de terminación de la sesión. Los recursos de la red DOCSIS se gestionan como dos flujos de servicio dinámicos utilizando los mecanismos definidos en la Rec. UIT-T J.112. Los recursos de la red troncal pueden ser gestionados para cada uno de los flujos o, más probablemente, utilizando un mecanismo de calidad de servicio global. La gestión de los recursos de la red troncal queda fuera del ámbito de esta Recomendación.

La *puerta* es un concepto definido en términos de QoS que constituye un punto de control para la conexión de las redes de acceso a un servicio de alta calidad de la red troncal. La puerta la implementa un CMTS y consta de un clasificador de paquetes, un elemento de implementación de la política de tráfico y una interfaz con una entidad que recopila estadísticas y eventos (todos estos componentes existen en la red DOCSIS). Una puerta asegura que sólo las sesiones que ha autorizado el proveedor de servicio recibirán una elevada calidad de servicio. Las puertas se gestionan de forma selectiva para cada flujo. En el caso de un servicio de comunicación vocal basado en IPCablecom se abre una puerta para cada llamada. La apertura de una puerta implica verificar el control de admisión cuando se recibe del cliente una petición de gestión de recurso para una determinada sesión, y puede implicar la reserva de recursos en la red para la sesión, si ello es necesario. El filtro de paquetes ascendentes de la puerta permite que un flujo de paquetes disponga de una QoS mejorada para una sesión desde una dirección y un número de puerto fuente IP específicos hacia una dirección y número de puerto de destino IP específicos. El filtro de paquetes descendentes de la puerta permite que un flujo de paquetes disponga de una QoS mejorada para una sesión desde una dirección de puerto fuente IP específicos hacia una dirección y número de puerto de destino IP específicos.

Una puerta es una entidad lógica que reside en un CMTS. Hay un identificador de puerta (*GateID*) para cada sesión, que tiene significado en la puerta; es un identificador singular a nivel local del CMTS y está asignado por dicho CMTS. Una puerta es unidireccional por naturaleza. Si una puerta está "cerrada", los datos que viajen en sentido ascendente o descendente en la red de acceso DOCSIS pueden ser descartados o cursados con las características de un servicio del tipo mejor esfuerzo. La elección entre descartar paquetes o atenderlos mediante un servicio del tipo mejor esfuerzo es una decisión del proveedor.

La función del controlador de puerta es decidir si una puerta debe estar abierta y cuándo. Dado que la puerta se establece con anterioridad a una petición de gestión de recursos, esta función de política localizada en el controlador de puerta se realiza sin contexto, es decir, no necesita conocer el estado de las sesiones en curso.

Si bien la puerta controla el tren con una QoS garantizada, otros flujos, tales como los mensajes de RTCP o los mensajes de señalización, no están sujetos a la política ejercida por la puerta. El soporte de una QoS mejorada para mensajes de señalización puede ser un elemento muy importante si el sistema de cable utiliza un tráfico considerable con servicio del tipo mejor esfuerzo. La utilización de un flujo de señalización dedicado con los conceptos de QoS apropiados podría ser fundamental para satisfacer los objetivos de calidad de señalización indicados al principio de este capítulo. Obsérvese que las características detalladas de la QoS que se atribuirá al flujo de señales dedicadas dependerá del tráfico y de la ingeniería del CMTS, y se dejan a discreción de los proveedores.

## 5.6 Requisitos de la gestión de recursos en la red de acceso

La prestación de servicios de comunicación vocal sobre redes IP con el mismo nivel de calidad que ofrece la red telefónica pública conmutada (RTPC) supone unos valores límite de pérdida y retardo de paquetes de voz y requiere una gestión activa de los recursos en las redes de acceso y en la red troncal. Es importante que el proveedor de servicio pueda controlar el acceso a los recursos de red para garantizar la capacidad extremo a extremo adecuada, incluso en condiciones extraordinarias o de sobrecarga. El proveedor de servicio puede tratar de conseguir ingresos adicionales por la prestación de un servicio de comunicaciones vocales con estas características de calidad mejoradas (una calidad superior a la que se obtiene con un servicio del tipo "mejor esfuerzo"). Los mecanismos que se proporcionan a continuación para la gestión del acceso a una QoS mejorada permiten al proveedor de servicio limitar el acceso a usuarios autorizados y autenticados de forma específica para cada sesión, y evitar el robo del servicio.

Los clientes del servicio informan de sus parámetros de tráfico y de calidad de funcionamiento a la "puerta" situada en el borde de la red, en donde la red toma decisiones de control de admisión sobre la base de los recursos disponibles y de la información relativa a la política asociada a dicha puerta.

Las redes DOCSIS tienen una capacidad limitada y es necesario gestionar los recursos de cada flujo. En la red troncal existen varias alternativas que van desde un control de admisión por flujo y por tramo hasta el aprovisionamiento de recursos de forma aproximada. Esta Recomendación sólo trata de la QoS de las redes de acceso y es neutra en relación con los esquemas de QoS de la red troncal.

### 5.6.1 Prevención del robo del servicio

Los siguientes mecanismos protegen contra la utilización indebida de los recursos de red dedicados a una sesión:

- Autorización y seguridad: garantiza que los usuarios son autenticados y autorizados antes de acceder a la QoS mejorada asociada al servicio de comunicaciones vocales. El CMS/controlador de puerta (GC) que participa en la señalización de la llamada tiene la función de hacer la verificación y es la única entidad que puede crear una nueva puerta en un CMTS. El CMS/GC actúa como un punto de decisión de política desde la perspectiva de la gestión de la QoS.
- Control de recursos: garantiza que la utilización de los recursos se contabiliza adecuadamente y a imagen de los convenios de proveedores de la RTPC, donde la tasación sólo se realiza cuando la parte llamada descuelga. Ello incluye prevenir la utilización de recursos reservados para fines distintos a la sesión a la que se asignan. Se consigue utilizando puertas y realizando una coordinación de las puertas que consiste en combinar mecanismos de filtrado de direcciones con la reserva de recursos.

Dado que este servicio puede facturarse en función de su utilización, existe un riesgo significativo de fraude y robo del servicio. Al permitir que el proveedor cobre por la calidad de servicio ofrecida, la arquitectura evita situaciones de robo del servicio, algunas de ellas se describen en el apéndice IX.

Esta y otras Recomendaciones incluyen medidas para evitar situaciones de robo del servicio, que son la razón de ser de algunos de los componentes de las arquitecturas y protocolos de QoS y de señalización de llamada.

### 5.6.2 Compromiso de recursos en dos fases

Para ofrecer servicios de comunicación vocal de calidad comercial es necesario un protocolo de compromiso de recursos en dos fases, por dos motivos que tienen que ver con los requisitos particulares. En primer lugar, garantiza que los recursos están disponibles antes de señalar una comunicación entrante a la parte del extremo distante. En segundo lugar, garantiza que el registro y la facturación por la utilización no comienzan hasta que el extremo distante ha descolgado, momento en el que también se establece la señal vocal entre las partes. Son propiedades que ofrecen los protocolos de señalización de telefonía convencional y se trata de emular la misma semántica en este documento. Por otra parte, si se asigna anchura de banda antes de que el extremo distante haya descolgado, hay un riesgo de robo del servicio. La exigencia de que los puntos extremos envíen explícitamente un mensaje de compromiso garantiza que el registro de utilización está basado en la utilización consciente de la parte extrema y sus acciones explícitas.

El marco de referencia también soporta entidades, tales como servidores de anuncios y pasarelas a la RTPC, que necesitan que la señal vocal se establezca después de la primera fase del protocolo de gestión de recursos.

### 5.6.3 Asignación de recursos segmentada

La arquitectura de QoS dinámica divide la gestión de recursos en segmentos diferenciados de acceso y de red troncal. La asignación de recursos segmentada es preferible por dos motivos:

- Permite que existan diferentes mecanismos de configuración de anchura de banda y de señalización para la red del origen, la red del extremo distante y la red troncal.
- Permite mantener reservas para cada flujo en segmentos con pocos recursos y gestionar cuidadosamente la utilización de los recursos. Asimismo, cuando los segmentos de red troncal tienen recursos suficientes que permiten una gestión de recursos menos detallada, la red troncal no tiene que mantener el control de estados de cada flujo, mejorando así la escalabilidad.

Cuando la red troncal no requiere una señalización explícita para cada flujo (como ocurre en el caso de una red troncal DiffServ), se reduce el tiempo necesario para establecer una sesión (se minimiza el retardo posterior a la marcación) y se evita que el tiempo de establecimiento de la señal vocal se vea afectado (minimiza el retardo posterior al descuelgue).

Puede reducir la importancia del estado de reserva que es necesario almacenar si el cliente distante es una pasarela RTPC.

Después de la primera fase de señalización de llamada, ambos clientes han finalizado su negociación y conocen los recursos extremo a extremo que son necesarios. Los clientes envían mensajes de gestión de recursos utilizando la interfaz de servicios de control MAC. El CMTS refleja los mensajes de gestión de recursos en el protocolo de gestión de recursos utilizado en la red troncal (por ejemplo, DiffServ del IETF). También refleja los mensajes de gestión de recursos en el protocolo de gestión de recursos utilizado en el enlace de acceso (es decir, DOCSIS).

### 5.6.4 Modificación de los recursos durante una sesión

Es posible modificar los recursos asignados a una sesión durante la misma. Esta posibilidad facilita cambios como la conmutación de un códec vocal de baja velocidad a un códec G.711 cuando se detectan tonos de módem durante la sesión, o añadir datos de vídeo a una sesión que se ha iniciado exclusivamente con voz.

### 5.6.5 Vinculación dinámica de recursos

La vinculación dinámica de recursos (segunda reserva) es un requisito que permite una utilización eficiente de recursos cuando se invocan servicios tales como llamada en espera. La segunda reserva consiste en tomar la anchura de banda que fue asignada para una sesión entre un anfitrión de VoIP y un cliente, y reasignarla a una sesión con un cliente distinto.

Es importante entender cabalmente los riesgos del procedimiento que consiste en desasignar la anchura de banda de una sesión y hacer otra petición para asignar de nuevo anchura de banda. Otro cliente podría utilizar la anchura de banda residual entre ambos pasos, dejando la sesión original sin un trayecto de calidad garantizada. El mecanismo de segunda reserva en un solo paso evita este riesgo, ya que la anchura de banda no queda en ningún momento a disposición de otros clientes.

### 5.6.6 Adaptación dinámica de la QoS

Los mensajes de QoS se intercambian en tiempo real mientras la parte llamante espera que los servicios sean activados o modificados. Por eso es necesario utilizar un protocolo rápido. Se reduce al mínimo el número de mensajes, especialmente el número de mensajes que transitan por la red troncal y el número de mensajes ascendentes DOCSIS.

Los mensajes de gestión DOCSIS y los mensajes de señalización de llamada (denominados en general mensajes de señalización) son todos transportados por la red DOCSIS con un servicio de tipo mejor esfuerzo. Si el CM también soporta servicios de datos, es posible que este servicio de tipo mejor esfuerzo no pueda proporcionar el bajo retardo de mensajes de señalización que es

necesario. En esta situación, se PUEDE configurar un flujo del servicio separado en el CM, con QoS mejorada, destinado a transportar tráfico de señalización. Por ejemplo, el flujo del servicio de señalización podría emplear el servicio de escrutinio en tiempo real o no tiempo real. Este flujo de servicio separado se configura de la misma forma que otros trenes de medios DOCSIS y PUEDE incluir clasificadores que hacen su presencia transparente para el MTA.

### 5.6.7 Clase de sesión

Los recursos pueden reservarse para distintos tipos de servicios, cada uno de los cuales puede a su vez definir clases de servicio diferentes para sus sesiones. Las reservas de QoS para sesiones que el proveedor de servicio designa con prioridad superior (por ejemplo, llamadas de emergencia), tienen una probabilidad de pérdida inferior que las sesiones normales. El proveedor de servicio determina la clase que se asigna a cada sesión, siendo ésta una política que ejerce el agente de llamada/controlador de puerta cuando se hace la petición de sesión inicial.

### 5.6.8 Soporte de redes intermedias

La arquitectura no debe impedir que existan redes intermedias entre el MTA o anfitrión multimedia y el CM (por ejemplo, una red de cliente). Aunque la red intermedia puede no estar bajo el domino administrativo o responsabilidad del operador de cable, cuando existe una red intermedia es posible asignar anchura de banda en la red DOCSIS del operador de cable. También es conveniente disponer de una solución que permita reservar recursos en la red intermedia de forma transparente.

### 5.6.9 Soporte de la calidad de servicio de la red troncal

Es posible que sean necesarios algunos mecanismos para la gestión explícita de los recursos de la red troncal. El alcance de esta Recomendación es la QoS en la red DOCSIS, pero la arquitectura proporciona interfaces abiertas y suficientemente generales que son compatibles con muchos de los mecanismos de QoS de la red troncal.

### 5.6.10 Funcionamiento con varios códecs

La señalización NCS de IPCablecom permite establecer conexiones con múltiples códecs. En las conexiones procesadas satisfactoriamente con una lista negociada de varios códecs, es importante asignar los recursos adecuados para que los cambios ulteriores de códec funcionen correctamente. Ahora bien, corresponde al CMS decidir cuándo autoriza anchura de banda durante la fase de establecimiento de llamada, y también controlar la eficacia que desearía en su capacidad máxima autorizada. Si decidiese autorizar anchura de banda antes de la instrucción CreateConnection NCS inicial (CRCX), tendría que basar la capacidad máxima autorizada en los parámetros LCO propuestos (dado que no conoce el subconjunto que el MTA pudiera negociar). Si el CMS espera a que se negocien los códecs en la fase de establecimiento de llamada, podrá autorizar un subconjunto de LCO basados en la lista negociada actual sin efecto negativo alguno (el DSA/DSC seguirá pasando la autorización). Es necesario asignar los siguientes recursos:

- Anchura de banda autorizada: Cuando el CMS pide al MTA que reserve o comprometa recursos mediante la inclusión de un ID de puerta (Gate-ID) en una instrucción NCS CreateConnection o ModifyConnection (CRCX o MDCX), el CMS TIENE QUE garantizar que la anchura de banda autorizada en la puerta gestionará toda petición de recursos legitima (DSA/DSC) que haga el MTA al CMTS como resultado del procedimiento de negociación de códecs. Dicho de otro modo, la anchura de banda autorizada por el CMS/GC TIENE QUE ser mayor o igual que el valor superior mínimo (LUB, *least-upper-bound*) de la lista de códecs negociada .
- Anchura de banda reservada: el MTA TIENE QUE reservar el mínimo valor superior de anchura de banda del códec que se podrá utilizar durante la llamada (los códecs se determinan en un proceso de negociación definido en 6.7/J.162).

  NOTA – Si la anchura de banda reservada es superior a la anchura de banda comprometida, habrá que renovar el primero enviando un mensaje de cambio de servicio dinámico (DSC) al CMTS.

- Anchura de banda comprometida: el MTA COMPROMETERÁ sólo el códec utilizado en sentido ascendente. Así, la anchura de banda adicional no utilizada (la diferencia entre los valores reservado y comprometido) se podrá utilizar para un tráfico de mejor esfuerzo. En sentido descendente, el MTA TIENE QUE comprometer el mínimo valor superior de anchura de banda del códec que se podrá utilizar durante la llamada (los códecs se determinan en un proceso de negociación definido en 6.7/J.162).

Este procedimiento garantiza que se atenderá satisfactoriamente la petición de un CMS para conmutar a uno de los códecs de la lista negociada. Es especialmente importante para soportar funciones como fax/módem que es necesario conmutar a G.711 para transmitir satisfactoriamente.

Si el proveedor del servicio considera que esta asignación de recursos es demasiado restrictiva con respecto al número de canales de voz soportados (la reserva de recursos puede ser excesiva en muchos casos), sólo es necesario que el CMS precise un códec en el campo LocalConnectionOptions de la petición de conexión. Así coincidirán los recursos reservados y comprometidos (se utiliza el mismo mecanismo del caso de varios códecs). Para cambiar el códec, el CMS hará una petición de modificación con otro códec en el campo LocalConnectionOptions. Ahora bien, esta solución tiene algunos riesgos; por ejemplo, al detectar y notificar al CMS una llamada de modem, es posible que la petición de modificación de conexión a G.711 no sea atendida porque no hay suficientes recursos en el CMTS. No ocurriría si se han definido varios códecs, porque ya habría un valor LUB reservado y de acceso garantizado para un compromiso ulterior.

### 5.6.11 Llamadas puerto a puerto en el MTA

Cuando se establecen comunicaciones vocales entre distintos puertos (puntos extremo) de un MTA, las reglas de transmisión DOCSIS especifican que el CM no debe transmitir paquetes sobre la red DOCSIS. Por tanto, las medidas que toman el CMS y el MTA en estas circunstancias particulares son diferentes del flujo de llamada habitual MTA a MTA. Los puntos extremo definen una llamada puerto a puerto utilizando la misma dirección IP.

Si un MTA recibe una petición de conexión sin GateID, NO INICIARÁ ningún mensaje DSx al CMTS. Si un MTA recibe instrucciones para hacer una llamada puerto a puerto, NO INICIARÁ ningún mensaje DSx para establecer un flujo de servicio para esa conexión NI ENVIARÁ paquetes de voz sobre la red. De otra parte, si el MTA había creado antes un flujo de servicio para una llamada sin el SDP del extremo distante (si se había especificado un GateID en un CRCX o MDCX), cuando reciba el SDP distante TIENE QUE desmontar el flujo de servicio si reconoce una llamada puerto a puerto.

El CMS DEBERÍA reconocer las llamadas puerto a puerto, DEBERÍA omitir el control de puerta en el CMTS y también DEBERÍA omitir el GateID en la instrucción de conexión al MTA. Como en el anterior caso del MTA, si el CMS ya ha establecido una puerta para una llamada sin el SDP del extremo distante, DEBERÍA esperar un mensaje Cerrar puerta del CMTS cuando el MTA desmonte el flujo de servicio al detectar una llamada puerto a puerto. El CMS NO DESMONTARÁ una llamada entre puntos extremo con la misma dirección IP al recibir el mensaje Cerrar puerta.

### 5.6.12 Múltiples autorizaciones por intervalo

Para utilizar eficientemente los recursos DOCSIS, el MTA PUEDE incluir múltiples subflujos con los mismos conjuntos de parámetros QoS en el mismo flujo de servicio. Dado que el tipo ServiceFlowScheduling (planificación de flujo de servicio) forma parte del conjunto de parámetros QoS, TIENE QUE ser idéntico en todos los subflujos que utilizan el mismo flujo de Servicio DOCSIS. Por ejemplo, si un flujo que admite supresión de silencios utiliza UGS/AD, y el flujo de servicio existente está configurado para utilizar sólo UGS, el nuevo flujo TIENE QUE ser creado en otro flujo de servicio. Por razones prácticas, cuando se utilicen varias autorizaciones por intervalo el tipo planificación de flujo de servicio no puede ser cambiado.

Esta característica es facultativa para el MTA. El CMTS DEBE poder utilizar un número de autorizaciones por intervalo mayor que 1. Si un MTA solicita varias autorizaciones por intervalo y el CMTS rechaza el mensaje DSx (es decir, el planificador CMTS no puede planificar adecuadamente esta petición en el flujo de servicio existente, pero puede atender esta petición en otro flujo de servicio), el MTA PUEDE repetir la petición por otro flujo de servicio (si hubiesen recursos suficientes).

El campo autorizaciones activas por intervalo en el encabezamiento MAC ampliado se utiliza para contabilizar las autorizaciones activas de un determinado flujo de servicio que contiene múltiples subflujos. Por ejemplo, si se tienen dos llamadas activas y una entra en modo supresión de silencios, el número de autorizaciones activas en el encabezamiento MAC ampliado pasará de 2 a 1. En este caso, no es necesario actualizar el DSC en el flujo, dado que la detección de actividad se basa en el flujo y no en la autorización. El número de autorizaciones por intervalo en el DSC sigue siendo 2 para los valores admitido y activo y sólo se requeriría actualización de flujo cuando las autorizaciones activas pasan a 0 todos los subflujos que entraron en el modo supresión de silencios. El número de autorizaciones activas por intervalo DEBE ser menor o igual que el número de subflujos.

Las reglas PHS DEBEN ser las mismas para todos los subflujos de un flujo de servicio.

## 5.7 Teoría de funcionamiento

### 5.7.1 Establecimiento de una sesión básica

La reserva de recursos se divide en dos fases separadas: reserva y compromiso. Cuando finaliza la primera fase los recursos están reservados pero aún no están disponibles para el MTA. (En los enlaces DOCSIS se permiten flujos de servicio en cada sentido.) Al final de la segunda fase los recursos quedan disponibles para el MTA y se inicia el registro de utilización para poder facturar al usuario por dicha utilización. (En los enlaces DOCSIS los flujos de servicio están activos.)

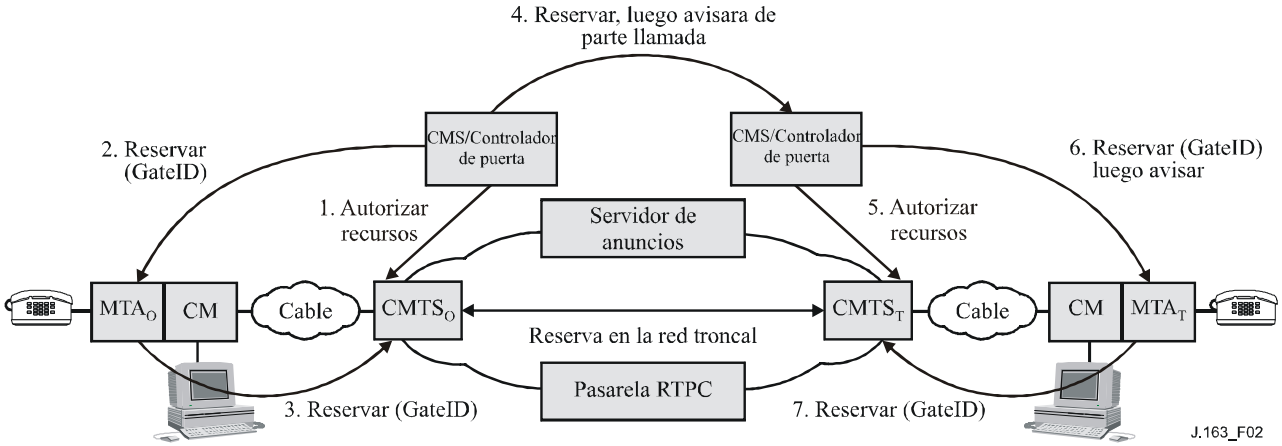



**Figura 2/J.163 – Fase 1 de la gestión de recursos**

La figura 2 muestra la primera fase del protocolo de gestión de recursos para una llamada . En esta descripción, los subíndices "O" y "T" designan los puntos de origen y terminación de la llamada. Como se muestra en la figura 2, $MTA_O$ y $MTA_T$ hacen una petición de reserva de recursos (señalización dinámica de servicios DOCSIS para clientes integrados) a $CMTS_O$ y $CMTS_T$ respectivamente. $CMTS_O$ y $CMTS_T$ realizan un control de admisión para determinar si hay recursos disponibles (inician la señalización de reserva de recursos en la red troncal si es necesario) y envían una respuesta a los MTA respectivos que, a su vez, responden al CMS.

La figura 3 muestra la segunda fase. Después de determinar que los recursos están disponibles, el CMS envía a $MTA_T$ un mensaje para activar la señal de llamada del teléfono. Cuando la parte llamada descuelga el teléfono, $MTA_T$ envía un mensaje al CMS y éste encarga al $MTA_O$ y $MTA_T$ que soliciten un compromiso de recursos. La recepción de mensajes Commit en $CMTS_T$ y $CMTS_O$ hace que éstos abran sus puertas y que se comience a contabilizar la utilización de recursos. Para evitar que se produzcan situaciones de robo de servicio, cada CMTS informa del cambio de estado al CMS respectivo enviando el mensaje GATE-OPEN (apertura de puerta).

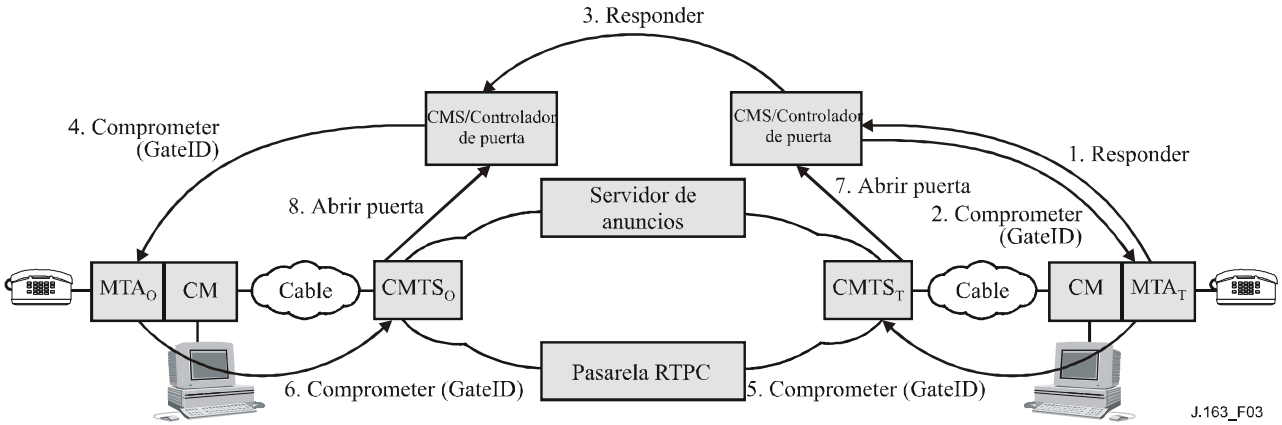



**Figura 3/J.163 – Fase 2 de la gestión de recursos**

### 5.7.2 Coordinación de puertas

La señalización de QoS da lugar a la creación de una puerta en cada CMTS asociado con un cliente que participa en la sesión. Cada puerta mantiene datos de utilización para la sesión y controla si los paquetes generados por el cliente asociado son tratados con la QoS mejorada. Es necesario coordinar las puertas para prevenir situaciones de fraude y robo de servicio que podrían darse si un cliente que funciona mal o ha sido modificado no emite los mensajes de señalización esperados. Hay que implementar mecanismos de protocolo con suficientes garantías[2]. Un protocolo de coordinación de puertas garantiza que:

- Se evita el establecimiento de una sesión unidireccional sin que ésta sea facturada. Los clientes que tengan la habilidad necesaria y abusen de la confianza podrían establecer dos sesiones unidireccionales para proporcionar a los usuarios un canal de comunicación vocal interactivo. La coordinación de puertas evita que se establezcan dichas sesiones sin que el proveedor las facture.
- La apertura y el cierre de las puertas está muy sincronizado y se producen los cambios de estado correspondientes en el CMS.

### 5.7.3 Cambio de los clasificadores de paquetes asociados a una puerta

Una vez que se han establecido dos puertas, los clientes pueden comunicar a través de la red con una QoS mejorada. En algunos servicios comerciales de comunicación vocal es necesario modificar los clientes que participan en una sesión, por ejemplo cuando se transfiere o redirecciona una sesión, o durante una conferencia a tres. Entonces habrá que modificar los clasificadores de paquetes asociados con una puerta, para reflejar la dirección del nuevo cliente. Además, el cambio de los puntos extremos de una sesión puede influir en la forma de facturación de la sesión. Como consecuencia de ello, las puertas incluyen información de direccionamiento para los puntos de origen y destino.

---

2 En el apéndice IX se describen distintas situaciones de robo de servicio.

### 5.7.4 Recursos de la sesión

En la figura 4 se muestra la relación que existe entre las distintas categorías de recursos, que pueden ser autorizados, reservados y comprometidos. Un conjunto de recursos se representa mediante un espacio *n*-dimensional (aquí se muestra de dos dimensiones) donde *n* es el número de parámetros (por ejemplo, anchura de banda, tamaño de la ráfaga, fluctuación, clasificadores) necesarios para describir los recursos. Los procedimientos detallados para comparar vectores de recursos *n*-dimensionales se describen en la Rec. UIT-T J.112.

Cuando se establece por vez primera una sesión, los protocolos de QoS dinámica autorizan la utilización de una cantidad máxima de recursos (el óvalo más externo) que corresponde a los recursos autorizados. Cuando un cliente reserva para una sesión, reservará una determinada cantidad de recursos que no es superior a la cantidad autorizada. Cuando la sesión está lista para proceder, el cliente compromete una determinada cantidad de recursos que no es superior a los recursos reservados. En muchos casos coinciden las cantidades de recursos comprometidos y reservados. Los recursos comprometidos están siendo utilizados actualmente por la sesión activa, y los recursos reservados han sido puestos a disposición del cliente y se han retirado de la disponibilidad a efectos de control de admisión, pero no están siendo utilizados por el cliente necesariamente.

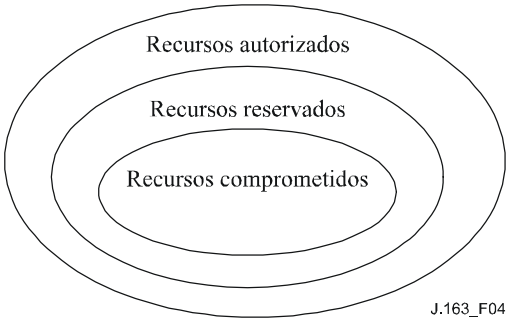



**Figura 4/J.163 – Recursos autorizados, reservados y comprometidos**

Las autorizaciones sólo valen para las peticiones de reserva de recursos ulteriores. Los recursos que se hayan reservado con anterioridad a un cambio de autorización no se ven afectados.

Los recursos que han sido reservados pero no comprometidos están disponibles en el sistema sólo para ser utilizados a corto plazo, por ejemplo para procesar datos con servicio de mejor esfuerzo. Estos recursos no están disponibles para otras reservas (es decir, no se permite hacer sobrerreservas). El número máximo de recursos que pueden ser reservados de una vez constituye una decisión de política por parte del CMTS y queda fuera del alcance de la QoS dinámica.

Se libera el exceso de recursos reservados con respecto a los comprometidos, excepto si el cliente solicita explícitamente que se mantengan, renovando periódicamente las operaciones. No es conveniente mantener esta situación durante mucho tiempo porque reduce la capacidad global del sistema. Sin embargo, existen situaciones que requieren una reserva en exceso (por ejemplo, el servicio de llamada en espera, en los que la llamada retenida requiere recursos adicionales a los de la llamada activa).

### 5.7.5 Control de admisión y clases de sesiones

Está previsto que la puerta de un CMTS pueda utilizar una o más clases de sesión para recursos reservados desde un MTA. Las clases de sesión definen las políticas de control de admisión configuradas o sus parámetros. Es previsible que el proveedor configurará los parámetros necesarios y/o las políticas de control de admisión alternativas en el CMTS y en el controlador de puerta. Por ejemplo, se podría definir una clase de sesión para comunicaciones de voz normales y

otra clase de sesión prioritaria para llamadas de emergencia a fin de permitir la atribución de hasta el 50% y el 70% de los recursos totales a estas clases de llamada, respectivamente, dejando el restante 30-50% de la anchura de banda disponible para otros servicios, probablemente de menor prioridad. Además, las clases de sesión pueden permitir la toma prioritaria de recursos que ya han sido reservados, en cuyo caso es el proveedor de servicio quien define las políticas de toma prioritaria. Cuando el controlador de puerta comunica la capacidad máxima autorizada a la puerta en el CMTS, mediante el mensaje establecimiento de puerta, incluye la información adecuada para indicar la clase de sesión aplicable cuando se procese la correspondiente petición de DSA/DSC.

### 5.7.6 Renegociación de los recursos

Algunas de las características soportadas requieren la renegociación de los parámetros de QoS asociados a la sesión durante la duración de la misma. Por ejemplo, los clientes pueden comenzar la comunicación utilizando un códec de audio de baja velocidad. Posteriormente, pueden conmutar a un códec de velocidad binaria superior o añadir un tren de vídeo en la medida en que la QoS requerida esté dentro de la capacidad máxima autorizada y exista anchura de banda disponible en la red. La utilización de una capacidad máxima de QoS que ha sido previamente autorizada por el controlador de puerta, que actúa como punto de decisión de políticas, ofrece a los clientes la flexibilidad necesaria para renegociar la QoS con la red sin que sea necesaria la participación ulterior del controlador de puerta. Dicho de otra forma, se autoriza pero NO se reserva previamente la utilización de recursos hasta la capacidad máxima. No se garantiza que se pueda asignar efectivamente recursos hasta la capacidad máxima autorizada, y es necesaria una decisión del control de admisión. Una vez realizado el control de admisión, los recursos quedan reservados para el flujo, aunque la utilización real de los recursos sólo se permite una vez que se completa la fase de compromiso del protocolo de reserva de recursos (RSVP). Sin embargo, no es necesaria ninguna decisión de control de admisión en el momento de comprometer los recursos. No serán necesarias otras reservas para modificar el compromiso de recursos dentro de los límites de la decisión de control de admisión. Todas las peticiones de reserva admitidas en el control de admisión TIENEN QUE estar dentro de la capacidad máxima autorizada.

### 5.7.7 Vinculación dinámica de recursos (segunda reserva)

La arquitectura de QoS dinámica reconoce que puede ser necesario compartir recursos entre varias sesiones, especialmente cuando los recursos son escasos. En concreto, cuando se utilice la llamada en espera en una aplicación de tipo telefónico, el cliente puede encontrarse en dos sesiones, pero en cada instante sólo estará activo en una conversación. En este caso es posible compartir los recursos de la capa de red (en particular, en el enlace de acceso) entre las dos conversaciones. Por lo tanto, esta arquitectura permite identificar explícitamente un conjunto de recursos de la capa de red (tal como la reserva de anchura de banda) y asociar una o más puertas con dichos recursos. Las primitivas de señalización permiten que los recursos asociados con una puerta puedan *compartirse* con otra puerta del mismo CMTS para mejorar la eficiencia de utilización de recursos en la red DOCSIS.

Cuando se conmuta alternativamente entre dos sesiones en una situación de llamada en espera, un cliente debe mantener suficientes recursos reservados para las dos sesiones que, en general, no necesitarán la misma cantidad de recursos. La operación de segundo compromiso puede modificar los recursos comprometidos, pero los recursos reservados son los mismos porque el cliente no debe pasar por un nuevo control de admisión cuando conmuta de una sesión a otra.

Si bien los recursos comprometidos siempre están asociados con la sesión activa en curso (y con su correspondiente flujo IP), los recursos reservados pueden estar vinculados a distintos flujos y puertas en un momento diferente. Se utiliza un alias (identificador de recursos) para identificar un conjunto de recursos reservados y vincular a ellos un flujo.

### 5.7.8 Soporte de la facturación

La señalización de QoS puede utilizarse para soportar una amplia gama de modelos de facturación, basándose exclusivamente en un tren de registro de eventos procedente del CMTS. Como la puerta se encuentra en el trayecto de los datos y participa en las interacciones de la gestión de recursos con un cliente, es el elemento que contabiliza los recursos utilizados. La puerta en el CMTS es el lugar adecuado para contabilizar los recursos, ya que el CMTS está directamente implicado en la gestión de los recursos proporcionados a un cliente. También es importante contabilizar los recursos utilizados en el CMTS a fin de tener en cuenta los posibles fallos del cliente. El CMTS TIENE QUE detectar la interrupción de un cliente que participa en una sesión, y detener la contabilización de la sesión. Hay distintas soluciones: supervisar el flujo de paquetes en el trayecto de datos para aplicaciones de medios continuos o mediante cualquier otro mecanismo del CMTS (por ejemplo mantenimiento de estación). Además, como la puerta mantiene un estado para flujos que han sido autorizados por un controlador de puerta específico del servicio, se utiliza para mantener información de tasación específica del servicio, por ejemplo el número de cuenta del abonado que pagará la sesión. Así, la función de políticas en el controlador de puerta se realiza sin contexto (stateless).

El CMTS debe generar y transmitir un mensaje de evento a un servidor de mantenimiento de registros cada vez que se modifica la QoS como ha sido autorizado y especificado por una puerta. También pueden incluirse en el mensaje datos opacos proporcionados por el controlador de puerta y que pueden ser relevantes para el servidor de mantenimiento de registros. Los requisitos para el tratamiento de registros de eventos están incluidos en otras especificaciones del sistemas de soporte de operaciones.

### 5.7.9 Gestión de los recursos de la red troncal

Cuando un CMTS recibe un mensaje de reserva de recursos de un MTA, verifica en primer lugar si hay anchura de banda ascendente y descendente disponible en el canal de acceso, utilizando información de planificación disponible a nivel local. Si la conclusión es positiva, el CMTS puede generar un nuevo mensaje de reserva de recursos de la red troncal, o enviar a la red troncal una versión modificada del mensaje de reserva de recursos recibido del MTA. El CMTS reflejará la reserva de recursos en la tecnología específica de la red troncal si es necesario. Así, la arquitectura se adapta a diferentes tecnologías de red troncal, a elección del proveedor de servicio. Los mecanismos específicos para la reserva de QoS en la red troncal quedan fuera del alcance de esta Recomendación.

En la red DOCSIS (encaminamiento simétrico) se utiliza un modelo bidireccional para la reserva de recursos. En la red troncal se utiliza un modelo unidireccional para la reserva de recursos, que permite asimetrías en el encaminamiento. Por lo tanto, cuando el $MTA_O$ realiza una reserva al CMTS, conoce dos cosas: que dispone de la anchura de banda adecuada en ambos sentidos sobre la red DOCSIS, y que dispone de la anchura de banda adecuada en las redes troncales para el flujo entre el $MTA_O$ y el $MTA_T$. Al recibir la respuesta del $MTA_T$, el $MTA_O$ sabe que hay recursos disponibles extremo a extremo en ambos sentidos.

### 5.7.10 Asignación del valor del punto de código DiffServ

Esta arquitectura también permite la utilización de una red troncal con servicios diferenciados (DiffServ) con anchura de banda suficiente para el transporte de conversaciones vocales, pero de acceso controlado. Se dará acceso a la anchura de banda y se aplicará un tratamiento diferenciado a los paquetes que tengan la codificación de bits adecuada en el campo del encabezamiento IP especificado para el servicio diferenciado (DiffServ). Dicho campo se denomina punto de código DiffServ (DSCP, *DiffServ code point*). El nuevo campo DS es compatible con el actual sistema de bits de precedencia IP del byte tipo de servicio TOS IPv4 (IETF RFC 2474). Es conveniente que se pueda validar el punto de código DiffServ de los paquetes que van a entrar a la red troncal del proveedor desde el CMTS. Dado que los recursos de red troncal consumidos por dichos paquetes

dependen en gran medida de esta marca, esta arquitectura permite el control de dicha marcación en las entidades de red. Así, la red y el proveedor de servicio podrán controlar la utilización de QoS mejorada, sin delegar este control en el MTA. El proveedor puede establecer políticas en el CMTS que determinen como se debe fijar el DSCP en los flujos que pasan por el CMTS. El CMS/GC comunica estas políticas al CMTS en el protocolo de establecimiento de puerta.

Para conseguir una implementación eficiente, se transfiere al MTA información acerca del DSCP apropiado para una sesión determinada. De todas formas, el CMTS debe vigilar los paquetes recibidos a fin de garantizar que se ha utilizado el DSCP correcto y que el volumen de paquetes de una clase determinada está dentro de los límites autorizados.

## 5.8 Reflejar descripciones SDP en especificaciones de flujo RSVP

Las sesiones multimedia se presentan mediante mensajes del protocolo de descripción de sesión (SDP, *session descriptor protocol*): aviso de sesión, invitación a sesión y otras formas de iniciación de sesión multimedia conforme a IETF RFC 2327. En esta cláusula se precisa un mecanismo para reflejar la descripción del SDP en especificaciones de flujo RSVP.

La descripción SDP contiene habitualmente muchos campos con información descriptiva de la sesión (versión del protocolo, nombre de la sesión, líneas de atributos de la sesión, etc.), precisiones de tiempo (cuánto tiempo está activa la sesión, etc.) y descripción de medios (nombre y transporte de medios, título de los medios, información de conexión, líneas de atributos de los medios, etc.). Los dos componentes críticos para reflejar una descripción SDP en un mensaje de especificaciones de flujo RSVP son el nombre de los medios y la dirección de transporte (m) y las líneas de atributos de los medios (a).

Estructura del nombre de los medios y la dirección de transporte (m):

m = <medios> <puerto> <transporte> <fmt list>

Estructura de las líneas de atributos de los medios (a):

a = <token>:<valor>

Características de una comunicación vocal IP típica:

m = audio 3456 RTP/AVP 0

a = ptime: 10

En la línea de dirección de transporte (m), el primer término define el tipo de medios, (audio en el caso de una sesión vocal IP), y el segundo término define el puerto UDP al que se envían los medios (puerto 3456). El tercer término indica que se trata de un tren de tipo Audio/Vídeo con protocolo en tiempo real (RTP). El último término es el tipo de cabida útil de los medios, conforme al perfil RTP Audio/Vídeo (IETF RFC 3551). En este caso, "0" indica una cabida útil de tipo estático de audio ley-u con modulación por impulsos codificados (MIC) en un solo canal, muestreado a 8 kHz. En la línea de atributos de los medios (a), el primer término indica el tiempo de formación de paquetes (10 ms).

Los tipos de cabida útil distintos a los definidos en IETF RFC 3551 están vinculados dinámicamente utilizando un tipo de cabida útil dinámica comprendida en la gama 96-127 y definida en IETF RFC 2327, y una línea de atributos de medios. Por ejemplo, un mensaje típico SDP para G.726 se compondría de lo siguiente:

m = audio 3456 RTP/AVP 96

a = rtpmap:96 G726-32/8000

El tipo 96 indica que la cabida útil se define localmente para la duración de la sesión, y la línea siguiente indica que el tipo de cabida útil 96 está vinculado a la codificación "G726-32" con un reloj a 8000 muestras/s. Para cada uno de los CÓDEC definidos (representados en SDP como un tipo de cabida útil estática o dinámica) debe haber un cuadro que establezca una correspondencia

entre el tipo de cabida útil o la representación de la cadena ASCII y los requisitos de anchura de banda para dicho CÓDEC.

En el caso de códecs menos conocidos, no es posible determinar los requisitos de anchura de banda únicamente a partir del nombre de los medios y la dirección de transporte (m) y las líneas de atributos de los medios

a) en estos casos, el SDP TIENE QUE utilizar la línea parámetro de anchura de banda;

b) para especificar estos requisitos del códec desconocido. Estructura de la línea parámetro de anchura de banda (b):

b = <modifier>: <bandwidth-value>

Por ejemplo:

b = AS:99

Es OBLIGATORIO utilizar este parámetro de anchura de banda y los atributos de los medios al reflejar el SDP en las especificaciones de flujo que serán utilizadas en la decisión de autorización (políticas) y la consiguiente asignación de puerta.

NOTA – Aceptar o rechazar la anchura de banda solicitada en el SDP es una decisión de políticas del CMS/CMTS.

El parámetro anchura de banda (b) incluirá la tara de anchura de banda necesaria para los encabezamientos IP/UDP/RTP. De otra parte, en la petición de anchura de banda no se tendrá en cuenta una posible supresión de encabezamiento de cabida útil (PHS) del enlace DOCSIS. Si se especificaron varios códecs en el SDP, el parámetro anchura de banda debería contener el valor máximo de anchura de banda de estos códecs.

El cuadro 2/J.161 es la correspondencia entre el código RTP/AVP y las especificaciones de flujo RSVP.

## 6 Protocolo de calidad de servicio (QoS) entre el MTA integrado y el CM (pkt-q1)

El CMTS DEBE soportar la interfaz MAC DOCSIS que se describe en esta cláusula. El MTA integrado TIENE QUE utilizar los mecanismos definidos en esta cláusula para reservar dinámicamente recursos de QoS locales.

Al utilizar este enfoque, el MTA integrado señaliza directamente la QoS de acceso local utilizando la interfaz de servicio de control definida en la Recomendación DOCSIS RFI (Recs. UIT-T J.112 y J.122). El MTA integrado señaliza sus necesidades de QoS a nivel de sesión en protocolos de señalización (DCS y NCS). Una vez que el MTA integrado determina qué recursos de QoS hay que reservar o comprometer, el MTA DEBE iniciar la señalización de flujo de servicio dinámico DOCSIS para crear, modificar y/o suprimir flujos de servicio y la asignación de recursos DOCSIS. El MTA transfiere los requisitos de QoS al DOCSIS MAC por medio de la interfaz de servicio de control de MAC con independecia de si la sesión es creada por el MTA integrado, un nodo de red o una entidad par. Como resultado se crean o modifican los flujos de servicio necesarios para la sesión utilizando los mecanismos de mensajería de flujos de servicio dinámicos de DOCSIS. A continuación se describe la correspondencia de los requisitos de QoS a nivel de servicio del MTA con DOCSIS, el soporte de DOCSIS para reservar/comprometer en dos fases y la utilización de la interfaz de servicio de control DOCSIS MAC.

### 6.1 Especificaciones de flujo de RSVP

La arquitectura de servicios integrados del IETF utiliza descripciones generales (independientes de la capa 2) de las características del tráfico y los requisitos de recursos de un flujo. La descripción del tráfico es TSpec, los requisitos de recursos se incluyen en una RSpec y la combinación de ambos se denomina especificación de flujo (FlowSpec). Para reservar recursos en un medio de

capa 2 específico, como una red DOCSIS, es necesario definir una correspondencia entre la especificación de flujo independiente de la capa 2 y los parámetros específicos de la capa 2. Se han definido las correspondencias aplicables a diversas tecnologías (ATM, LAN 802.3, etc.).

En otras especificaciones (por ejemplo, en la especificación del CÓDEC IPCablecom Rec. UIT-T J.167) figuran los requisitos de la correspondencia que debe establecerse entre descripciones de servicios de capas superiores (por ejemplo, SDP utilizado en aplicaciones de VoIP) y las especificaciones de flujo. En esta cláusula se especifica la correspondencia OBLIGATORIA entre especificaciones de flujo y parámetros de capa 2 en el CMTS y el MTA.

La modalidad de servicios integrados (IntServ) define actualmente dos tipos de servicios, de carga controlada y garantizados, siendo este último el más adecuado para aplicaciones sensibles al retardo. La especificación de flujo de una reserva para servicios garantizados contiene lo siguiente:

TSpec (especificación de tráfico)

dimensión del contador (b) – bytes
tasa o velocidad del contador (r) – bytes/segundo
tasa de cresta (p) – bytes/segundo
mínima unidad supervisada (m) – bytes
tamaño máximo del datagrama (M) – bytes

RSpec (especificación de recursos)

tasa reservada (R) – bytes/segundo
término de inactividad (S) – microsegundos

El significado de los términos de las TSpec es bastante claro. La dupla (r,b) especifica la dimensión del contador válido para el tráfico, p es la tasa o velocidad de cresta a la que transmite la fuente, y M es el tamaño máximo del paquete (incluyendo los encabezamientos IP y de capa superior) que genera la fuente. La mínima unidad supervisada, m, es normalmente el menor tamaño de paquete que genera la fuente; un paquete más pequeño será considerado como un paquete de tamaño m a los efectos de aplicación de las políticas.

A fin de entender cabalmente la RSpec, conviene saber cómo se calcula el retardo en un entorno de servicios integrados. El máximo retardo extremo a extremo que experimenta un paquete que recibe un servicio garantizado es:

$$\text{Retardo} = b/R + C_{tot}/R + D_{tot}$$

siendo b y R los parámetros anteriormente definidos, y $C_{tot}$ y $D_{tot}$ "términos de error" acumulativos que proporcionan los elementos de red a lo largo del trayecto y que describen sus desviaciones respecto al comportamiento "ideal".

La velocidad R de RSpec es la anchura de banda atribuida al flujo. TIENE QUE ser igual al valor r de TSpec o mayor para mantener el límite anterior del retardo. Por lo tanto, el límite del retardo de un flujo queda completamente determinado por la elección de R; la razón de utilizar un valor de R mayor que r sería reducir el retardo que experimenta el flujo.

Sabiendo que R no puede ser inferior a r, este cálculo permite determinar si el límite de retardo es demasiado estricto, al hacer una reserva en un nodo. En tal caso, el nodo puede hacer R = r y dar a S un valor distinto de cero. El valor de S se elige de tal forma que:

$$\text{Límite deseado del retardo} = S + b/R + C_{tot}/R + D_{tot}$$

El servicio garantizado no pretende limitar la fluctuación más allá del valor determinado por el límite de retardo. En general, el retardo mínimo de un paquete viene dado por la velocidad de la luz, y el máximo es el límite antes identificado; la fluctuación máxima es la diferencia entre ambos. Por lo tanto, la fluctuación puede controlarse mediante una selección adecuada de R y S.

### 6.1.1 Descripciones del SDP complejas con múltiples códecs

Existen diversas situaciones en las que una reserva debe incluir distintas especificaciones de flujo posibles. Por ejemplo, para algunas aplicaciones conviene establecer una reserva que pueda realizar la transferencia de un códec a otro durante una sesión sin tener que someterse al control de admisión en cada conmutación.

ES OBLIGATORIO incluir en la TSpec del emisor el mínimo valor superior (LUB, *least-upper-bound*) de los parámetros de flujo necesarios para el componente.

No está autorizado el valor superior mínimo (LUB) de los flujos con dos tipos distintos de planificación DOCSIS.

El mínimo valor superior (LUB) de dos flujos A y B, LUB(A, B), es la "menor" capacidad máxima que permite transportar ambos flujos A, B de forma no simultánea. LUB(A, B) se calcula para cada parámetro separadamente de esta forma:

Definir los valores de TSpec indicados en la cláusula 6 para un flujo α. Definir también el periodo Pα como Mα/rα. La expresión de LUB(A, B) está basada en estos valores:

LUB(A, B) ≡ { bLUB(A, B) ≡ MAX(bA, bB),
r LUB(A, B) ≡ (M LUB(A, B)/P LUB(A, B)),
p LUB(A, B) ≡ MAX(pA, pB, r LUB(A, B)),
m LUB(A, B) ≡ MAX(mA, mB),
M LUB(A, B) ≡ MAX(MA, MB)
}

siendo:

p LUB(A, B) ≡ GCF(PA, PB);

la función MAX(x, y) significa "el mayor de la dupla (x, y)";

la función MAX(x, y, z) ≡ MAX(MAX(x, y), z);

la función GCF(x, y) significa "el mayor denominador común de la dupla (x, y)".

El valor LUB de n flujos (n ≠ 2), LUB(n1, n2, ...) se determina así por un proceso recursivo:

$$LUB(n1, n2, ..., N) \equiv LUB(n1, LUB(n2, ..., N))$$

Además, en las RSpec correspondientes se tiene que utilizar un término de inactividad apropiado para que todos los flujos componentes puedan utilizar los recursos. Esta condición se satisface adoptando el mínimo de los valores de RSpec de los flujos componentes, es decir:

$$SLUB(A, B) \equiv MIN(SA, SB)$$

donde la función MIN(x, y) significa "el menor de la dupla (x, y)".

El siguiente ejemplo ilustra la determinación de los parámetros de TSpec con el algoritmo de LUB aquí especificado:

1) Se han seleccionado los siguientes códecs para una llamada en el proceso de negociación:
   G711(20ms) y G728(10ms)
2) La capacidad del contador LUB para los códecs seleccionados es:
   G711(20ms) = (8000/50) + 40 = 200 bytes
   G728(10ms) = (2000/100) + 40 = 60 bytes
   b[LUB] = m[LUB] = M[LUB] = MAX(200, 60) = 200 bytes
3) La tasa o velocidad del contador LUB para los códecs seleccionados es:
   P [LUB] = GCF(10ms, 20ms) = 10ms = 0,01 segundo

r[LUB] = M × 1/P = 200 × 1/0,01 = 20,000 bytes por segundo

r[G711(20ms)] = 200 × 1/0,02 = 10,000 bytes por segundo

r[G728(10ms)] = 60 × 1/0,01 = 6,000 bytes por segundo

p[LUB] = MAX(10000, 6000, 20000) = 20,000 bytes por segundo

### 6.1.2 Correspondencia de especificaciones de flujo RSVP con parámetros de QoS DOCSIS

Al recibir una petición de reserva, el CMTS debe utilizar los siguientes algoritmos cuando traduzca las especificaciones de flujo RSVP en parámetros QoS DOCSIS.

El MTA DEBE utilizar los requisitos definidos en la siguiente cláusula para traducir los requisitos de QoS de nivel de sesión a los parámetros QoS DOCSIS.

Como complemento a estos requisitos, los MTA integrados TIENEN QUE incluir sus propias direcciones y puertos de emisión (es decir, el origen en sentido ascendente) y recepción (es decir, el destino en sentido descendente) en todos los TLV clasificadores proporcionados por la mesajería DSx. Las direcciones de extremo distante y puertos de recepción PUEDEN dejarse en blanco si el SDP del extremo distante no ha se do configurado y los valores no han sido asignados a través del LCO. Si esos valores se proporcionan en uno de los dos formatos, DEBEN incluirse en los TLV clasificadores. Los puertos de origen del extremo distante TIENEN QUE dejarse en blanco en todos los casos dado que estos parámetros no se comunican a través del SDP.

Cabe observar que en los ejemplos nostrados en esta cláusula se incluyen la tara relacionada con el encabezamiento ampliado BPI+ DOCSIS, de conformidad con lo dispuesto en la Recomendación sobre seguridad (Rec. UIT-T J.170). Si BPI+ está inhabilidato (por ejemplo, a efectos de prueba) los valores facilitados en estos ejemplos deben ser actualizados consecuentemente restando cinco bytes de la tara de la capa de enlace del cálculo del tamaño de autorización en sentido ascendente.

#### 6.1.2.1 Codificación de calidad de servicio en sentido ascendente

Se han indicado los valores de objetos DOCSIS en sentido ascendente. NO SE DEFINIRÁ ninguno de los otros códigos TLV de calidad de servicio del flujo, y se utilizarán los valores por defecto. Si el MTA proporciona uno de estos TLV, el CMTS RECHAZARÁ la petición con un código de error "rechazo definitivo/rechazo admin".

El valor del temporizador *DOCSIS Temporización de actividad* se utiliza para detectar inactividad e iniciar la recuperación de recursos para flujos de servicio comprometidos. El CMTS puede coordinar la sincronización MTA/CMTS proporcionando un valor apropiado en el mensaje DSA/DSC REQ/RSP. El MTA NO PODRÁ definir este campo.

El valor del temporizador *DOCSIS Temporización de admisión* se utiliza para detectar inactividad e iniciar la recuperación de recursos para flujos de servicio reservados. El CMTS puede coordinar la sincronización MTA/CMTS proporcionando un valor apropiado en el mensaje DSA/DSC REQ/RSP. El MTA NO PODRÁ definir este campo.

El parámetro *DOCSIS Tamaño mínimo previsto de paquetes a la velocidad reservada* NO SE DEFINIRÁ para flujos ascendentes.

Si un dispositivo decide invocar múltiples autorizaciones por intervalo, el parámetro *DOCSIS Autorizaciones por intervalo* TIENE QUE ser un número entero mayor o igual que 1. Si el dispositivo no lo admite, o decide no utilizar múltiples autorizaciones por intervalo, el parámetro autorizaciones por intervalo DOCSIS TIENE QUE ponerse a 1.

El parámetro *DOCSIS Intervalo de autorización nominal* TIENE QUE ser el intervalo de paquetización del códec.

Intervalo de autorización nominal DOCSIS = 10000 ó 20000 ó 30000

El parámetro *DOCSIS Fluctuación de autorización tolerada* TIENE QUE SER un valor especificado por el CMS basado en información de costo de encaminamiento. Puede ser un valor entre 0 y 2 × intervalo de paquetización. Si el CMS no lo especifica, se utilizará un valor por defecto de 800 microsegundos.

El parámetro *DOCSIS Intervalo de interrogación nominal* NO SE ESPECIFICARÁ para flujos de servicio UGS, y DEBERÍA adoptarse un valor que sea un entero múltiplo del intervalo de paquetización del códec para los flujos de servicio UGS/AD.

El parámetro *DOCSIS Fluctuación de interrogación tolerada* NO SE ESPECIFICARÁ para flujos de servicio UGS, y DEBERÍA adoptarse un valor que sea un entero múltiplo del intervalo de paquetización del códec para los flujos de servicio UGS/AD.

El parámetro *DOCSIS Política de petición/transmisión* es una máscara de bits; ES OBLIGATORIO poner a 1 los bits 0-6 y 8 para flujos de servicio UGS y UGS/AD.

El parámetro *DOCSIS Reemplazar tipo de servicio* NO SE UTILIZARÁ. El parámetro ha sido definido en DOCSIS, pero PacketCable prohíbe su utilización.

El parámetro *DOCSIS Tamaño de autorización sin petición* SE TIENE QUE calcular desde el control de trama (FC) del encabezamiento MAC de DOCSIS hasta el final de la verificación de redundancia cíclica (CRC). Este valor incluye una tara de 18 bytes de encabezamiento Ethernet (6 bytes para dirección de fuente, 6 bytes para dirección de destino, 2 bytes para longitud y 4 bytes para CRC). También incluye la tara de encabezamiento MAC DOCSIS, que se compone del encabezamiento básico DOCSIS (6 bytes), el encabezamiento ampliado UGS (3 bytes) y encabezamiento ampliado BPI+ (5 bytes). Si se ha activado la supresión de encabezamiento de cabida útil (PHS), NO SE INCLUIRÁ el número de bytes suprimidos. El encabezamiento ampliado suprimido PHS (2 bytes) NO SE INCLUIRÁ para flujos de servicio UGS o UGS/AD porque la información pertinente aparece en el encabezamiento ampliado UGS.

Tamaño de autorización sin petición DOCSIS^8,9 = M + 32-PHS[3,4]

El parámetro *DOCSIS Tipo de planificación en sentido ascendente* TIENE QUE ser UGS o UGS/AD, se soporta o no la supresión de silencio en la llamada.

Si hace una reserva o un compromiso para un códec que no detecta actividad vocal, el MTA TIENE QUE utilizar el tipo de planificación UGS; en otros casos TIENE QUE utilizar UGS/AD.

Si hace una reserva para un flujo de servicio con múltiples códecs, y uno de ellos detecta actividad vocal, el MTA TIENE QUE hacer la petición de reserva para UGS/AD y comprometer sólo para las propiedades del códec activo según la descripción anterior.

#### 6.1.2.2 Codificación de clasificación de paquetes en sentido ascendente

**Peticiones DOCSIS de clasificación de paquetes en sentido ascendente**

Se han indicado los valores de objetos DOCSIS en sentido ascendente. NO SE DEFINIRÁ ninguno de los otros códigos TLV de clasificación y se utilizarán los valores por defecto. Si el MTA proporciona uno de estos TLV, el CMTS RECHAZARÁ la petición con un código de error "rechazo definitivo/rechazo admin".

ES OBLIGATORIO utilizar el parámetro *DOCSIS Identificador de clasificador* si lo ha definido el CMTS. Si no está definido, ES OBLIGATORIO atribuir un valor único al parámetro *DOCSIS Referencia de clasificador* para los mensajes de servicio dinámico.

---

3 En este ejemplo se supone que se utiliza BPI+ conforme a la especificación de seguridad PacketCable.

4 La supresión de encabezamiento (PHS) de este ejemplo está definida en la especificación DOCSIS RFI, cláusula B.C.2.2.10.4/J.112.

ES OBLIGATORIO atribuir un valor único del E-MTA para llamadas existentes al parámetro *DOCSIS Referencia de flujo de servicio* en mensajes DSA_REQ, y este parámetro NO SE INCLUIRÁ en ningún otro mensaje, SIENDO OBLIGATORIO utilizar el parámetro DOCSIS Identificador de flujo de servicio emitido por el CMTS.

El valor del parámetro *DOCSIS Prioridad de reglas* TIENE QUE ser 128.

El parámetro *DOCSIS Estado activación de clasificación* TIENE QUE tener el valor de activo (1) cuando se compromete la llamada que utiliza el flujo de servicio; en otros casos, TIENE QUE tener el valor de inactivo (0).

La acción *DOCSIS Modificación de servicio dinámica* PUEDE utilizar las acciones Añadir clasificador (0), Reemplazar clasificador (1) y Suprimir clasificador (2) definidas en la especificación DOCSIS RFI.

Los campos *DOCSIS Tipo de servicio IP y máscara* SE PUEDEN omitir porque PacketCable no incorpora parámetros TOS en su clasificador. Ahora bien, si se incluye este parámetro, TIENE QUE corresponder al valor TOS especificado por el CMS o un valor configurado para flujos de servicio vocal.

El parámetro *DOCSIS Protocolo IP* TIENE QUE ser UDP (17).

El parámetro *DOCSIS Dirección de fuente IP* TIENE QUE ser la misma dirección de la plantilla de emisor, si se indica un valor distinto de cero. Si la dirección indicada en el objeto plantilla de emisor es cero, SE OMITIRÁ este parámetro.

El parámetro *DOCSIS Máscara de fuente IP* SE OMITIRÁ.

Los parámetros *DOCSIS Puerto fuente IP inicial* y *Puerto fuente IP final* TIENEN QUE tener el mismo valor de puerto de transporte de la plantilla de emisor.

El parámetro *DOCSIS Dirección de destino IP* TIENE QUE ser la misma dirección especificada en el objeto Sesión, si se indica un valor distinto de cero. Si la dirección indicada en el objeto Sesión es cero, SE OMITIRÁ este parámetro.

El parámetro *DOCSIS Máscara de destino IP* SE OMITIRÁ.

Los parámetros *DOCSIS Puerto de destino IP inicial* y *Puerto de destino IP final* TIENEN QUE tener el mismo valor de puerto de transporte del objeto Sesión si se indica un valor distinto de cero. Si el puerto de destino IP indicado en el objeto Sesión es cero, SE OMITIRÁN los TLV Puerto de destino IP inicial y final.

Los parámetros *DOCSIS Códigos de clasificación de paquetes Ethernet LLC* SE OMITIRÁN.

Los parámetros *DOCSIS Códigos de clasificación de paquetes 802.1P/Q* SE OMITIRÁN.

**Acciones del CMTS frente a peticiones DOCSIS de clasificación de paquetes en sentido ascendente**

Al recibir una petición Añadir clasificador (por ejemplo, mediante mensajes DOCSIS DSx) el CMTS TIENE QUE comparar los valores de puerta del GateID y los TLV. Si los TLV no coinciden, el CMTS TIENE QUE responder con el código de error de clasificador DOCSIS, con la siguiente información:

- El valor del parámetro *Código de error* TIENE QUE ser "rechazo-no autorizado".
- El parámetro que indica *Parámetro erróneo* TIENE QUE indicar el primer TLV no autorizado. Como distintas implementaciones PUEDEN autenticar los TLV en distinto orden, este campo PUEDE comunicar un TLV diferente en las mismas circunstancias.
- El parámetro *Mensaje de error* PUEDE definirse.

#### 6.1.2.3 Codificación para supresión de encabezamiento de cabida útil

**Peticiones DOCSIS para supresión de encabezamiento de cabida útil (PHS)**

La supresión de encabezamiento de cabida útil es facultativa. Cuando se utiliza es preciso observar las siguientes reglas, que se aplican a la PHS en los flujos ascendente y descendente.

El parámetro *DOCSIS Campo supresión de encabezamiento de cabida útil* indica los bytes de los encabezamientos que la entidad emisora TIENE QUE suprimir, y la entidad receptora TIENE QUE restablecer.

El parámetro *DOCSIS Tamaño supresión de encabezamiento de cabida útil* TIENE QUE ser igual al número total de bytes del campo supresión de encabezamiento de cabida útil (PHSF, *payload header suppresion field*).

El parámetro *DOCSIS Máscara supresión de encabezamiento de cabida útil* TIENE QUE indicar los bytes que se han de suprimir.

El parámetro *DOCSIS Verificación supresión de encabezamiento de cabida útil* se DEBERÍA poner a 0 (verificar).

El parámetro *DOCSIS Identificador de clasificador* SE TIENE QUE utilizar si lo ha definido el CMTS. Si no lo ha definido, SE TIENE QUE utilizar el parámetro DOCSIS *Referencia de clasificador* utilizado en la definición del clasificador.

El parámetro *DOCSIS Referencia de clasificador* SE TIENE QUE utilizar si el CMTS no ha definido el Identificador de clasificador DOCSIS. Si está definido, SE TIENE QUE utilizar el parámetro DOCSIS Identificador de clasificador utilizado en la definición del clasificador.

El parámetro *DOCSIS Identificador de flujo de servicio* SE TIENE QUE utilizar si lo ha definido el CMTS. Si no lo ha definido, SE TIENE QUE utilizar el parámetro DOCSIS Referencia de flujo de servicio utilizado en la definición del clasificador.

La acción *DOCSIS Modificación de servicio dinámica* PUEDE utilizar las operaciones Añadir regla de PHS (0), Definir regla de PHS (1) y Suprimir todas las reglas de PHS (2) definidas en la especificación DOCSIS RFI.

**Acciones del CMTS frente a peticiones DOCSIS de supresión de encabezamiento de cabida útil**

Este procedimiento de errores de PHS constituye un mecanismo muy completo de retorno de información entre el CMTS que rechaza una petición inicial de PHS y el MTA solicitante. El objetivo es que la información proporcionada en la respuesta de error facilite una alternativa satisfactoria (admisión del flujo UGS sin supresión o con una regla PHS más simple).

Al recibir una petición DSx con supresión de encabezamiento de cabida útil DOCSIS, si el CMTS decide que no puede soportar la supresión solicitada (posiblemente porque hay pocos recursos locales de tratamiento o memoria), pero sí puede soportar el servicio de autorización sin petición sin la supresión, TIENE QUE incluir en su respuesta el código de confirmación "rechazar supresión de encabezamiento" en los códigos DOCSIS de supresión de encabezamiento de cabida útil, así como el parámetro de error DOCSIS descrito más adelante. PODRÁ utilizarse el mensaje de error DOCSIS.

Si no puede soportar una petición de supresión de encabezamiento de cabida útil compleja DOCSIS, pero sí una más simple, el CMTS TIENE QUE incluir la máscara de supresión de encabezamiento de cabida útil DOCSIS en el campo DOCSIS Parámetro con errores.

Parámetro con errores DOCSIS = Máscara de supresión de encabezamiento de cabida útil DOCSIS

Si el CMTS no puede soportar el tamaño de la petición DOCSIS para supresión de encabezamiento de cabida útil, pero sí un tamaño inferior, TIENE QUE especificar el tamaño de supresión de encabezamiento de cabida en el campo DOCSIS Parámetro con errores.

Parámetro con errores DOCSIS = Tamaño de supresión de encabezamiento de cabida útil DOCSIS

**Acciones del E-MTA frente a peticiones DOCSIS de supresión de encabezamiento de cabida útil**

Al recibir un código de confirmación "rechazar supresión de encabezamiento" que tiene un parámetro con errores DOCSIS que incluye la máscara de supresión de encabezamiento de cabida útil DOCSIS, el E-MTA PUEDE hacer una nueva petición sin supresión de encabezamiento de cabida útil DOCSIS, o PUEDE redefinir la máscara de supresión de encabezamiento de cabida útil DOCSIS con una regla de supresión más simple (por ejemplo, indicar un bloque contiguo de bytes suprimidos).

Al recibir un código de confirmación "rechazar supresión de encabezamiento" que tiene un parámetro con errores DOCSIS que incluye el tamaño de supresión de encabezamiento de cabida útil DOCSIS, el E-MTA PUEDE hacer una nueva petición de anchura de banda sin supresión de encabezamiento de cabida útil DOCSIS.

**Cómo utiliza el E-MTA el encabezamiento ampliado DOCSIS UGS**

El parámetro DOCSIS Índice de supresión de encabezamiento de cabida útil TIENE QUE ser el índice predefinido de PHS, o cero cuando no se ha definido ninguna supresión de encabezamiento de cabida útil para el flujo de servicio.

El parámetro DOCSIS Indicador de cola TIENE QUE definirlo el E-MTA si hay más de un paquete en cola de transmisión. En otros casos, este valor DEBERÍA ser cero.

El campo Autorizaciones activas del encabezamiento MAC ampliado DOCSIS sólo TIENE QUE reflejar únicamente los subflujos (obsérvese que como mínimo habrá uno) que no están en modo supresión de silencio, y SE TIENE QUE poner a cero cuando el E-MTA está el modo en supresión de silencio para el códec que se utiliza para el tren de datos asociado con este flujo de servicio.

### 6.1.2.4 Codificación de calidad de servicio en sentido descendente

Los códigos DOCSIS TLV para la calidad del flujo de servicio TIENEN QUE ajustarse a las siguientes reglas. NO SE DEFINIRÁ ninguno de los otros códigos TLV, y se utilizarán los valores por defecto. Si el MTA proporciona uno de estos TLV, el CMTS RECHAZARÁ la petición con un código de error "rechazo definitivo/rechazo admin".

Los parámetros DOCSIS en sentido descendente se calculan desde el byte del encabezamiento MAC de DOCSIS situado después de HCS, hasta el final de la verificación de redundancia cíclica (CRC). La tara de la capa MAC (Ethernet) es de 18 bytes (6 bytes para dirección de fuente, 6 bytes para dirección de destino, 2 bytes para longitud y 4 bytes para CRC).

Basándose en esta tara se calcula el parámetro *DOCSIS Tamaño mínimo previsto de paquetes a la velocidad reservada* de esta forma:

Tamaño mínimo previsto de paquetes a la velocidad reservada DOCSIS = m + 18 – PHS

El parámetro *DOCSIS Velocidad de tráfico máxima sostenida*[5] se indica en bits por segundo, incluyendo la tara de capa MAC Ethernet (no DOCSIS). Para convertir parámetros específicos IP, primero hay que determinar la tasa de paquetización, dividiendo Velocidad máxima por Mínima unidad supervisada. Luego se multiplica el resultado por el tamaño de paquete ajustado para incluir

5 Los valores con cifras decimales se redondean.

la tara de capa MAC, y el resultado final se convierte de bytes a bits. El valor DOCSIS de máxima velocidad de tráfico sostenida SE TIENE QUE calcular así:

$$\text{Máxima velocidad de tráfico sostenida DOCSIS} = p / m \times (m + 18 - PHS) \times 8 \times z$$

siendo z el número de subflujos del flujo de servicio.

El parámetro DOCSIS *Velocidad de tráfico mínima reservada*[5] se calcula como la velocidad de tráfico máxima sostenida DOCSIS, pero no se utiliza el parámetro Velocidad máxima (p), sino el parámetro Velocidad reservada (R).

$$\text{Velocidad de tráfico mínima reservada DOCSIS} = R / m \times (m + 18 - PHS) \times 8 \times z$$

siendo z el número de autorizaciones por intervalo del flujo de servicio en sentido ascendente.

El parámetro *DOCSIS Ráfaga de tráfico máxima* TIENE QUE ser el mayor de estos valores:

1) un entero múltiplo del tamaño mínimo previsto del paquete a la velocidad reservada; o
2) el valor mínimo de 1522 especificado en DOCSIS.

$$\text{Ráfaga de tráfico máxima DOCSIS} = \max( (M + 18 - PHS) \times 3 \times z, 1522)$$

siendo z el número de autorizaciones por intervalo del flujo de servicio en sentido ascendente.

El parámetro *DOCSIS Prioridad de tráfico* TIENE QUE ser cinco.

NO SE UTILIZARÁ el parámetro *DOCSIS Tiempo de espera en sentido descendente*.

El valor del temporizador *DOCSIS Temporización de actividad* se utiliza para detectar inactividad e iniciar la recuperación de recursos para flujos de servicio comprometidos. Como los flujos de servicio y las puertas ascendente y descendente se gestionan con un solo identificador GateID y se suprimen por pares, en el modelo PacketCable no es necesario supervisar la actividad de los dos flujos (ascendente y descendente). Sólo se supervisa el flujo de servicio ascendente, utilizando el valor de Temporizador de actividad DOCSIS. El MTA y el CMTS NO ESPECIFICARÁN ningún valor en este campo para el flujo de servicio descendente.

El valor del temporizador *DOCSIS Temporización de admisión* se utiliza para detectar inactividad e iniciar la recuperación de recursos para flujos de servicio reservados. Por los motivos expuestos antes para Temporización de actividad DOCSIS, no se ha definido en el modelo IPCablecom una supervisión del flujo de servicio descendente mediante un parámetro DOCSIS Temporización de admisión. El MTA y el CMTS NO ESPECIFICARÁN ningún valor en este campo para el flujo de servicio descendente.

#### 6.1.2.5 Codificación de clasificación de paquetes en sentido descendente

**Peticiones DOCSIS de clasificación de paquetes en sentido descendente**

Los objetos de clasificación DOCSIS en sentido descendente TIENE QUE ajustarse a las siguientes reglas. NO SE DEFINIRÁ ninguno de los otros códigos TLV de clasificación y se utilizarán los valores por defecto. Si el MTA proporciona uno de estos TLV que se omiten obligatoriamente, el CMTS RECHAZARÁ la petición con un código de error "rechazo definitivo/rechazo admin".

ES OBLIGATORIO utilizar el parámetro *DOCSIS Identificador de clasificador* si lo ha definido el CMTS. Si no está definido, ES OBLIGATORIO atribuir un valor único al parámetro *DOCSIS Referencia de clasificador* para los mensajes de servicio dinámico.

ES OBLIGATORIO atribuir un valor único del E-MTA para el parámetro *DOCSIS Referencia de flujo de servicio* en mensajes DSA_REQ, y este parámetro NO SE INCLUIRÁ en ningún otro mensaje, SIENDO OBLIGATORIO utilizar el parámetro *DOCSIS Identificador de flujo de servicio* emitido por el CMTS.

El valor del parámetro *DOCSIS Prioridad de reglas* TIENE QUE ser 128.

El parámetro *DOCSIS Estado activación de clasificación* TIENE QUE tener el valor de activo (1) cuando se compromete la llamada que utiliza el flujo de servicio; en otros casos TIENE QUE tener el valor de inactivo (0).

La *acción DOCSIS Modificación de servicio dinámica* PUEDE utilizar las operaciones Añadir clasificador (0), Reemplazar clasificador (1) y Suprimir clasificador (2) definidas en la especificación DOCSIS RFI.

Los campos *DOCSIS Tipo de servicio y máscara IP* NO SE UTILIZARÁN.

El parámetro *DOCSIS Protocolo IP* TIENE QUE ser UDP (17).

El parámetro *DOCSIS Dirección de fuente IP* TIENE QUE ser la misma dirección de la plantilla de emisor hacia atrás, si se indica un valor distinto de cero. Si la dirección indicada en el objeto Plantilla de emisor hacia atrás es cero, SE OMITIRÁ este parámetro.

El parámetro *DOCSIS Máscara de fuente IP* SE OMITIRÁ.

Los parámetros *DOCSIS Puerto fuente IP inicial* y *Puerto fuente IP final* TIENEN QUE tener el mismo valor de puerto de transporte de la plantilla de emisor hacia atrás si se indica un valor distinto de cero. Si el puerto fuente IP de la plantilla de emisor hacia atrás es cero, SE OMITIRÁN los TLV DOCSIS de puerto fuente inicial y final.

El parámetro *DOCSIS Dirección de destino IP* TIENE QUE ser la misma dirección especificada en el objeto Sesión hacia atrás.

El parámetro *DOCSIS Máscara de destino IP* SE OMITIRÁ.

Los parámetros *DOCSIS Puerto de destino IP inicial* y *Puerto de destino IP final* TIENEN QUE tener el mismo valor de puerto indicado en el objeto Sesión hacia atrás.

Los códigos *DOCSIS Clasificación de paquetes Ethernet LLC* SE OMITIRÁN.

Los códigos *DOCSIS Clasificación de paquetes 802.1P/Q* SE OMITIRÁN.

**Acciones del CMTS frente a peticiones DOCSIS de clasificación de paquetes en sentido descendente**

Al recibir una petición Añadir clasificador (por ejemplo, mediante mensajes DOCSIS DSx) el CMTS TIENE QUE comparar los valores de puerta del GateID y los TLV. Si los TLV no coinciden, el CMTS TIENE QUE responder con el código de error de clasificador DOCSIS, con la siguiente información:

- El valor del parámetro *Código de error* TIENE QUE ser "rechazo-no autorizado".
- El parámetro que indica *Parámetro erróneo* TIENE QUE indicar el primer TLV no autorizado. Como distintas implementaciones PUEDEN autenticar los TLV en distinto orden, este campo PUEDE comunicar un TLV diferente en las mismas circunstancias.
- El parámetro *Mensaje de error* PUEDE definirse.

#### 6.1.2.6 Ejemplo de correspondencia

Considérese el ejemplo siguiente. Un códec de voz produce un tren de datos de salida CBR de 64 kbit/s que se paquetiza a intervalos de 10 ms, produciendo por tanto una cabida útil de 80 bytes cada 10 ms. La cabida útil se encapsula utilizando RTP/UDP/IP, lo que representa 40 bytes adicionales, y el total es un paquete de 120 bytes cada 10 ms. Entonces TSpec sería:

Capacidad del contador (b) = 120 bytes

Velocidad del contador (r) = 12 000 bytes/segundo

Velocidad máxima (p) = 12 000 bytes/ segundo

Mínima unidad supervisada (m) = 120 bytes

Tamaño máximo del datagrama (M) = 120 bytes

Supóngase que un cliente solicita una reserva utilizando estas TSpec y RSpec con R = r. Un CMTS que reciba esta petición establecerá un flujo de servicio con autorización sin petición, porque p = r y M = b indican que se trata de un flujo CBR. Puede utilizar un tamaño de autorización de M bytes e intervalos de M/R = 10 ms.

Para calcular la fluctuación, el MTA no sabe cuánto se desvía el CMTS de un comportamiento ideal en su planificación. El cliente debería asumir que el CMTS es ideal, lo cual significa que el retardo que experimentará con estas TSpec y su velocidad reservada R = r es simplemente:

b/r + retardos de propagación

Si no se tiene en cuenta el tiempo de propagación, el retardo es de 10 ms. Supóngase que el cliente está dispuesto a tolerar un retardo de 15 ms para esta sesión (solamente en el trayecto cliente-CMTS), lo que supone un término de inactividad (S) de 15 – 10 = 5 ms. Al recibir la reserva, el CMTS interpreta esto como una indicación de que el cliente acepta una fluctuación de autorización de 5 ms.

Supóngase que el cliente está dispuesto a tolerar un retardo de 25 ms y fija su término de inactividad en 25 – 10 = 15 ms. El CMTS puede utilizar esta información para determinar que puede utilizar un intervalo superior de autorización, por ejemplo 20 ms, que significa un posible retardo de 20 ms máximo para un paquete que llegue al CM inmediatamente después de una autorización. Todavía queda un margen de inactividad de 5 ms, que el CMTS puede adoptar como valor de fluctuación de autorización.

Obsérvese que este método facilita considerablemente la satisfacción de requisitos del cliente en lo relativo al retardo, porque el CMTS puede adoptar la solución más adaptada a sus capacidades.

### 6.1.3 Autorización y comportamiento del CMTS

Al recibir una solicitud de reserva o compromiso de anchura de banda con un identificador (GateID), el CMTS tiene que hacer un control de admisión para esa petición con los objetos de puerta asociados al GateID.

Todas las peticiones DSA o DSC procedentes de un E-MTA para una determinada sesión TIENEN QUE incluir un GateID en el bloque de autorización. Si no se ha incluido, el CMTS TIENE QUE rechazar la petición con el código de confirmación 24 (Autorización denegada). Si recibe un mensaje de petición DSC que contiene un GateID diferente del GateID registrado en la petición DSA con la que se ha creado el flujo de servicio, el CMTS TIENE QUE ejecutar los procedimientos normales de autorización y admisión utilizando la puerta asociada al nuevo GateID.

Si el MTA no utiliza múltiples autorizaciones por intervalo en el flujo de servicio que se está modificando y el resultado del control de autorización y admisión es positivo, el CMTS TIENE QUE asociar el nuevo GateID al flujo de servicio modificado, reemplazar los valores Temporización de flujo admitido y Temporización de flujo de activo del flujo de servicio asociado, por los temporizadores T7 y T8 de la nueva puerta en sentido ascendente, e incluir estos valores de temporización en la respuesta DSC al MTA. En este caso, el CMTS TIENE QUE retirar inmediatamente la puerta original y notificar al CMS mediante un mensaje Cierre de puerta con el subcódigo de motivo 0 (Normal).

Si el MTA utiliza múltiples autorizaciones por intervalo en el flujo de servicio que se está modificando y el resultado del control de autorización y admisión es positivo, el CMTS TIENE QUE asociar el nuevo GateID al nuevo flujo de servicio, sin introducir modificaciones a los flujos o puertas existentes asociados con esos subflujos. El CMTS DEBE reemplazar los valores Temporización de flujo admitido y Temporización de flujo de activo asociados con el flujo de servicio, con los temporizadores T7 y T8 de la nueva puerta en sentido ascendente, e incluir estos valores de temporización en la respuesta DSC al MTA.

Al autorizar otro flujo de servicio, los elementos del CMTS y el CMS NO REUTILIZARÁN una puerta asociada anteriormente a un flujo de servicio. En estos casos, el CMTS TIENE QUE rechazar las peticiones de reserva o compromiso para un nuevo flujo de servicio, transmitiendo el código de confirmación DOCSIS 24 (Autorización denegada).

Si el módulo de autorización IPCablecom recibe una petición de reserva de anchura de banda sin bloque de autorización, el CMTS TIENE QUE rechazarla con el código de confirmación 24 (Autorización denegada).

Obsérvese que el requisito anterior se aplica a peticiones de anchura de banda procesadas por el módulo de autorización de IPCablecom. Sin embargo, esto no impide usar el módulo de autorización DOCSIS para procesar otras peticiones sin un bloque de autorización. El módulo de autorización IPCablecom y el módulo de autorización DOCSIS son funciones lógicas del CMTS que aprueban o deniegan parámetros QoS y clasificadores. Conceptualmente, cuando una petición QoS llega al CMTS, el módulo de autorización DOCSIS determina si la petición se procesará en el propio módulo de autorización DOCSIS o la pasará al módulo de autorización IPCablecom.

Si el CMTS no encuentra ninguna puerta asociada al GateID, TIENE QUE transmitir un código de confirmación 24, (Autorización denegada) para indicar que se ha denegado la autorización y la petición será rechazada.

Si el CMTS encuentra una puerta asociada al GateID, tiene que ejecutar el siguiente procedimiento de autorización. Para hacer el control de admisión de mensajes DOCSIS DSx y comparar los parámetros de estos mensajes con los parámetros de los mensajes autorizados mediante el objeto GateSpec, el CMTS tiene que determinar parámetros de QoS estándar de capa dos o tres, introduciendo o retirando tara. En los ejemplos de normalización a parámetros de capa tres de esta Recomendación, los parámetros DOCSIS se convierten en sus equivalentes RSVP por los métodos descritos en la presente cláusula.

- La capacidad del contador en GateSpec (b) TIENE QUE ser igual al valor de la petición del MTA o superior.
- La velocidad del contador en GateSpec (r) TIENE QUE ser igual al valor de la petición del MTA o superior.
- El tamaño máximo del datagrama en GateSpec (M) TIENE QUE ser igual al valor de la petición del MTA o superior.
- El tamaño minimo de datagrama GateSpec (m) TIENE QUE ser igual al valor de la petición del MTA o superior.
- La velocidad máxima en GateSpec (p) TIENE QUE ser igual al valor de la petición del MTA o superior.
- La velocidad reservada en GateSpec (R), TIENE QUE ser igual al valor de la petición del MTA o superior.
- El término de inactividad en GateSpec (s), TIENE QUE ser igual al valor de la petición del MTA o superior.
- El protocolo en GateSpec TIENE QUE corresponder al protocolo de la petición del MTA.
- La dirección de destino en GateSpec TIENE QUE ser la misma de la petición del MTA, si el valor de GateSpec es diferente de cero. Si el valor de GateSpec es cero, NO SE HARÁ esta comparación.
- El puerto de destino en GateSpec TIENE QUE ser el mismo de la petición del MTA, si el valor de GateSpec es diferente de cero. Si el valor de GateSpec es cero, NO SE HARÁ esta comparación.

– La dirección de fuente en GateSpec TIENE QUE ser la misma de la petición del MTA, si el valor de GateSpec es diferente de cero. Si el valor de GateSpec es cero, NO SE HARÁ esta comparación.
– El puerto de fuente en GateSpec TIENE QUE ser el mismo de la petición del MTA, si el valor de GateSpec es diferente de cero. Si el valor de GateSpec es cero, NO SE HARÁ esta comparación.

Si el resultado de una de estas comparaciones de autorización es negativo para un mensaje de petición de un nuevo flujo de servicio o de aviso de parámetros de reserva de un flujo existente, el CMTS NO APROBARÁ la petición (creación de un nuevo flujo de servicio o modificación de los parámetros del flujo de servicio existente). Si el MTA envía una petición para comprometer recursos para un flujo de servicio reservado, el proceso de autorización SE TIENE QUE hacer con los parámetros DOCSIS y el método definido en DOCSIS.

## 6.2 Soporte de DOCSIS para la reserva de recursos

En la Rec. UIT-T J.112 no existe una forma definida de transmitir información de autorización desde el CM al módulo de autorización del CMTS. El módulo de autorización es una función lógica del CMTS definida en la Rec. UIT-T J.112. En esta Recomendación se utiliza una nueva codificación TLV (tipo/longitud/valor) DOCSIS que comunica al CMTS un bloque de autorización consistente en una cadena arbitraria de longitud *n* que sólo es interpretada y procesada por el módulo de autorización.

En el modelo de QoS dinámica se autoriza cada sesión y para ello se asigna un alias al CMTS y al MTA, que permite relacionar las peticiones y las autorizaciones. Este alias es el identificador de puerta (GateID). Cuando recibe la información de señalización de llamada, el MTA comunica este identificador al CMTS utilizando el TLV bloque de autorización (AuthBlock) incluido en un mensaje DSA/DSC.

El CMTS IPCablecom DEBE disponer de mecanismos para habilitar/inhabilitar varios métodos de autorizar una petición CM DSx para iniciar y/o modificar flujos de servicio. El CMTS IPCablecom DEBE aplicar el método "autorización de GateID" , en el que el CMTS autoriza únicamente a las peticiones que contengan un GateID en el bloque de autorización IPCablecom. El CMTS DEBERÍA aplicar la autorización nombre de clase de servicio (SCN, *service class name*), en la que el CMTS autoriza peticiones DSx sólo para un conjunto configurado de nombres de clase de servicio definidos en el CMTS.

### 6.2.1 Reserva/Compromiso de QoS en dos fases

Hay tres conjuntos de parámetros de calidad de servicio asociados a un flujo de servicio DOCSIS: de estado Configurado, de estado Admitido o de estado Activo, que se relacionan exactamente como los recursos autorizados, reservados o comprometidos de 5.7.4.

Las operaciones de reserva y compromiso se realizan mediante mensajes de servicio dinámico DOCSIS, modificando los valores AdmittedQoSParameterSet y ActiveQoSParameterSet del flujo de servicio. En un mensaje Añadir servicio de forma dinámica (DSA, *dynamic service addition*) o Modificar servicio de forma dinámica (DSC, *dynamic service change*), la reserva consiste en incluir el TLV "tipo de conjunto de parámetros de QoS" (QoSParameterSetType) con el valor Admisión (valor 2) en las codificaciones de flujo de servicio ascendente o descendente. Asimismo, el compromiso se realiza seleccionando los valores Actividad (valor 4) o Admisión+Actividad (valor 6) para QoSParameterSetType.

Los intercambios de DSA y DSC entre el CM y el CMTS son una toma de contacto triple que consiste en un mensaje de petición seguido de una respuesta y un acuse de recibo. Esto se ilustra en la figura 5.

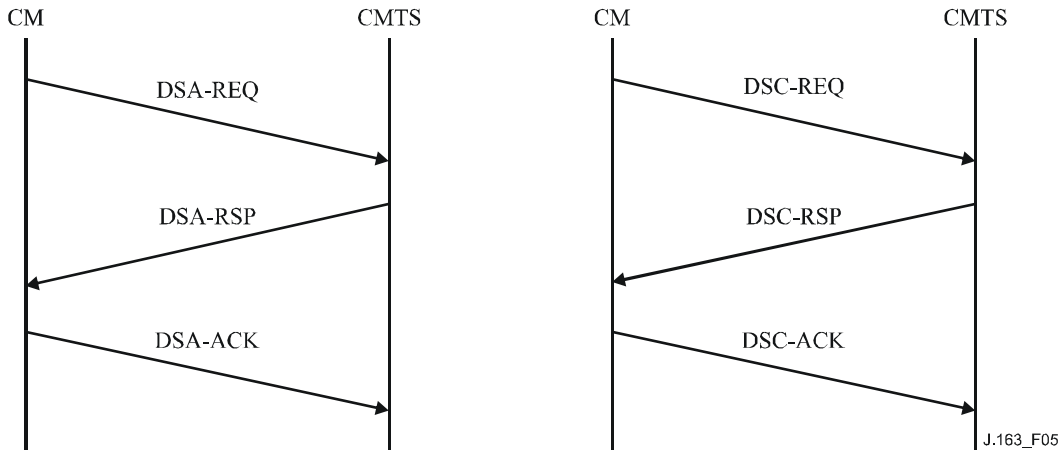



**Figura 5/J.163 – Mensajes DSA y DSC entre el CM y el CMTS**

Por ejemplo, el resultado del siguiente mensaje DSA-REQ es la admisión de los flujos de servicio ascendente y descendente, es decir, la reserva de los recursos de QoS que se han de utilizar en la red DOCSIS.

DSA-REQ

| | | |
|---|---|---|
| Identificador de transacción | | 1 |
| Flujo de servicio ascendente | Referencia flujo de servicio | 1 |
| | Tipo de parámetros de QoS | Admitido (2) |
| | Planificación flujo de servicio | UGS (6) |
| | Intervalo de autoriz. nominal | 10 ms |
| | Fluctuación de autoriz. tolerada | 2 ms |
| | Autorizaciones por intervalo | 1 |
| | Tamaño autorizac. sin petición | 222 |
| Flujo de servicio descendente | Referencia flujo de servicio | 2 |
| | Tipo de parámetros de QoS | Admitido (2) |
| | Prioridad del tráfico | 3 |
| | Velocidad máxima sostenida | 12000 |

Otro ejemplo: el resultado del siguiente mensaje DSC-REQ sería la activación del flujo de servicio, es decir, el compromiso de los recursos de QoS que se han de utilizar en la red DOCSIS.

DSC-REQ

| | | |
|---|---|---|
| Identificador de transacción | | 1 |
| Flujo de servicio ascendente | Identificador flujo de servicio | 10288 |
| | Tipo de parámetros de QoS | Admitido + Activo (6) |
| | Planificación flujo de servicio | UGS (6) |
| | Intervalo de autoriz. nominal | 10 ms |
| | Fluctuación de autoriz. tolerada | 2 ms |
| | Autorizaciones por intervalo | 1 |
| | Tamaño de autoriz. sin petición | 222 |

DSC-REQ

| | | |
|---|---|---|
| Flujo de servicio descendente | Identificador flujo de servicio | 10289 |
| | Tipo de parámetros de QoS | Admitido + Activo (6) |
| | Prioridad del tráfico | 3 |
| | Velocidad máxima sostenida | 12000 |

Para especificar los conjuntos de parámetros de QoS Admitido y Activo el MTA envía las peticiones MAC_CREATE_SERVICE_FLOW y MAC_CHANGE_SERVICE_FLOW. Generalmente, el flujo de servicio que se admite ya tiene clasificadores asociados.

### 6.2.2 Mantenimiento de la reserva

Los parámetros de QoS "Temporización de actividad" (TimeoutForActiveQoSParameters) y "Temporización de admisión" (TimeoutForAdmittedQoSParameters) del flujo de servicio DOCSIS permiten terminar una sesión inactiva y liberar sus recursos.

La temporización de actividad (TimeoutForActiveQoSParameters) permite recuperar recursos asignados a CM que han perdido la conexión con la red de cable por cese, fallo o de otra forma. Esta acción de recuperación no se realizará mientras se transmitan paquetes de datos normalmente sobre el flujo de servicio.

Si la temporización de actividad DOCSIS expira en el CMTS para un flujo de servicio autorizado a través de una puerta (por ejemplo, PacketCable), el CMTS transmitirá una petición DOCSIS DSD para suprimir todos los flujos de servicio asociados a la puerta. En su mensaje de notificación de cierre al GC, el CMTS especificará "Expiración de temporización T8 – Inactividad del flujo de servicio en sentido ascendente".

Si el MTA ha habilitado la detección de actividad vocal mediante una planificación UGS/AD del flujo de servicio, y el CMTS supervisa de forma activa la actividad del flujo ascendente, durante los periodos de silencio prolongados el MTA TIENE QUE enviar paquetes de datos periódicamente sobre el flujo de servicio o renovar el temporizador de actividad mediante mensajes DSC. La temporización de admisión (TimeoutForAdmittedQoSParameters) permite recuperar recursos reservados por un CM pero no comprometidos. Habitualmente no es necesario, porque los parámetros comprometidos son idénticos a los parámetros reservados. Si el compromiso es inferior a la reserva es necesario restablecer periódicamente el temporizador del CMTS y para ello se realiza una operación DSC-REQ que reserva nuevamente los mismos recursos.

### 6.2.3 Soporte de la vinculación dinámica de recursos

El modelo de QoS dinámico exige la capacidad de modificar dinámicamente la vinculación de recursos a flujos. Por ejemplo, para proporcionar espera de llamada puede resultar conveniente mantener recursos suficientes para una sola sesión por la red DOCSIS y conmutar la atribución de esos recursos de un llamante a otro.

Para acomodar esta funcionalidad se añade un objeto Resource-ID, que es un identificador opaco generado por el nodo que controla los recursos, en este caso el CMTS.

Cuando un cliente emite una petición de reserva para un nuevo flujo, incluye el ResourceID en dicha petición para indicar al CMTS que esta sesión desea compartir recursos para esta nueva puerta (puerta 2) con una puerta creada anteriormente (puerta 1). Siempre que la QoS solicitada para la nueva puerta pueda ser satisfecha con una atribución de anchura de banda menor o igual que la de la puerta existente, no será necesario reservar anchura de banda adicional en la red DOCSIS. Ahora bien, quizá sea necesario reservar anchura de banda en la red troncal, dependiendo del trayecto de extremo a extremo que tome la nueva sesión. El acceso a la reserva compartida se realiza de manera mutuamente excluyente.

La vinculación dinámica de recursos (cláusula 5.7.7) se realiza en la Rec. UIT-T J.112 mediante el TLV bloque de autorización.

El CMTS TIENE QUE incluir el identificador de recursos en el TLV bloque de autorización para el mensaje DSA-RSP que envía al cliente. El cliente PUEDE incluir este identificador en los siguientes mensajes DOCSIS relativos a los mismos recursos. Principalmente, si el cliente desea establecer otra sesión y reutilizar los recursos de una sesión existente, TIENE QUE desactivar, en primer lugar, los flujos de servicio de la sesión anterior mediante una DSC-REQ e incluir el identificador de recursos asociado a esta última sesión en el mensaje DSA-REQ que envía al cliente.

### 6.2.4 Concordancia de parámetros de QoS para la autorización

La puerta correspondiente al identificador se parametriza mediante una especificación de flujos RSVP (objetos ASPEC y TSpec RSVP) en los dos sentidos. El módulo de autorización del CMTS tiene que convertir los parámetros DOCSIS de QoS en los respectivos parámetros RSVP, aplicando las siguientes reglas:

Los parámetros *Tamaño de contador de testigos* (b), *Tamaño máximo del paquete* (M), y *Mínima unidad supervisada* (m) SE TIENEN QUE configurar con el valor *DOCSIS Tamaño de autorización sin petición* menos la tara UGS ascendente DOCSIS[6] (en sentido ascendente), y el valor *DOCSIS Tamaño mínimo previsto de paquete a la velocidad reservada* menos la tara DOCSIS descendente[7] (en sentido descendente).

En sentido descendente, los parámetros *Velocidad del contador de testigos* (r) y *Velocidad de datos máxima* (p) SE TIENEN QUE calcular convirtiendo el valor *DOCSIS Velocidad máxima sostenible* en valores de capa 3, dividiendo ese valor por el valor *DOCSIS Tamaño mínimo previsto de paquete a la velocidad reservada* y multiplicando el resultado por el *Tamaño máximo del paquete* calculado antes. En sentido ascendente, los parámetros *Velocidad del contador de testigos* (r) y *Velocidad de datos máxima* (p) SE TIENEN QUE configurar con el valor *DOCSIS Intervalo nominal de autorización* multiplicado por el valor *Tamaño de autorización sin petición*.

En sentido descendente, el parámetro *Velocidad* (R) SE TIENE QUE calcular convirtiendo el valor *DOCSIS Velocidad del tráfico máxima reservada* en valores de capa 3, dividiendo ese valor por el valor *DOCSIS Tamaño mínimo previsto de paquete a la velocidad reservada* y multiplicando el resultado por el valor de *Mínima unidad supervisada* calculado antes. En sentido ascendente, el parámetro *Velocidad* (R) SE TIENE QUE configurar con el valor *DOCSIS Intervalo nominal de autorización* multiplicado por el valor *Tamaño de autorización sin petición*.

El *Término de inactividad* SE TIENE QUE configurar con el valor *DOCSIS Fluctuación de autorización tolerada* en sentido ascendente. El término de inactividad TIENE QUE ser cero para el flujo descendente, para indicar que este parámetro no será especificado por el MTA.

El *Protocolol ID* TIENE QUE ser el *Protocolo IP DOCSIS*.

---

6 En esta tara deberían incluirse los 18 bytes de tara de encabezamiento Ethernet (6 bytes para dirección de fuente, 6 bytes para dirección de destino, 2 bytes para longitud y 4 bytes para CRC). También se incluye la tara de capa MAC DOCSIS: encabezamiento básico DOCSIS (6 bytes), encabezamiento ampliado UGS (3 bytes) y encabezamiento ampliado BPI+ (5 bytes). Si se ha validado la supresión de encabezamiento de cabida útil (PHS, *payload header suppression*) hay que añadir el número de bytes suprimidos al valor DOCSIS Tamaño de autorización sin petición.

7 Hay 18 bytes de tara de capa MAC DOCSIS (6 bytes para la dirección de fuente, 6 bytes para la dirección de destino, 2 bytes para la longitud y 4 bytes para CRC). Si se ha validado la supresión de encabezamiento de cabida útil (PHS) en sentido descendente, hay que restar el número de bytes suprimidos del valor *DOCSIS Tamaño mínimo previsto de paquete a la velocidad reservada*.

La *Dirección de destino* TIENE QUE ser la *Dirección de destino IP DOCSIS*. Si se omite este parámetro ES OBLIGATORIO asignar el valor cero.

El *Puerto de destino* TIENE QUE ser el *Puerto de destino IP inicial DOCSIS*. Si se omite este parámetro ES OBLIGATORIO asignar el valor cero.

La *Dirección de fuente* TIENE QUE ser la *Dirección de fuente IP DOCSIS*. Si se omite este parámetro ES OBLIGATORIO asignar el valor cero.

El *Puerto de fuente* TIENE QUE ser el *Puerto de fuente IP inicial DOCSIS*. Si se omite este parámetro ES OBLIGATORIO asignar el valor cero.

Ahora es necesario verificar los objetos resultantes por referencia a la puerta correspondiente y aplicando las siguientes reglas:

Todos los parámetros solicitados de *especificación de flujo RSVP* y *término de inactividad* TIENEN QUE ser iguales a los valores especificados de la puerta o inferiores.

Todos los parámetros solicitados de *especificación de tráfico RSVP* TIENEN QUE ser iguales a los valores especificados de la puerta. Ahora bien, si el valor de la puerta es cero, NO SE VERIFICARÁ el correspondiente parámetro solicitado.

Si el resultado de la verificación es positivo, el CMTS TIENE QUE tratar la petición. Si el resultado es negativo, el CMTS TIENE QUE rechazar definitivamente la petición por denegación de autorización.

Véase por ejemplo el caso de un códec G.711 con formación tramas a 20 ms, con un MAC RTP-S de 2 bytes y capacidad BPI+:

G.711 @ 20 ms

velocidad binaria nominal de 64 kbit/s

velocidad de bytes nominal de 8 kbyte/s

tasa de formación de tramas de 20 ms = 50 paquetes/segundo

8 kbyte/s / 50= 160 bytes por paquete de cabida útil

42 bytes de encabezamiento IP/UDP/RTP

160 + 42 = 202 bytes en total por paquete

202 × 50 = velocidad de bytes efectiva de 10,1 kbyte/s

10,1 × 8 = velocidad binaria efectiva de 80,8 kbyte/s

Estos serían los parámetros GateSpec resultantes establecidos por el CMS:

Capacidad del contador (b) = tamaño del datagrama, incluyendo la tara de encabezamiento IP/UDP/RTP-S = 202 bytes

Mínima unidad supervisada (m) = Capacidad del contador (b) = 202 bytes

Tamaño máximo del datagrama (M) = Capacidad del contador (b) = 202 bytes

Velocidad del contador (r) = velocidad de datos efectiva, incluyendo la tara de encabezamiento IP/UDP/RTP-S = 10100 bytes por segundo

Velocidad máxima (p) = Velocidad del contador (r) = 10100 bytes por segundo

Velocidad reservada (R) = Velocidad del contador (r) = 10100 bytes por segundo

Los parámetros DOCSIS en sentido ascendente incluyen la tara desde el byte FC hasta la CRC.

Encabezamiento básico DOCSIS (FC hasta HCS, ningún encabezamiento ampliado): 6 bytes

Encabezamiento ampliado UGS: 3 bytes

Encabezamiento ampliado BPI+: 5 bytes

Encabezamiento Ethernet: 14 bytes

CRC: 4 bytes

Tara total en sentido ascendente: 32 bytes por paquete

Parámetros de flujo de servicio DOCSIS:

Tipo de planificación en sentido ascendente: UGS

Política de petición/transmisión (máscara de bits): bits 0-6 y 8 puestos a uno (valor binario 101111111)

Tamaño de autorización: 234 bytes

Autorizaciones por intervalo (entero): 1

Intervalo de autorización: 20000 microsegundos

Fluctuación de autorización tolerada: 800 microsegundos

El procedimiento de control de autorización CMTS para los parámetros en sentido ascendente:

Es necesario retirar la tara capa MAC de los parámetros DOCSIS, para poder comparar con los parámetros GateSpec.

Capacidad del contador en GateSpec (b) ≥ Valor DOCSIS Tamaño de autorización sin petición – 32 bytes

202 bytes ≥ 234 bytes – 32 bytes = 202 bytes

Velocidad del contador en GateSpec (r) ≥ 1/Intervalo de autorización DOCSIS × (Tamaño de autorización sin petición DOCSIS – 32)

10,1 kbyte/s ≥ 1/20 ms × (234 bytes – 32 bytes) = 50 paquetes por segundo × 202 bytes por paquete = 10,1 kbyte/s.

Los parámetros DOCSIS en sentido descendente incluyen la tara, desde el byte situado inmediatamente después de HCS hasta la CRC.

Encabezamiento Ethernet: 14 bytes

CRC: 4 bytes

Tara total en sentido descendente: 18 bytes por paquete

Parámetros de flujo de servicio DOCSIS en sentido descendente:

Ráfaga de tráfico máxima (valor mínimo de 1522): 1522 bytes

Velocidad máxima soportada: 88000 bits por segundo

Tamaño mínimo previsto de paquete a la velocidad reservada: 220 bytes

Velocidad mínima reservada: 88000 bits por segundo

Prioridad del tráfico: 5

Procedimiento de control de autorización del CMTS para los parámetros en sentido descendente:

En este caso también es necesario restar la tara de los parámetros DOCSIS para poder comparar con GateSpec. En el caso del parámetro DOCSIS Tamaño mínimo previsto de paquete a la velocidad reservada es una simple sustracción, pero la adaptación del parámetro Velocidad mínima reservada es algo más compleja.

Mínima unidad supervisa en GateSpec (m) ≥ Valor DOCSIS Tamaño mínimo previsto de paquete a la velocidad reservada – (18 × z) bytes

Por ejemplo, si autorizaciones por intervalo=z=1

202 bytes ≥ 220 bytes – 18 bytes = 202 bytes

Velocidad del contador en GateSpec (r) ≥ (Velocidad mínima reservada DOCSIS/ (8 × Tamaño mínimo previsto de paquete a la velocidad reservada DOCSIS )) = (Tamaño mínimo previsto de paquete a la velocidad reservada DOCSIS – 18 × z bytes)

Por ejemplo, si autorizaciones por intervalo=z=1

10,1 kbyte/s ≥ (88 kbit/s / (8 × 220 bytes)) × (220 bytes – 18 bytes) = 10,1 kbyte/s

### 6.2.5 Codificación del bloque de autorización

El bloque de autorización es una cadena de bytes que se codifica con campos TLV (Tipo-Longitud-Valor) para permitir su adaptación. Los campos de tuplas TLV no están ordenados y pueden aparecer anidados. En el campo Valor (bytes) debe utilizarse un valor superior a cero. Los campos Tipo y Longitud son de un byte de longitud. Téngase presente que la longitud sólo incluye el campo Valor, no la tupla TLV completa.

Formato del bloque de autorización

**Codificación del bloque de autorización IPCablecom**

Este campo define los parámetros asociados al bloque de autorización IPCablecom. Obsérvese que este campo está formado por subcampos anidados.

| Tipo | Longitud | Valor |
|---|---|---|
| 1 | n | "véanse los siguientes subcampos" |

**Codificación de Gate ID**

El valor de este campo es el alias gate-id que se utiliza para los fines de autorización.

| Tipo | Longitud | Valor |
|---|---|---|
| [1].1 | 4 | GateID |

**Codificación de Resource-id**

El valor de este campo es el alias resource-id que se utiliza para identificar exclusivamente el conjunto de recursos asociados al flujo de servicio.

| Tipo | Longitud | Valor |
|---|---|---|
| [1].2 | 4 | resource-id |

**Estado del subflujo**

| Tipo | Longitud | Valor |
|---|---|---|
| [1].3 | 1 | estado |

Este byte especifica el estado en que se encuentra el subflujo que puede tener 4 estados: (0-admitido, 1-activo, 2-suprimido, 3-transferido). El byte de estado sirve para ayudar al CMTS a controlar el estado de las diversas puertas que pueden estar en un mismo flujo de servicio. Este parámetro DEBE estar incluido en todas las peticiones DSx iniciadas por el CM cuyo parámetro múltiples autorizaciones por intervalo tenga un valor mayor que 1.

Admitido (0) – el subflujo se encuentra en el estado admitido

Activo (1) – el subflujo se encuentra en estado activo

Suprimido (2) – puerta que se ha de suprimir como consecuencia de esta DSC

Transferido (3) – subflujo transferido a un nuevo flujo de servicio

Para permitir que el CMTS relacione adecuadamente los cambios de un determinado GateID, el MTA DEBE incluir únicamente un bloque de autorización DOCSIS (tipo 30) en una determinada petición DSx. Para cada subflujo del flujo, el bloque de autorización DOCSIS DEBE contener una

codificación de bloque de autorización IPCablecom (tipo 30.1) junto con el necesario sub-TL GateID (tipo 30.1.1) y posiblemente otros sub-TLV. Si sólo se utiliza una autorización por intervalo (y, por consiguiente, un solo GateID), el campo Bloque de autorización DEBE estar presente y, no obstante, el campo estado del subflujo DEBE omitirse.

Para mayor información sobre autorización CMTS, véase 6.1.3.

### 6.2.6 Supresión del encabezamiento de cabida últil

La especificación DOCSIS RFI describe las reglas para añadir y suprimir reglas PHS (asociadas con un clasificador). Sin embargo, no está claramente definido el procedimiento para actualizar una regla PHS cuando ésta resulte insuficiente. El procedimiento descrito a continuación para el MTA y el CMTS es OBLIGATORIO cuando sea necesario modificar una regla PHS de un flujo de voz.

En caso de que una regla PHS existente sea insuficiente, el MTA DEBE generar una sola transacción DSC que:

– Añada un nuevo clasificador con una nueva regla PHS.

– Ajuste la capacidad máxima de QoS con arreglo a la nueva regla PHS.

– Suprima el clasificador anterior y la correspondiente regla PHS.

## 6.3 Utilización de la interfaz de servicio de control MAC DOCSIS

Los parámetros de QoS DOCSIS del flujo de servicio que se obtienen de la descripción SDP serán comunicados para establecer el flujo o flujos de servicio. En esta cláusula se describe este proceso utilizando las interfaces de servicio de control MAC DOCSIS (anexo E al anexo B/J.112).

El MTA integrado envía los siguientes mensajes de señalización para los recursos de QoS entre las primitivas de la interfaz del servicio de control MAC DOCSIS:

1) Petición MAC_CREATE_SERVICE_FLOW:

   Tal como se describe en B.E.3.2/J.112, mediante esta primitiva el MTA integrado puede solicitar que se añada un flujo de servicio. Esta primitiva también puede utilizarse para definir clasificadores para el nuevo flujo de servicio, así como para suministrar los conjuntos de parámetros de QoS del flujo de servicio Admitido y Activo. Para señalar el resultado positivo o negativo de esta primitiva se envía la primitiva de respuesta MAC_CREATE_SERVICE_FLOW.

2) Petición MAC_CHANGE_SERVICE_FLOW:

   Mediante esta primitiva el MTA integrado puede iniciar una modificación de los conjuntos de parámetros de QoS Admitido y Activo, por ejemplo para poner la parte llamante en espera. Para señalar el resultado positivo o negativo de esta primitiva se envía la primitiva de respuesta MAC_CHANGE_SERVICE_FLOW.

3) Petición MAC_DELETE_SERVICE_FLOW:

   Cuando el MTA integrado ya no necesita el flujo de servicio, envía al CM integrado una petición MAC_DELETE_SERVICE_FLOW para poner a cero los conjuntos de parámetros de QoS del flujo de servicio Admitido y Activo.

Los parámetros de estas primitivas concuerdan con los parámetros asociados a los mensajes DSA, DSC y DSD descritos en el anexo B/J.112.

### 6.3.1 Establecimiento de la reserva

El MTA inicia la reserva de recursos de QoS mediante la primitiva de petición MAC_CREATE_SERVICE_FLOW. El MTA TIENE QUE incluir el ID de puerta en el TLV bloque de autorización. Al recibir este mensaje, la capa MAC del CM invoca la señalización DSA enviando al CMTS una petición DSA_REQ. El CMTS TIENE QUE verificar la autorización

tomando como referencia el identificador de puerta (incluido en el TLV bloque de autorización) y rechazar la petición si la puerta no es válida o los recursos autorizados son insuficientes para la petición. Al recibir la respuesta DSA_RSP del CMTS, el servicio MAC informa de ello a la capa superior utilizando el mensaje respuesta MAC_CREATE_SERVICE_FLOW. Este proceso se ilustra en la figura 6.

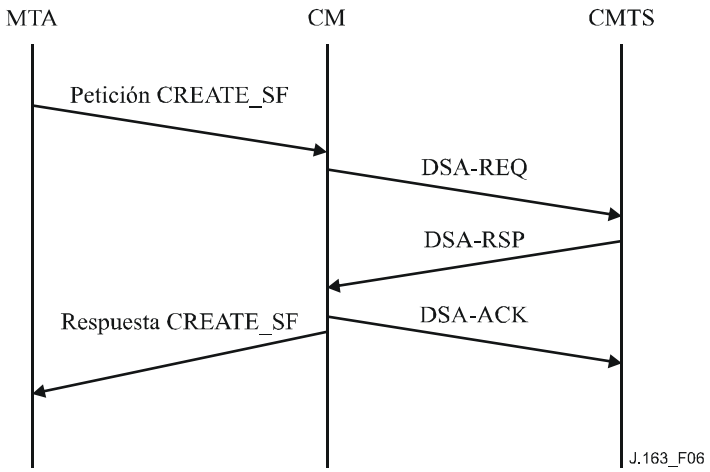



**Figura 6/J.163 – Establecimiento de la reserva**

### 6.3.2 Modificación de la reserva

El MTA inicia cambios en los recursos de QoS utilizando la primitiva de petición MAC_CHANGE_SERVICE_FLOW. Este proceso se ilustra en la figura 7.

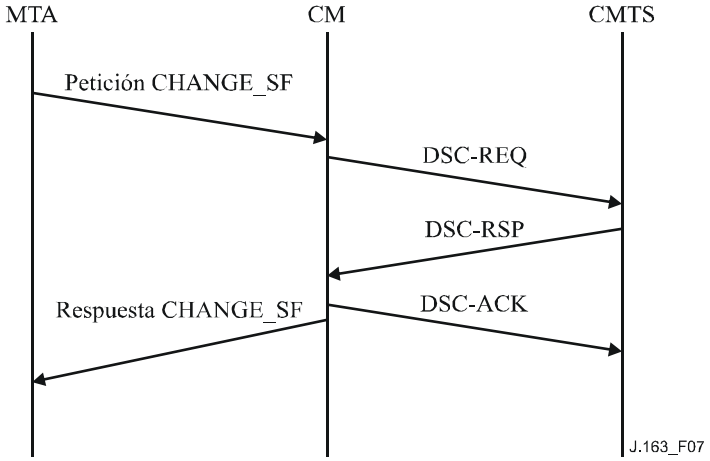



**Figura 7/J.163 – Modificación de la reserva**

Al recibir este mensaje la capa MAC del CM invoca la señalización DSC. Al recibir la respuesta DSC_RSP del CMTS, el servicio MAC informa a la capa superior mediante el mensaje respuesta MAC_CHANGE_SERVICE_FLOW.

### 6.3.3 Supresión de la reserva

El MTA inicia la desasignación de una reserva de QoS mediante la primitiva de petición MAC_DELETE_SERVICE_FLOW. Al recibir este mensaje la capa MAC invoca la señalización DSD. Al recibir la respuesta DSD_RSP del CMTS, el servicio MAC informa a la capa superior mediante el mensaje de respuesta MAC_DELETE_SERVICE_FLOW. Este proceso se ilustra en la figura 8.

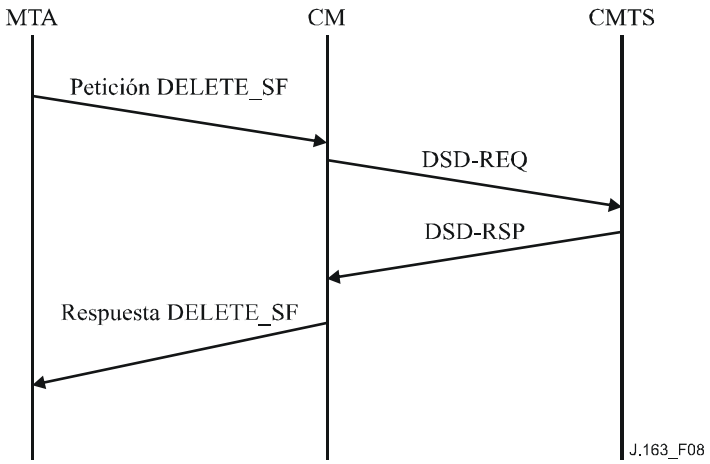



**Figura 8/J.163 – Supresión de la reserva**

### 6.3.4 Consideraciones relativas a multiples autorizaciones por intervalo

#### 6.3.4.1 Adición de un par de subflujos

Dado que únicamente se permite un solo bloque de autorización en un determinado mensaje DSx, cuando el MTA añade un clasificador, DEBE utilizar el TLV de acción de cambio de servicio dinámico (además del campo estado del subflujo en el bloque de autorización) con un valor de 0.

Para añadir un par de subflujos el MTA TIENE QUE hacer lo siguiente:

– Enviar un DSC con un bloque de autorización que contenga información para todas las puertas del subflujo.

– Poner a 0 (reservar) a (comprometer) el campo estado de subflujo de cada puerta.

– Incluir los clasificadores (sentidos ascendente y descendente) relacionados con la puerta con el TLV de acción de cambio de servicio dinámico puesto a 0 – DSC añadir clasificador. El MTA DEBE incluir únicamente clasificadores pertinentes a la puerta que está funcionanto en el DSC.

– Incluir los parámetros de QoS en sentido ascendente y aumentar en una unidad el número de autorizaciones por intervalo para el conjunto de parámetros de QoS admitidos (y posiblemente el conjunto de parámetros de QoS activos si además se asignan los recursos).

– Ajustar el LUB del parámetro de QoS en sentido descendente para tratar todos los subflujos en sentido descendente.

Tras recibir este DSC, el CMTS DEBE realizar el control de admisión de conformidad con 6.1.3.

#### 6.3.4.2 Modificación de un par de subflujos

Cuando resulte necesario un cambio de recursos, el MTA NO DEBE modificar los parámetros de QoS del flujo de servicio DOCSIS existentes, sino que DEBE transferir el subflujo a un nuevo flujo de servicio, o a un nuevo subflujo en el flujo de servicio existente. Para transferir un par de subflujos (en los sentidos ascendente y descendente relacionados con un GateID) el MTA DEBE hacer lo siguiente:

– El MTA envía una DSC-REQ para poner el subflujo en el estado "transferido" , pone el clasificador en estado inactivo y anula todos los recursos activos comprometidos para el par de subflujos.

– El CMTS envía un DSC-RSP y arranca el temporizador de admisión DOCSIS cuyo valor TIENE QUE ser el del temporizador T7 configurado en el GateSet asociado con el GateID incluido en la DSC-REQ.

– Tras recibir el DSC-RSP, el MTA envía un DSC-ACK y comienza a transferir el subflujo enviando una DSA-REQ (para transferirlo a un nuevo flujo de servicio) o DSC-REQ (para transferirlo a un flujo de servicio existente) a fin de reservar/comprometer el nuevo par de flujo de servicio (con el mismo GateID).
– Tras establecer correctamente el nuevo par de flujos de servicio, el MTA DEBE enviar inmediatamente una DSC-REQ para suprimir el anterior par de subflujos.
– Si el temporizador T7 del anterior subflujo expira antes de recibir una DSA-REQ o una DSC-REQ con el mismo GateID, el CMTS DEBE suprimir el par de subflujos expirado y cerrar la puerta.
– Si el temporizador T7 del anterior subflujo expira después de recibir una DSA-REQ o una DSC-REQ (con los parámetros de QoS admitidos) con el mismo GateID, pero antes de recibir la DSC-REQ que suprime el anterior par de subflujos, el CMTS TIENE QUE suprimir el subflujo expirado y trasferir la puerta al nuevo flujo.

#### 6.3.4.3 Supresión de un par de subflujos

El MTA o el CMTS pueden suprimir pares de subflujos. A continuación se describen los respectivos procedimientos:

**Por el MTA**

Para suprimir un par de subflujos, el MTA DEBE:

– enviar un DSC cuyo bloque de autorización contega información para todas las puertas de subflujos.
– Poner al campo estado del subflujo a 2 – suprimido, a fin de suprimir el par de subflujos.
– Incluir los clasificadores (sentidos ascendente y descendente) asociados con las puertas cuyo TLV de acción de cambio de servicio dinámico esta puesto a 2 – DSC suprimir clasificador, para cada calsificador. El MTA TIENE QUE incluir únicamente la puerta a que está funcionando en el DSC.
– Incluir los parámetros QoS en sentido ascendente y disminuir en una unidad el número de autorizaciones por intervalo para el conjnto de parámetros de QoS admitidos (y posiblemente el conjunto de parámetros de QoS activo, si los recursos estuviesen activos).
– Recalcular el LUB para el flujo descendente una vez suprimido el flujo.

Tras recibir este DSC, el CMTS DEBE suprimir los recursos asociados con el GateID, suprimir la puerta, enviar un mensaje cerrar puerta (Gate-Close) al CMS y enviar una DSC-RSP.

**Por el CMTS**

Aunque no es lo común, puede haber casos en los que el CMTS necesite suprimir recursos, en los sentidos ascendente y descendente, asociados con un GateID (porque recibio una instrucción suprimir puerta). Para suprimir un subflujo de un flujo que contiene otros subflujos válidos, el CMTS DEBE:

– Enviar un DSC que incluya los clasificadores (en los sentidos ascendente y descendente) asociados con la puerta, cuyo TLV de acción de cambio de servicio dinámico está puesto a 2 – DSC suprimir clasificador, para cada clasificador.
– Incluir los parámetros de QoS reduciendo en una unidad el número de autorizaciones por intervalo.
– Recalcular el LUB para el flujo descendente una vez suprimido el flujo.
– Tras recibir un DSC, el MTA DEBE suprimir el calsificador del caso y enviar una DSC-RSP.

Si se suprime el último subflujo HAY QUE, emplear un mensaje DSD para suprimir todo el flujo.

#### 6.3.4.4 Agrupación de flujos de servicio

Pueden añadirse subflujos a los flujos de servicio existentes utilizando para ello el mecanismo definido en 6.3.4.1. Por otra parte, es posible transferir subflujos de un flujo de servicio existente a uno nuevo mediante los mecanismos definidos en 6.3.4.2. Ahora bien, para facilitar la aplicación, NO DEBE transferirse un flujo de servicio existente a otro flujo existente como un subflujo.

Además, el MTA NO DEBE tratar de compartir recursos del flujo de servicio a no ser que así lo indique el CMS mediante la inclusión del ID del recurso (resourceID).

## 7 Descripción de la interfaz de autorización (pkt-q6)

En esta cláusula se describen las interfaces entre el CMTS y el controlador de puerta que autorizan que el MTA reciba una calidad de servicio elevada. La señalización entre el controlador de puerta y el CMTS es necesaria para la gestión de la puerta y para el servicio de control de admisión de la QoS de IPCablecom. Además, para facturar correctamente a los abonados es necesario que el CMTS informe de la utilización real de recursos de QoS "comprometidos" en cada sesión. En esta cláusula también se describe la utilización del protocolo de servicio común de política abierta (COPS, *common open policy service*) para el transporte de mensajes de QoS IPCablecom entre el controlador de puerta y el CMTS.

### 7.1 Puertas: marco de referencia para el control de la QoS

Una "puerta" de QoS dinámica IPCablecom es una entidad de control de políticas implementada en el CMTS para controlar el acceso a servicios de QoS mejorada de una red DOCSIS para un flujo IP. Las puertas son unidireccionales: controlan el acceso a un flujo en sentido ascendente o descendente. Las puertas permiten la creación de clasificadores de flujo DOCSIS que, a su vez, controlan el encaminamiento de paquetes a flujos DOCSIS.

Una puerta se define mediante una N-tupla como un clasificador, pero es diferente. El CMTS TIENE QUE establecer la puerta cuando se autoriza el flujo, y esa puerta existirá hasta que sea explícitamente inhabilitada para terminar la autorización del flujo. SE PUEDE establecer un clasificador DOCSIS y asociarlo a una puerta. Una puerta PUEDE existir antes que el clasificador que ella autoriza o después. Es posible que una puerta esté asociada a uno o dos clasificadores, o ninguno.

Un CMTS que sea conforme a esta Recomendación NO CREARÁ dinámicamente un clasificador con una petición o respuesta de Adición de servicio dinámica (DSA) DOCSIS, excepto si la existencia de una puerta para dicho clasificador lo autoriza. Las puertas tienen un identificador asociado (ID de puerta, GateID). Este identificador, que es administrado localmente por el CMTS en el que se ha creado la puerta, PUEDE estar asociado con una o más puertas unidireccionales. En el caso de una sesión punto a punto, habitualmente existen dos puertas unidireccionales asociadas a un único ID de puerta. Además, existen clasificadores DOCSIS para cada flujo unidireccional establecido.

#### 7.1.1 Clasificador

Un clasificador es una séxtupla con los elementos siguientes:

- Sentido (ascendente/descendente).
- Protocolo.
- IP de fuente.
- IP de destino.
- Puerto de destino.
- Puerto de origen.

Si existe un flujo ascendente y un flujo descendente asociado (que forma parte de la misma sesión), ES OBLIGATORIO crear clasificadores separados para cada uno de ellos. El clasificador se actualiza mediante la reserva para los flujos ascendente y descendente. El flujo de datos de la sesión TIENE QUE coincidir con el clasificador a fin de recibir la calidad de servicio asociada al mensaje de reserva.

El CMTS DEBE aplicar filtros de clasificación de paquetes en sentido ascendente para los flujos de Servicio IPCablecom. Es decir, el CMTS TIENE QUE descartar los paquetes en sentido ascendente que no concuerden con el conjunto de clasificadores de paquetes en sentido ascendente de ese flujo de servicio.

El filtrado de clasificación de paquetes en sentido ascendente es un requisito opcional del CMTS en DOCSIS 1.1. Esta Recomendación exige que se aplique a los flujos de servicio que se utilizan para transportar trenes de medios IPCablecom. Si un CMTS decide aplicar filtros de clasificación en sentido ascendente solamente a los flujos de servicio IPCablecom, y no a otros de flujos de servicio, corresponde al fabricante del CMTS decidir cómo determinar los flujos de servicio IPCablecom. Como ejemplo de política CMTS podría citarse la aplicación de filtros de clasificación de paquetes en sentido ascendente solamente a flujos de servicio ascendentes distintos de los primarios.

### 7.1.2 Puerta

La puerta se asocia a un flujo unidireccional y está definida por los siguientes elementos:

- ID de puerta.
- Clasificador prototipo.
- Varios bits bandera descritos a continuación.
- Capacidad máxima autorizada (especificación de flujo).
- Capacidad máxima reservada (especificación de flujo).
- ID de recurso.

El identificador de puerta (descripción en la cláusula siguiente) tiene 32 bits y lo asigna el espacio local del CMTS en el que reside la puerta. El mismo ID de puerta PUEDE ser compartido por dos puertas máximo. Habitualmente un ID de puerta identifica un único flujo ascendente y un único flujo descendente, y corresponde a una única sesión multimedia.

El clasificador prototipo consta de los mismos seis elementos de un clasificador descritos en la cláusula anterior. El IP de fuente es la dirección IP del iniciador del flujo (desde el punto de vista del CMTS). En el caso de una puerta ascendente en el canal DOCSIS, la dirección IP de fuente es la dirección IP del MTA local. Para un flujo descendente, la dirección IP de fuente es la dirección IP del MTA distante. Se puede atribuir libertad de elección a algunos parámetros del clasificador prototipo. En la señalización de llamada multimedia no se señala el puerto UDP de fuente y por eso no se considera que su valor forme parte de la información de puerta.

El puerto de fuente PUEDE ser de libre elección a fin de soportar los dos protocolos de señalización de llamada IPCablecom (DCS y Rec. UIT-T J.162). Si el puerto de fuente es de libre elección, su valor en los parámetros de puerta es cero.

La dirección IP de fuente puede ser de libre elección a fin de soportar el protocolo de señalización de llamada J.162. En este caso, su valor en los parámetros de puerta es cero.

Las capacidades máximas autorizada y reservada forman parte de las especificaciones de flujo RSVP (tanto T-Spec como R-Spec) y se describen en las cláusulas anteriores.

Una petición de reserva de recursos (tal como se especifica en el mensaje Adición/modificación dinámica del flujo de servicio) SE TIENE QUE comparar con lo autorizado para el identificador de puerta asociado al sentido de la petición del recurso. Los recursos autorizados vienen dados por una

Capacidad máxima autorizada. También se verifica la posibilidad de libre elección de la puerta para determinados elementos.

El ID de recurso es un identificador local de 32 bits que asigna el espacio local del CMTS en el que reside la puerta. Un identificador de recurso puede ser compartido por un número indeterminado de puertas que comparten un conjunto común de recursos, con la única restricción de que sólo una de dichas puertas de cada sentido puede tener recursos comprometidos.

### 7.1.3 Identificador de puerta

El identificador único de puerta (GateID) tiene 32 bits y lo asigna localmente el CMTS en el que reside la puerta. Un ID de puerta PUEDE estar asociado a una o más puertas. En los dos protocolos de señalización de llamada J.162 y DCS se asocia un ID de puerta a cada tramo de la llamada, formado por una única puerta en sentido ascendente y una única puerta en sentido descendente.

El ID de puerta TIENE QUE asociarse a la información siguiente:

- Una o dos puertas (TIENE QUE ser una de las siguientes combinaciones):
  - Una única puerta ascendente.
  - Una única puerta descendente.
  - Una única puerta ascendente y una única puerta descendente.
- Información de contabilidad y facturación:
  - Direcciones: puerto del servidor de mantenimiento de registros primario que debería recibir los registros de eventos.
  - Direcciones: puerto del servidor de mantenimiento de registros secundario que se utilizará si el primario no está disponible.
  - Bandera que indica si los mensajes de evento deben enviarse en tiempo real al servidor de mantenimiento de registros, o bien enviarse por lotes a intervalos regulares.
  - Identificador de correlación para facturación que debe enviarse al servidor de mantenimiento de registros con cada registro de evento.
  - Información adicional de facturación (en su caso) que se utiliza para generar mensajes de eventos respuesta de llamada y desconexión de llamada.
  - Si se omite la información de generación de eventos (objeto Event-Generation-Info), NO SE PRODUCIRÁN mensajes de eventos para la puerta.

El ID de puerta TIENE QUE ser único entre todos los valores de las puertas actualmente atribuidas por el CMTS. El número de 32 bits NO DEBERÍA determinarse a partir de un conjunto de números enteros de dos bytes, ya que conocer el valor del ID de puerta es un elemento clave en la autenticación de los mensajes Commit procedentes del MTA. PUEDE utilizarse un algoritmo para asignar el identificador de puerta de la forma siguiente: la palabra de 32 bits se divide en dos partes: un índice y una parte aleatoria. La parte índice identifica la puerta por referencia a un cuadro de valores reducido, mientras que la parte aleatoria proporciona un cierto nivel de confidencialidad al valor. Sea cual sea el algoritmo utilizado, el CMTS DEBERÍA tratar de evitar en lo posible ambigüedades de GateID, evitando la reutilización de un GateID durante los tres minutos que siguen al cierre o supresión. En el caso del algoritmo aquí mencionado, la solución sería asignar cada vez el siguiente valor en la parte índice para cada GateID asignado consecutivamente y retornar a cero al alcanzar el valor máximo del entero de la parte índice.

### 7.1.4 Diagrama de transición de puerta

Las puertas pueden encontrarse en uno de los estados siguientes:

- Asignado – El estado inicial de una puerta creada a petición del controlador de puerta (GC).
- Autorizado – El GC ha autorizado el flujo con los límites de recursos definidos.

- Reservado – Se han reservado los recursos para el flujo.
- Comprometido – Los recursos se están utilizando.

El CMTS TIENE QUE soportar los estados y las transiciones de puerta de la figura 9, que se describen en esta cláusula. Todas las puertas a las que el CMTS asigna el mismo identificador TIENEN QUE realizar simultáneamente la transición a través de los estados que se muestran en la figura 9, incluso cuando sólo se permite el paso de tráfico por uno de los flujos ascendente/descendente. Para mayor claridad no se han incluido en el diagrama de transición de la figura 9 todas las transiciones a implementar. Ahora bien, todas las transiciones incluidas tienen que implementarse como se indica.

El CMTS crea una puerta mediante una instrucción asignación de puerta (Gate-Alloc) o de establecimiento de puerta (Gate-Set) emitida por el controlador de puerta (GC). En ambos casos el CMTS asigna un identificador inequívoco, denominado ID de puerta, que se devuelve al GC. Si la puerta ha sido creada mediante un mensaje de establecimiento, el CMTS TIENE QUE marcarla con el estado "Autorizado" y TIENE QUE arrancar el temporizador T1. Si la puerta ha sido creada mediante un mensaje de asignación, el CMTS TIENE QUE marcarla con el estado "Asignado", arrancar el temporizador T0 y esperar una instrucción establecimiento de puerta; al recibir esta instrucción TIENE QUE marcar la puerta con el estado "Autorizado". Si el temporizador T0 expira y la puerta está en el estado "Asignado", o el temporizador T1 expira estando la puerta en el estado "Autorizado", el CMTS TIENE QUE suprimir la puerta. El temporizador T0 establece un periodo de validez del identificador de puerta sin que se hayan especificado parámetros de puerta. El temporizador T1 establece un periodo de validez de la autorización.

En el caso de puertas en estado "Asignado", al recibir un mensaje de supresión (Gate-Delete) SE TIENE QUE suprimir la puerta y el CMTS TIENE QUE responder con un acuse de recibo (Gate-Delete-Ack) y TIENE QUE detener el temporizador T0. En el caso de puertas en estado "Autorizado", al recibir un mensaje de supresión (Gate-Delete) también SE TIENE QUE suprimir la puerta y el CMTS TIENE QUE responder con un acuse de recibo (Gate-Delete-Ack) y TIENE QUE detener el temporizador T1.

Una puerta que se encuentre en el estado "Autorizado" espera que el cliente intente reservar recursos. El cliente lo hace mediante la interfaz de servicios de control de la capa MAC. Cuando se recibe esta petición de reserva, el CMTS TIENE QUE verificar que la petición se encuentra dentro de los límites establecidos para la puerta, y lleva a cabo los procedimientos de control de admisión.

El CMTS TIENE QUE implementar al menos dos políticas de control de admisión, una para comunicaciones normales de voz y otra para comunicaciones de emergencia. Estas dos políticas TIENEN QUE tener parámetros configurables que, como mínimo, especifiquen:

1) la cantidad máxima de recursos que pueden asignarse de forma no exclusiva a sesiones de este tipo (que puede ser el 100% de la capacidad);
2) la cantidad de recursos que pueden asignarse de forma exclusiva a sesiones de este tipo (que puede ser el 0% de la capacidad); y
3) la cantidad máxima de recursos que pueden asignarse a sesiones de los dos tipos.

La política de control de admisión también PUEDE especificar si una nueva sesión de ese tipo puede "pedir prestado" a clases de prioridad inferior o bien debe interrumpir una sesión existente de algún otro tipo con el fin de satisfacer los valores que especifica la política de control de admisión.

Si la petición de reserva consiste en añadir un subflujo a un flujo de servicio existente, el ID de la clase de sesión para la puerta DEBE concordar con el ID de la clase de sesión del resto de las puertas de los subflujos que ya constituyen el flujo de servicio del caso. Si la clase de sesión de todas las puertas de los subflujos no concuerda, el CMTS DEBE rechazr la petición de reserva.

Si los procedimientos de control de admisión son positivos y sólo se ha solicitado una reserva de recursos, la puerta SE TIENE que marcar con el estado "Reservado". Si los procedimientos de

control de admisión son positivos y la solicitud es de reserva y compromiso de recursos en una sola operación, la puerta SE TIENE que marcar con el estado "Comprometido" y el CMTS TIENE QUE enviar al GC un mensaje Gate-Open y detener el temporizador T1.

Si los procedimientos de control de admisión son negativos, la puerta TIENE QUE permanecer en el estado "Autorizado".

Obsérvese que el cliente puede reservar una cantidad menor que la autorizada, por ejemplo, reservar solamente en sentido ascendente cuando se han establecido dos puertas autorizando flujos ascendente y descendente.

En el estado "Reservado" la puerta espera que el cliente comprometa los recursos (los active). La instrucción de compromiso (Commit) del cliente es una transacción de petición satisfactoria para activar un flujo de servicio a través de la interfaz de servicios de control MAC. Si la puerta aún se encuentra en el estado "Reservado" y el temporizador T1 expira (el cliente no emite la instrucción Commit), el CMTS TIENE QUE liberar los recursos reservados y suprimir la puerta. Si recibe un mensaje de supresión (Gate-Delete) cuando se encuentra en el estado "Reservado", el CMTS TIENE QUE responder con un mensaje de acuse de recibo (Gate-Delete-Ack), liberar los recursos asociados a esa puerta y detener el temporizador T1.

A los fines de este diagrama de transición de estados, la instrucción "Commit" del cliente es un mensaje que compromete el flujo ascendente. Si el CMTS recibe una petición asimétrica para autorizar el tráfico en el flujo descendente, pero no en el flujo ascendente, PERMANECERÁ en el estado "Reservado". Al contrario, si el CMTS recibe una petición asimétrica para autorizar el tráfico en el flujo ascendente, pero no en el flujo descendente, TIENE QUE tratarla como una instrucción Commit y cambiar de estado como se indica a continuación.

A efectos de este diagrama de transición de estados, el mensaje "suprimir" enviado por el cliente es un mensaje que suprime el flujo ascendente. Si el CMTS recibe una petición asimétrica, por ejemplo, que se suprime el flujo descendente pero no el ascendente, el CMTS NO DEBE cambiar de estado. Si en cambio el CMTS recibe una petición asimétrica según la cual el flujo ascendente se suprime pero no así el descendente, el CMTS DEBE considerar la petición como un mensaje "suprimir" y cambiar de estado de acuerdo con las reglas de transición de puertas.

Si el temporizador T0 expira en el CMTS antes de recibir una instrucción de establecimiento (Gate-Set) del CMS, el CMTS TIENE QUE iniciar un mensaje de cierre (Gate-Close) con el código de motivo "Expiración de temporizador T0; Ningún mensaje Gate-Set del CMS" y suprimir la puerta asociada.

Si el temporizador T1 expira en el CMTS antes de recibir una instrucción de compromiso (Commit) del MTA, el CMTS TIENE QUE liberar los recursos reservados y asociados al identificador de puerta (GateID) correspondiente, iniciar un mensaje de cierre (Gate-Close) con el código de motivo "Expiración de temporizador T1; Ningún mensaje Commit del MTA" y suprimir la puerta asociada.

Si estando el CMTS en el estado "Reservado" recibe del cliente una instrucción Commit, TIENE QUE marcar la puerta con el estado "Comprometido", detener el temporizador T1 e iniciar el mensaje de apertura (Gate-Open).

Si el temporizador T7 expira mientras que el MTA utiliza múltiples autorizaciones por intervalo y cuando aún no se ha comprometido en el CMTS ningún subflujo de un flujo de servicio correspondiente a la(s) puerta(s) indicada(s) por el identificador (GateID), el CMTS TIENE QUE iniciar un mensaje de cierre (Gate-Close) con el código de motivo "Expiración de temporizador T7; Expiración de reserva de flujo de servicio" y suprimir la(s) puerta(s) asociada(s). Si hay compromiso, el CMTS TIENE QUE establecer el mismo valor de capacidad máxima reservada y capacidad máxima comprometida para los flujos correspondientes a la(s) puerta(s) indicada(s) por el identificador asociado.

Si el temporizador T7 expira cuando el MTA no está utilizando múltiples autorizaciones por intervalo y cuando aún no se ha comprometido en el CMTS un flujo de servicio correspondiente a la(s) puerta(s) indicada(s) por el identificador (GateID), el CMTS TIENE QUE iniciar un mensaje de cierre (Gate-Close) con el código de motivo "Expiración de temporizador T7; Expiración de reserva de flujo de servicio" y suprimir la(s) puerta(s) asociada(s). Si hay compromiso, el CMTS TIENE QUE establecer el mismo valor de capacidad máxima reservada y capacidad máxima comprometida para los flujos correspondientes a la(s) puerta(s) indicada(s) por el identificador asociado.

Si el temporizador T8 expira en el CMTS por inactividad del flujo de servicio, el CMTS TIENE QUE iniciar un mensaje de cierre (Gate-Close) para cada puerta asociada con el flujo con el código de motivo "Expiración de temporizador T8; Inactividad del flujo de servicio en sentido ascendente" y suprimir la puerta asociada.

La puerta en estado "Comprometido" ya tiene una configuración estable. Se han comprometido recursos en las puertas locales y se mantendrán activados hasta que el cliente indique una instrucción liberación (Release), hasta la expiración del temporizador de actividad o hasta que el CMS emita una instrucción de supresión (Gate-Delete).

Si estando el CMTS en el estado "Comprometido" recibe del cliente una instrucción de liberación a través de la interfaz de servicios de control MAC, porque un cliente no ha renovado una reserva o debido a mecanismos internos DOCSIS que detectan un fallo de cliente, el CMTS TIENE QUE desactivar todos los recursos comprometidos para el cliente, liberar todos los recursos reservados, enviar un mensaje de cierre (Gate-Close) a la entidad de coordinación de puerta y suprimir la puerta.

Si estando el CMTS en el estado "Comprometido" recibe un mensaje de supresión (Gate-Delete), el CMTS TIENE QUE desactivar todos los recursos comprometidos para el cliente local, liberar todos los recursos reservados y suprimir la puerta. Además, el CMTS tiene que responder con un mensaje de acuse de recibo (Gate-Delete-Ack).

Mientras esté en el estado "Comprometido" el CMTS TIENE QUE permitir que el cliente inicie una modificación de la reserva o activación de recursos, dentro de los límites de la autorización y el control de admisión local.

### 7.1.5 Coordinación de puertas

Los mensajes de coordinación de puertas en la interfaz de control de puertas COPS (mensajes de apertura Gate-Open y de cierre Gate-Close) constituyen un mecanismo de información sin petición del CMTS al CMS, para mantener la sincronización de estados entre estos elementos. Es particularmente útil en el caso de una petición de reserva o compromiso prematura iniciada por el MTA, que no ha sido motivada por el CMS, y en el caso de fallo de un MTA, para iniciar la recuperación de recursos en el CMTS. En estas dos situaciones se actualizará el estado interno mantenido en el CMS para reflejar el cambio de estado en el CMTS, y esta información permitirá que el CMS tome las medidas apropiadas.

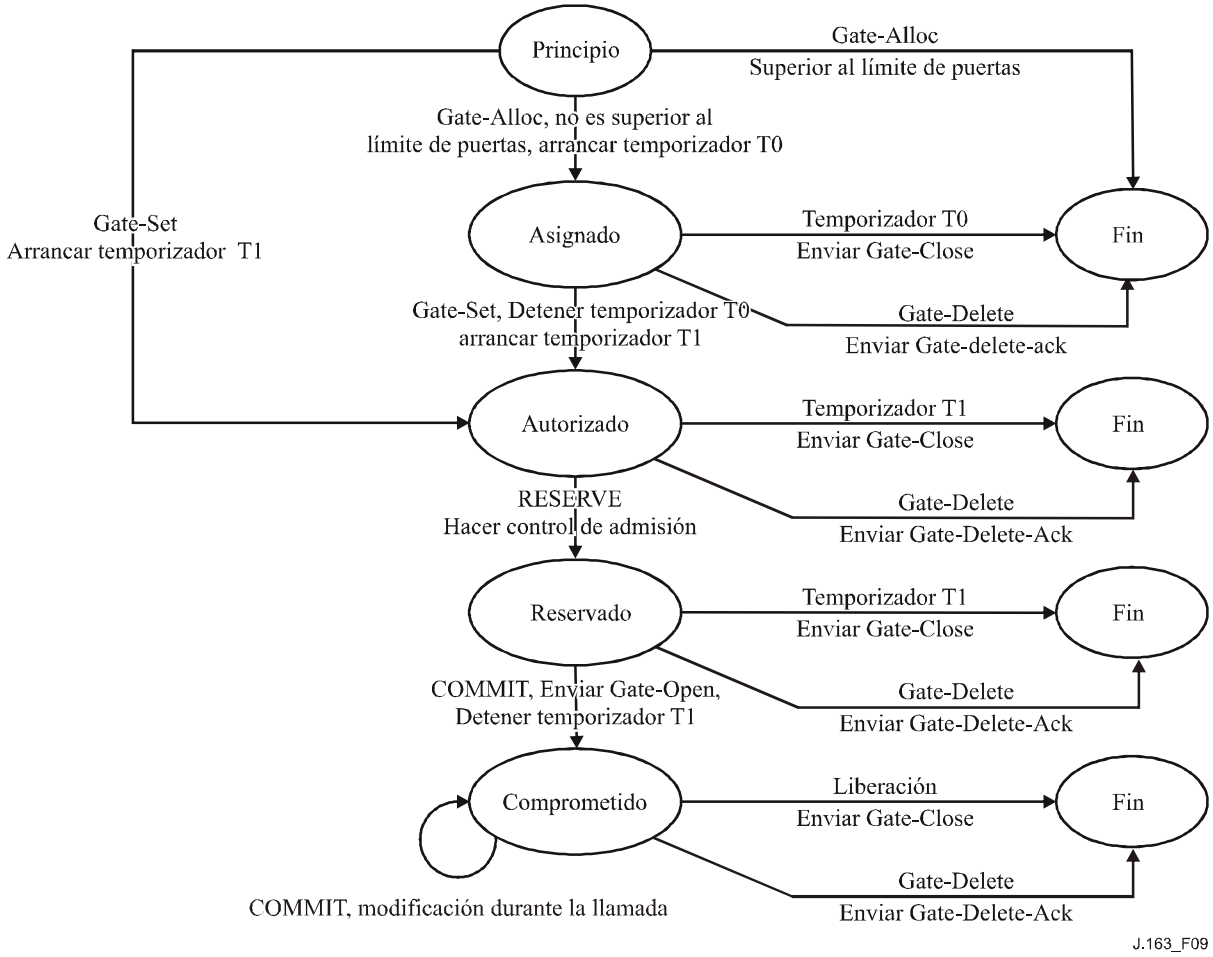



**Figura 9/J.163 – Diagrama de transición de estados de una puerta**

## 7.2 Perfil COPS para IPCablecom

El control de admisión de QoS IP consiste en la gestión de la asignación de recursos de QoS sobre la base de políticas administrativas y de la disponibilidad de recursos. El servicio de control de admisión de QoS de IPCablecom utiliza una arquitectura cliente/servidor. En la figura 10 se representan los módulos operacionales en lenguaje explícito. Las políticas administrativas se almacenan como una base de datos de políticas y están controladas por el servidor del protocolo de servicio común de política abierta (COPS). Si bien en una implementación IntServ típica de COPS es el servidor el que determina los recursos disponibles, una implementación DiffServ incluye al cliente en las políticas y le permite tomar decisiones de control de admisión.

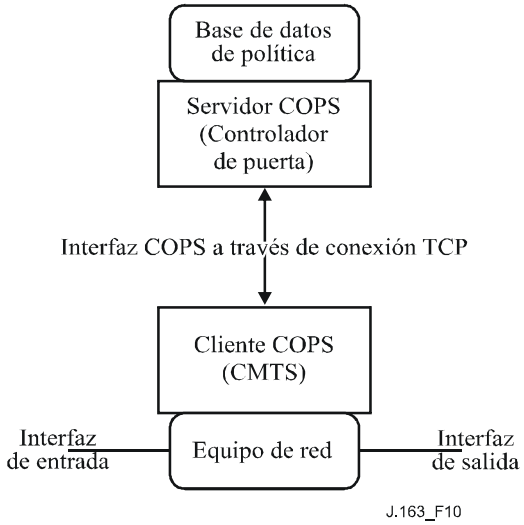



**Figura 10/J.163 – Esquema del control de admisión de QoS**

Las decisiones de control de admisión de QoS que toma el servidor COPS SE TIENEN que comunicar al cliente COPS utilizando el servidor COPS. El cliente COPS PUEDE hacer algunas peticiones de control de admisión de QoS al servidor COPS relativas a eventos de red iniciados por el protocolo de señalización de QoS o mediante mecanismos de detección del flujo de datos. La necesidad de una gestión de la anchura de banda con QoS también constituye un evento de red, por ejemplo cuando se habilita una nueva interfaz con capacidades de QoS.

Las decisiones de políticas de QoS que toma el servidor COPS PUEDEN extenderse al cliente COPS si hay una petición de servicio de QoS externa, fuera de banda, por ejemplo una petición procedente del CMTS de terminación o de un controlador de puerta. El cliente COPS PUEDE almacenar estas decisiones de políticas en un punto de decisión de política local, y el CMTS puede acceder a dicha información para tomas decisiones de control de admisión relativas a peticiones de sesión entrantes recibidas en el CMTS.

El protocolo COPS del IETF proporciona el soporte necesario para las interacciones entre cliente COPS y servidor COPS para el control de admisión con QoS. El protocolo COPS incluye las operaciones siguientes:

- Apertura de cliente (OPN, *client-open*)/Aceptación de cliente (CAT, *client-accept*)/Cierre de cliente (CC, *client-close*): el cliente COPS envía un mensaje OPN para iniciar una conexión con el servidor COPS, éste responde con un mensaje CAT para aceptar la conexión. El servidor envía un mensaje CC para terminar la conexión con el cliente.
- Petición (REQ, *request*): el cliente COPS envía un mensaje REQ al servidor para solicitar información de decisión de control de admisión o información sobre la configuración del dispositivo. Este mensaje puede contener información específica del cliente que será utilizada por el servidor, y la base de datos de políticas de admisión de la sesión, que se utilizan para tomar decisiones basadas en la política.
- Decisión (DEC): el servidor responde a los mensajes REQ devolviendo un mensaje DEC al cliente que hizo la petición original. Los mensajes DEC pueden enviarse inmediatamente en respuesta a una REQ (petición de DEC) o en cualquier instante después de modificar/actualizar una decisión anterior (DEC no solicitada).
- Información de estado (RPT, *report state*): el cliente COPS envía un mensaje RPT al servidor COPS indicando cambios del mismo cliente COPS en el estado señalado por la petición. El cliente COPS lo envía para informar al servidor COPS de los recursos que

están reservados una vez que éste ha concedido la admisión. El cliente COPS también puede utilizar RPT para informar periódicamente al servidor COPS sobre su estado.

- Supresión del estado señalado por la petición (DEL, *delete request state*): el cliente COPS envía un mensaje DEL al servidor COPS para solicitar que se elimine el estado señalado por la petición. Puede ser el resultado de una liberación de recursos de QoS por parte del cliente COPS.
- Mantener vigente (KA, *keep alive*): puede ser enviado por el cliente COPS y por el servidor COPS para la detección de fallos de comunicación.
- Petición de sincronización de estado (SSR, *synchronize state request*)/Sincronización de estado realizada (SSC, *synchronize state complete*): el servidor COPS envía un SSR solicitando información de estado del cliente COPS. El cliente vuelve a enviar peticiones al servidor para sincronizar, y después envía un mensaje SSC para indicar que se ha realizado la sincronización. Como el GC funciona sin contexto (*stateless*), las operaciones SSR/SSC no son significativas en el contexto IPCablecom y no son utilizadas por el CMTS ni por el GC.

En la arquitectura IPCablecom, el controlador de puerta es una entidad COPS punto de decisión de políticas (PDP) y el CMTS es la entidad COPS punto de imposición de políticas (PEP, *policy enforcement point*).

Los detalles del protocolo COPS figuran en RFC 2748. Este RFC 2748 describe el protocolo COPS básico con independencia del tipo de cliente. Otros proyectos de documentos proporcionan información adicional para la utilización de COPS para servicios integrados (IntServ) con RSVP y para servicios diferenciados (DiffServ) (configuración de clientes). En el apéndice X se presenta una visión general más detallada del protocolo COPS.

## 7.3 Formatos de los mensajes del protocolo de control de puerta

Los mensajes del protocolo del control de puerta se transportan en mensajes de protocolo COPS. Este protocolo utiliza una conexión TCP establecida entre el CMTS y el controlador de puerta, y utiliza los mecanismos especificados en la Rec. UIT-T J.170 para garantizar la seguridad del trayecto de comunicación.

### 7.3.1 Formato común de los mensajes COPS

Todos los mensajes COPS constan de un encabezamiento COPS seguido de un número de objetos tipificados. El GC y el CMTS TIENEN QUE soportar los mensajes COPS definidos a continuación (véase la figura 11):

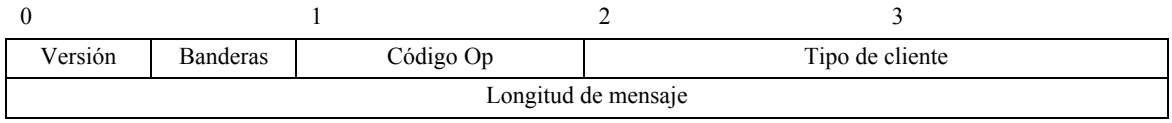



**Figura 11/J.163 – Encabezamiento común de mensajes COPS**

En el campo Versión de 4 bits se indica el número de la versión COPS vigente. SE TIENE que poner a 1.

El campo Banderas tiene 4 bits. 0x1 es la bandera de mensaje solicitado. Cuando se envía un mensaje COPS en respuesta a otro mensaje (por ejemplo, una decisión solicitada que se envía en respuesta a una petición) esta bandera SE TIENE que poner a 1. En cualquier otro caso (por ejemplo, una decisión no solicitada) NO SE PONDRÁ a 1 esta bandera (valor = 0). Todas las demás banderas deben ponerse a 0.

El campo Código-Op de 1 byte indica la operación COPS que debe realizarse. Las operaciones COPS utilizadas en esta especificación IPCablecom son las siguientes:

1 = Petición (REQ)

2 = Decisión (DEC)

3 = Información de estado (RPT)

6 = Apertura de cliente (OPN)

7 = Aceptación de cliente (CAT)

9 = Mantener vigente (KA)

El campo Tipo de cliente es un identificador de 16 bits. En los sistemas IPCablecom SE TIENE QUE especificar cliente IPCablecom (0x8008). Para mensajes Mantener vigente (KA) (Código Op = 9) el tipo de cliente SE TIENE que poner a 0, ya que KA se utiliza para la verificación de la conexión y no para la verificación de la sesión del cliente.

El campo Longitud del mensaje tiene 32 bits e indica el tamaño del mensaje en octetos. La longitud del mensaje SE TIENE QUE ajustar por tramos de 4 bytes (el valor de longitud TIENE QUE ser múltiplo de cuatro).

Al encabezamiento común COPS sigue un número variable de objetos. Todos los objetos tienen el mismo formato: una o más palabras de 32 bits con un encabezamiento de cuatro octetos de acuerdo con el formato siguiente (véase la figura 12).

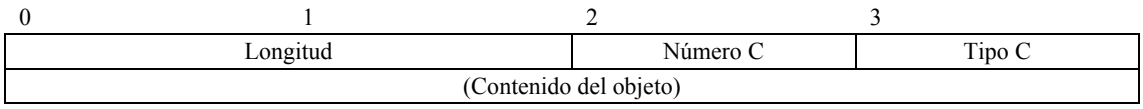



**Figura 12/J.163 – Formato común de objetos COPS**

Longitud es un valor de dos octetos que TIENE QUE indicar el número de octetos del objeto (incluido el encabezamiento). Si la longitud en octetos no es un múltiplo de cuatro, ES OBLIGATORIO rellenar al final del objeto de forma que éste quede alineado con el siguiente límite de 32 bits. En el lado de recepción, ES OBLIGATORIO que el límite del siguiente objeto coincida con la posición que se obtiene redondeando la longitud del objeto anterior hasta el límite de 32 bits.

Número C identifica la clase de información contenida en el objeto, y Tipo C identifica el subtipo o versión de la información contenida en el objeto. Los objetos COPS normalizados (definidos en RFC 2748) que se utilizan en esta Recomendación y sus valores de Número C son los siguientes:

1 = Alias

6 = Decisión

8 = Error

9 = Información específica de cliente

10 = Temporizador de mantener vigente

11 = Identificación de punto de imposición de política (PEP)

### 7.3.2 Objetos COPS adicionales para el control de puertas

Al igual que ocurre con los tipos de cliente COPS-PR y COPS-RSVP, el tipo de cliente IPCablecom define una serie de formatos de objeto. ES OBLIGATORIO colocar estos objetos dentro de un objeto Decisión, Número C = 6, Tipo C = 4 (datos de decisión específicos de cliente) cuando se transportan desde el GC al CMTS en un mensaje de decisión. También ES OBLIGATORIO

colocarlos dentro de un objeto ClientSI, Número C = 9, Tipo C = 1 (información de señalización del cliente) cuando se transportan desde un CMTS al GC en un mensaje de informe. Se codifican de forma similar a los objetos específicos de cliente para COPS-PR; véanse los detalles a continuación. Al igual que en COPS-PR, para enumerar estos objetos se utiliza un espacio de numeración específico del cliente, independiente del espacio de numeración de objetos COPS del nivel superior. Por eso se utilizan las denominaciones Número-S y Tipo-S para designar el número y el tipo de objeto respectivamente.

A continuación se describen objetos COPS adicionales que se utilizan en IPCablecom:

#### 7.3.2.1 Identificador de transacción (Transaction-ID)

El identificador de transacción contiene un testigo que el GC utiliza para comparar las respuestas del CMTS a las peticiones anteriores, y el tipo de instrucción que identifica la acción de se debe tomar o la respuesta.

| Longitud = 8 | Número S = 1 | Tipo S = 1 |
|---|---|---|
| Identificador de transacción | Tipo de instrucción de puerta | |

El identificador de transacción es una cantidad de 16 bits que el GC PUEDE utilizar para comparar respuestas e instrucciones.

El tipo de instrucción de puerta TIENE QUE ser uno de los valores siguientes:

| | |
|---|---|
| Gate-Alloc | 1 |
| Gate-Alloc-Ack | 2 |
| Gate-Alloc-Err | 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 |
| Gate-Open | 13 |
| Gate-Close | 14 |

#### 7.3.2.2 Identificador de abonado (Subscriber-ID)

Identifica al abonado para esta petición de servicio. Su utilización principal es evitar distintos ataques de denegación de servicio.

| Longitud = 8 | Número S = 2 | Tipo S = 1 |
|---|---|---|
| Dirección IPv4 (32 bits) | | |

o:

| Longitud = 20 | Número S = 2 | Tipo S = 2 |
|---|---|---|
| Dirección IPv6 (128 bits) | | |

#### 7.3.2.3 Identificador de puerta (Gate-ID)

Este objeto identifica la puerta o el conjunto de puertas a las que hace referencia el mensaje de instrucción, o que son asignadas por el CMTS para un mensaje de respuesta.

| Longitud = 8 | Número S = 3 | Tipo S = 1 |
|---|---|---|
| ID de puerta (32 bits) | | |

#### 7.3.2.4 Total de actividad (Activity-Count)

Cuando se utiliza en un mensaje Gate-Alloc, este objeto especifica el número máximo de puertas que pueden asignarse simultáneamente al ID de abonado indicado. Este objeto devuelve, en un mensaje Gate-Set-Ack o Gate-Alloc-Ack, el número de puertas asignadas a un abonado. Es útil para prevenir ataques de denegación de servicio.

| Longitud = 8 | Número S = 4 | Tipo S = 1 |
|---|---|---|
| Total (32 bits) | | |

#### 7.3.2.5 Especificación de puerta (Gate-Spec)

| Longitud = 60 | | Número S = 5 | Tipo S = 1 |
|---|---|---|---|
| Sentido | ID de protocolo | Banderas | Clase de sesión |
| Dirección IP de fuente (32 bits) | | | |
| Dirección IP de destino (32 bits) | | | |
| Puerto de fuente (16 bits) | | Puerto de destino (16 bits) | |
| Punto de código Diffserv (DSCP) | | | |
| Valor del temporizador T1 | | Reservado | |
| Valor del temporizador T7 | | Valor del temporizador T8 | |
| Velocidad contador de testigos [r] (número en coma flotante de 32 bits del IEEE) | | | |
| Tamaño del contador de testigos [b] (número en coma flotante de 32 bits del IEEE) | | | |
| Velocidad de datos máxima (p) (número en coma flotante de 32 bits del IEEE) | | | |
| Mínima unidad supervisada [m] (entero de 32 bits) | | | |
| Tamaño máximo de paquete [M] (entero de 32 bits) | | | |
| Velocidad [R] (número en coma flotante de 32 bits del IEEE) | | | |
| Término de inactividad [S] (entero de 32 bits) | | | |

El sentido puede ser 0 (puerta en sentido descendente) o 1 (puerta en sentido ascendente).

El ID de protocolo es el valor que debe aparecer en el encabezamiento IP o cero si no hay requisito de concordancia.

Las banderas se definen del modo siguiente:

0x01 Ya no se consideran las funciones de compromiso automático (Auto-Commit) y compromiso no permitido (Commit-Not-Allowed) indicadas inicialmente mediante el campo de banderas. Por tanto, los bits uno y dos quedan reservados.

Todos los bits TIENEN QUE ser cero.

La clase de sesión indica cuáles son las políticas o los parámetros de control de admisión que hay que aplicar a la puerta. Los valores posibles son:

0x00 No especificado

0x01 Sesión de VoIP de prioridad normal

0x02 Sesión de VoIP de alta prioridad (por ejemplo, E911).

Actualmente los otros valores están en reserva.

Los campos Dirección IP de fuente y Dirección IP de destino son dos direcciones IPv4 de 32 bits, o cero si no hay requisito de concordancia (en un caso de libre elección que permite la concordancia con cualquier petición del MTA).

Los campos Puerto de fuente y Puerto de destino definen dos valores de 16 bits, o cero si no hay requisito de concordancia.

Los valores r, b, p, m, M y R se describen en 6.1. En vez del término de inactividad definido en RFC RSVP, el valor S representaría la fluctuación mínima de autorización permitida (en microsegundos) en sentido ascendente, y el retardo mínimo tolerado en sentido descendente.

En otras cláusulas de esta especificación se dan requisitos normativos o limitaciones de la capacidad máxima de autorización definida por estos parámetros. Concretamente, en el texto sobre múltiples códecs de 5.6.10 se define un límite superior para esta capacidad máxima de autorización, y en la cláusula 7.5 se indican distintos condiciones mínimas para estos parámetros. Se insiste para que las implementaciones de CMS limiten hasta donde sea posible los parámetros de autorización, ya que se trata de conceptos fundamentales para la definición y la aplicación de políticas de gestión de la anchura de banda de un proveedor de servicio.

El campo DS tiene la estructura siguiente:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Punto de código de servicios diferenciados (DSCP) | | | | | | No utilizado | No utilizado |

En la RFC 2474 se define el campo servicios diferenciados como parte de una máscara de bits de dos partes, una DSCP de 6 bits y 2 bits reservados. En la RFC 3168 se definen 2 bits reservados para la notificación explícita de congestión (ECN, *explicit congestion notification*). Estes bits son utilizados por los encaminadores para notificar congestiones y activar la gestión de colas. El CMS DEBE poner a cero los bits 6 y 7 del campo DS. Si estos bits no están a cero, el CMTS DEBE responder Gate-Set con Gate-Set-Error con el código de error 8 (valor del campo DS no permitido).

Para la compatibilidad hacia atrás con las implementaciones de sistemas actuales y el uso la precedencia IP tal como se define en IETF RFC 2474 e IETF RFC 791, PUEDEN insertarse en el campo DS los bits adecuados del byte TOS de IPv4 que se muestra a continuación. Ahora bien, se aplica aun la restricción de los valores de los bits 6 y 7. Las redes DiffServ no admiten el campo TOS IP (bits 3-6).

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Precedencia IP | | | TOS IP de IPv4 | | | | No utilizado |

El temporizador T1, definido en milisegundos, se utiliza en el diagrama de transición de puertas que se describe en 7.1.4. Si un mensaje COPS contiene múltiples objetos especificación de puerta (Gate-Spec), los valores de T1 TIENEN QUE ser idénticos en todos los casos. Si hay diferencias entre los valores de T1 de objetos Gate-Spec en sentido ascendente y descendente, el CMTS TIENE QUE utilizar el T1 especificado en el Gate-Spec en sentido ascendente para la gestión de las dos puertas.

Los temporizadores T7 y T8, definidos en milisegundos, se utilizan para controlar la temporización DOCSIS de parámetros de QoS de Admisión y Actividad, respectivamente.

#### 7.3.2.6 Información de puerta distante (Remote-Gate-Info)

Este objeto ya no es válido y Num-S 6 queda en reserva para evitar confusiones.

| Longitud 36 | Número-S = 6 | Tipo-S = 1 |
|---|---|---|
| Dirección IP del CMTS (32 bits) | | |
| Puerto de CMTS (16 bits) | Banderas, abajo definidas | |
| ID de puerta distante | | |
| Algoritmo | Reservado | |
| Clave de seguridad (16 bytes) | | |

### 7.3.2.7 Información de generación de eventos (Event-Generation-Info)

Este objeto contiene toda la información necesaria para soportar los mensajes de eventos conforme a la especificación y los requisitos de la Rec. UIT-T J.164.

| Longitud = 44 | Número-S = 7 | Tipo-S = 1 |
|---|---|---|
| Dirección IP del servidor de mantenimiento de registros primario (32 bits) | | |
| Puerto del servidor de mantenimiento de registros primario | Banderas, véase abajo | Reservado |
| Dirección IP del servidor de mantenimiento de registros secundario (32 bits) | | |
| Puerto del servidor de mantenimiento de registros secundario | Reservado | |
| ID de correlación para facturación (24 bytes) | | |

La Dirección IP del servidor de mantenimiento de registros primario es la dirección del sistema de mantenimiento al que se envían los registros de eventos.

El Puerto del servidor de mantenimiento de registros primario es el número del puerto al que se envían los registros de eventos.

Los valores de las banderas son los siguientes:

0x01 Indicador de procesamiento en lotes. Si se valida el CMTS TIENE QUE acumular registros de eventos en un fichero por lotes que se envía periódicamente al servidor de mantenimiento de registros. Si no se valida el CMTS TIENE QUE enviar los registros de eventos al servidor de mantenimiento en tiempo real.

Los restantes quedan en reserva y TIENEN QUE ser cero.

La Dirección IP del servidor de mantenimiento de registros secundario es la dirección del sistema de mantenimiento secundario al que se envían los registros si el servidor de mantenimiento de registros primario no está disponible.

El Puerto del servidor de mantenimiento de registros secundario es el número del puerto al que se envían los registros de eventos.

El Identificador de correlación para facturación es el que asigna el CMS a todos los registros relacionados con esta sesión.

### 7.3.2.8 Información de eventos de conexión de medios (Media-Connection-Event-Info)

Este objeto ya no es necesario. Número S 8 queda en reserva para evitar confusiones.

### 7.3.2.9 Motivo de IPCablecom (IPCablecom-Reason)

Este objeto contiene el motivo de supresión de la puerta.

| Longitud = 8 | Número S = 13 | Tipo S = 1 |
|---|---|---|
| Código de motivo | Subcódigo de motivo | |

Valores del código de motivo definidos en esta Recomendación:

0: Operación de supresión de puerta (Gate-Delete)

1: Operación de cierre de puerta (Gate-Close)

Los subcódigos de motivo son:

Operación de supresión de puerta (Gate-Delete):

0 = Operación normal

1 = Coordinación puerta local no realizada

2 = Coordinación puerta distante no realizada

3 = Autorización denegada

4 = Apertura de puerta inesperada

5 = Cierre de puerta local no realizado

127 = Otros, error no especificado

Operación de cierre de puerta (Gate-Close):

0 = Liberación iniciada por el cliente (operación normal)

1 = Reasignación de reserva (por ejemplo, a una sesión con prioridad)

2 = No se ha mantenido la reserva (por ejemplo, mediante renovación de interfaces de servicios de control MAC)

3 = No hay respuestas DOCSIS de capa MAC (por ejemplo, mantenimiento de estación)

4 = Expiración del temporizador T0; ningún Gate-Set recibido del CMS

5 = Expiración del temporizador T1; ningún Commit recibido del MTA

6 = Expiración del temporizador T7; plazo de reserva del flujo de servicio

7 = Expiración del temporizador T8; inactividad del flujo de servicio ascendente

127 = Otros, error no especificado

#### 7.3.2.10 Error de IPCablecom (IPCablecom-Error)

Es un objeto de error específico de cliente que tiene la siguiente estructura:

| Longitud = 8 | Número S = 9 | Tipo S = 1 |
|---|---|---|
| Código de error | Subcódigo de error | |

Los valores de código de error definidos en esta Recomendación son los siguientes:

1 = No ha y puertas actualmente disponibles

2 = Identificador de puerta desconocido

3 = Valor de clase de sesión no válido

4 = Límite de puertas rebasado por el abonado

5 = Puerta ya configurada

6 = Falta un objeto necesario

7 = Objeto no válido

8 = Valor del campo DS no permitido

127 = Otro, error no especificado

El campo subcódigo de error completa la descripción del error. En el caso de los códigos de error 6 a 7, este campo de 16 bits contiene el Número S y el Tipo S (valores de 8 bits) del objeto

que falta o que se encuentra en error. Los valores Número S y Tipo S del subcódigo de error TIENEN QUE aparecer en el mismo orden del mensaje original. Si hay varias posibilidades para el Tipo S de un objeto que falta, esta porción del subcódigo de error se debería poner a 0.

#### 7.3.2.11 Parámetros de vigilancia electrónica (Electronic-Surveillance-Parameters)

El objeto parámetros de vigilancia electrónica contiene toda la información necesaria para soportar la vigilancia electrónica. Este objeto PUEDE incluirse en la instrucción Gate-Set para activar la vigilancia. El CMTS DEBE aceptar este objeto en la instrucción Gate-Set y realizar las acciones pertinentes que se describen a continuación.

| | | |
|---|---|---|
| Longitud = 24 | Número S = 10 | Tipo S = 1 |
| Dirección IP de DF para CDC (32 bits) | | |
| Puerto de DF para CDC (16 bits) | Banderas, abajo definidas | |
| Dirección IP de DF para CCC (32 bits) | | |
| Puerto de DF para CCC (16 bits) | Reservado | |
| CCCID (32 bits) | | |
| ID de correlación de facturación (24 bytes) | | |

Dirección IP de DF para CDC: dirección IP de la función de distribución (DF, *delivery function*) de vigilancia electrónica a la que se envían mensajes de eventos duplicados (conexión de datos de la llamada, *CDC, call data connection*).

Puerto de DF para CDC: el número del puerto para los mensajes de eventos duplicados.

Definición de las banderas:

0x0001 DUP-EVENT. Si se pone a uno, el CMTS TIENE QUE enviar un duplicado de todos los mensajes de eventos relacionados con esta puerta a la dirección IP de DF para CDC.

0x0002 DUP-CONTENT. Si se pone a uno, el CMTS TIENE QUE enviar un duplicado de todos los paquetes concordantes con el(los) clasificador(es) de esta puerta, a la dirección IP de DF para CCC (conexión de contenido de la llamada, *CCC, call content connection*) y al puerto DF para CCC. El formato especifico de los paquetes interceptados se describe más adelante en esta cláusula.

Los restantes están reservados y TIENEN QUE ser cero.

Dirección IP de DF para CCC: dirección de la función de distribución de supervisión electrónica a la que se envían los paquetes duplicados de contenido de la llamada.

Puerto de DF para CCC: número del puerto para duplicados de contenido de la llamada.

CCCID es un identificador para paquetes duplicados de contenido de la llamada.

El ID de correlación de facturación es el identificador asignado por el CMS para todos los registros relacionados con esta sesión. En la Rec. UIT-T J.164 se describe el formato. La inclusión del ID de correlación de facturación permite la entrega de mensajes de eventos al DF sin tener que incluir el objeto información de generación de evento (véase 7.3.2.7). El CMS DEBE garantizar que los ID de correlación de facturación son idénticos cuando se incluyen los dos objetos, parámetros de vigilancia electrónica e información de generación de evento.

Los paquetes copiados DEBEN transmitirse en la forma de un tren de datagramas UDP/IP que se envía a la dirección IP (Dirección IP de DF para CCC) y al número de puerto (puerto DF para CCC) especificados en el objeto parámetros de vigilancia electrónica. La cabida útil UDP/IP DEBE tener el formato siguiente:

**Cuadro 2/J.163 – Cabida útil de los datagramas de conexión de contenido de llamada**

| CCCID (4 bytes) |
|---|
| Información interceptada (longitud arbitraria) |
| |
| |
| |
| |

La información RTP interceptada tendrá el siguiente formato:

**Cuadro 3/J.163 – Información interceptada**

| Encabezamiento IP original (20 bytes) |
|---|
| |
| |
| |
| |
| Encabezamiento UDP original (8 bytes) |
| |
| Encabezamiento RTP original (longitud variable, 12-72 bytes) |
| |
| |
| Cabida útil original (longitud arbitraria) |
| |
| |

Obsérvese que pueden ser interceptados protocolos distintos del RTP, tales como el de retrasmisión de fax T.38.

#### 7.3.2.12 Parámetros de descripción de sesión (Session-Description-Parameters)

Este objeto ya no se utiliza. Número S 11 queda en reserva para evitar confusiones.

| Longitud = | Número S = 11 | Tipo S = 1 |
|---|---|---|
| | | |
| | | |
| | | |

### 7.3.3 Definición de mensajes de control de puerta

Los mensajes que realizan el control de puerta entre el GC y el CMTS TIENEN QUE tener las características y el formato que se indican a continuación. Los mensajes enviados del GC al CMTS son mensajes COPS de decisión, y los mensajes enviados del CMTS al GC son mensajes COPS de informe.

<Gate-Control-Cmd> := <COPS-Common-Header> <Handle>
<Context> <Decision Flags>
<ClientSI-Data>
<ClientSI-Data> := <Gate-Alloc> | <Gate-Set> | <Gate-Info>> |
<Gate-Delete>

```
<Gate-Control-Response>   ::= <COPS-Common-Header> <Handle>
                          <Report-Type> <ClientSI-Object>
<ClientSI-Object>         ::= <Gate-Alloc-Ack> | <Gate-Alloc-Err> |
                          <Gate-Set-Ack> | <Gate-Set-Err> |
                          <Gate-Info-Ack> | <Gate-Info-Err> |
                          <Gate-Delete-Ack> | <Gate-Delete-Err>
<Gate-Alloc>              := <Decision-Header> <Transaction-ID>
                                                <Subscriber-ID>[<Activity-Count>]
<Gate-Alloc-Ack>          ::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                          <Gate-ID> <Activity-Count>

<Gate-Alloc-Err>          ::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                                <IPCablecom-Error>
<Gate-Set>                ::= <Decision-Header> <Transaction-ID> <Subscriber-ID>
                          [<Activity-Count>] [<Gate-ID>]
                          [<Event-Generation-Info>]
                          [<Electronic-Surveillance-Parameters>]
                                <Gate-Spec> [<Gate-Spec>]
<Gate-Set-Ack>            ::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                          <Gate-ID> <Activity-Count>
<Gate-Set-Err>            ::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                                <IPCablecom-Error>
<Gate-Info>               := <Decision-Header> <Transaction-ID> <Gate-ID>
<Gate-Info-Ack>           := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                                <Gate-ID>
                          [<Event-Generation-Info>][<Electronic-Surveillance-Parameters>]
                                [<Gate-Spec>] [<Gate-Spec>]
<Gate-Info-Err>           ::= <ClientSI-Header> <Transaction-ID> <Gate-ID>
                                <IPCablecom-Err>
<Gate-Delete>             ::= <Decision-Header> <Transaction-ID> <Gate-ID> <IPCablecom
                                reason>
<Gate-Delete-Ack>         := <ClientSI-Header> <Transaction-ID> <Gate-ID>
<Gate-Delete-Err>         := <ClientSI-Header> <Transaction-ID> <Gate-ID>
                                <IPCablecom-Err>

<Gate-Open>               :: = <ClientSI-Header> <TransactionID> <GateID>

<Gate-Close>              :: = <ClientSI-Header> <TransactionID> <GateID>
                          <IPCablecom-Reason>
```

El objeto contexto (NUM-C = 2, TIPO-C = 1) del mensaje de decisión COPS tiene el valor de Tipo-R (bandera de tipo petición) puesto a 0x08 (petición de configuración) y el valor de Tipo-M puesto a cero. El campo código de instrucción del objeto obligatorio banderas de decisión (NUM-C = 6, TIPO-C = 1) se pone a 1 (instalar configuración). Otros valores hacen que el CMTS genere un mensaje informe que indica fallo. El objeto de tipo informe (NUM-C = 12, TIPO-C = 1) incluido en el mensaje informe COPS tiene el campo de tipo informe puesto a 1 (positivo) o 2 (negativo) dependiendo del resultado de la instrucción de control de puerta. En todos los mensajes informe que incluyen la respuesta del control de puerta se debería poner a uno el bit de la bandera del mensaje solicitado en el encabezamiento COPS. En todos los mensajes decisión (DEC), excepto el primero, se debería poner a uno el bit de la bandera del mensaje solicitado en el encabezamiento COPS. En el primer mensaje decisión enviado por el CMS al CMTS se debería validar la bandera solicita. Los valores de esta bandera deben ser conformes a la especificación COPS. No deberían afectar los procesos del protocolo de control de puertas.

Si un objeto recibido en un mensaje de control de puertas contiene un Número-S o un Tipo-S no reconocidos, NO SE TENDRÁ EN CUENTA. La presencia de un objeto de estas características en un mensaje de control de puertas NO SERÁ CONSIDERADA como un error, ya que se descarta y el mensaje contiene todos los objetos necesarios.

## 7.4 Procesos del protocolo de control de puerta

### 7.4.1 Secuencia de inicialización

Al arrancar, el CMTS (es decir, el punto de imposición de políticas, PEP-COPS) TIENE QUE buscar conexiones COPS entrantes en el número de puerto TCP 2126 (asignado por IANA). Cualquier controlador de puerta que necesite contactar al CMTS TIENE QUE establecer una conexión TCP con él a través de dicho puerto. Es previsible que varios controladores de puerta establezcan conexiones COPS con un único CMTS. Una vez establecida la conexión TCP entre el CMTS y el GC, el CMTS envía información sobre sí mismo al GC mediante un mensaje CLIENT-OPEN. Esta información incluye el identificador del CMTS (CMTS-ID) configurado en el objeto Identificación del PEP (PEPID, *PEP identification*). El CMTS DEBERÍA omitir el objeto última dirección del PDP (LastPDPAddr) en el mensaje CLIENT-OPEN.

En su respuesta, el controlador de acceso envía un mensaje CLIENT-ACCEPT. Este mensaje incluye el objeto Temporizador de vigencia (Keep-Alive-Timer) que comunica al CMTS el intervalo máximo entre mensajes Mantener vigente.

El CMTS envía entonces un mensaje REQUEST que incluye los objetos Alias y Contexto. El objeto Contexto (NUM-C = 2, TIPO-C = 1) PUEDE tener el valor TIPO-R (bandera de tipo petición) puesta a 0x08 (petición de configuración) y el Tipo M puesto a cero. El objeto Alias contiene un número que elige el CMTS. El único requisito es que ESTÁ PROHIBIDO que el CMTS utilice el mismo número para dos mensajes de petición (request) distintos en la misma conexión COPS; en el entorno IPCablecom el alias no tiene otro significado en el protocolo. Con ello se completa la secuencia de inicialización, que se muestra en la figura 13.

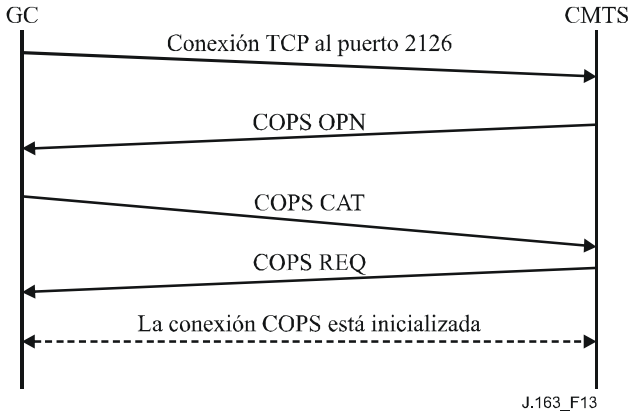



**Figura 13/J.163 – Establecimiento de conexión COPS**

El CMTS TIENE QUE enviar periódicamente al GC un mensaje COPS KEEP-ALIVE (KA). Cuando recibe el mensaje COPS KA, el CMS TIENE QUE devolver al CMTS el mensaje COPS KA. Esta transacción, representada en la figura 14, está documentada en detalle en IETF RFC 2748. ES OBLIGATORIO hacerlo, como mínimo, con la frecuencia que especifica el objeto temporizador de mensajes mantener vigente, que se devuelve en el mensaje CLIENT-ACCEPT. El mensaje KEEP-ALIVE se envía con el tipo de cliente puesto a cero.

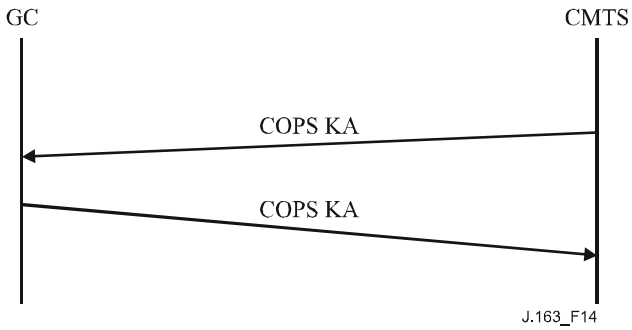



**Figura 14/J.163 – Intercambio del mensaje COPS mantener vigente (KA)**

### 7.4.2 Desarrollo del proceso

El protocolo entre el controlador de puerta y el CMTS tiene por objeto la política de control y de asignación de recursos. El controlador de puerta implementa todas las políticas de asignación y utiliza dicha información para gestionar el conjunto de puertas implementadas en el CMTS. El controlador de puerta inicializa las puertas con una fuente, un destino y restricciones de anchura de banda específicas; una vez inicializadas, el MTA puede solicitar asignaciones de recursos dentro de los límites impuestos por el controlador de puerta.

Los mensajes que inicia el controlador de puerta son Gate-Alloc, Gate-Set, Gate-Info y Gate-Delete. Los mensajes que inicia el CMTS son Gate-Open y Gate-Close. En las cláusulas siguientes se describen los procedimientos para dichos mensajes.

Los mensajes que inicia el controlador de puerta se envían utilizando objetos específicos del cliente dentro del objeto de decisión de mensajes COPS DECISIÓN. Las respuestas del CMTS a estos mensajes que inicia el controlador de puerta se envían como mensajes REPORT-STATE con objetos específicos del cliente en el objeto ClientSI. En el caso de mensajes de acuse de recibo (ACK), el valor COPS Tipo-Informe TIENE QUE ser 1, y en el caso de mensajes de ERROR (ERR) TIENE QUE ser 2. Los mensajes Gate-Open y Gate-Close SE TIENEN QUE enviar como mensajes REPORT-STATE no solicitados, con el identificador de transacción cero, con objetos específicos del cliente en el objeto ClientSI, utilizando el valor Tipo-Informe 3, destinados al CMS a través de la conexión TCP que creó inicialmente la puerta. Si esa conexión TCP ya no fuera válida, el CMTS TIENE QUE descartar los mensajes del GC sin otra forma de acción.

Los mensajes DECISIÓN y REPORT-STATE TIENEN QUE contener el mismo alias utilizado en el mensaje REQUEST inicial enviado por el CMTS cuando se inició la conexión COPS.

Gate-Alloc valida el número de sesiones simultáneas que se pueden establecer desde el MTA de origen y asigna un ID de puerta que debe utilizarse para todos los futuros mensajes relativos a esta puerta o conjunto de puertas.

Gate-Set inicializa y modifica todos los parámetros de políticas y de tráfico para la puerta o conjunto de puertas, y establece la información de facturación y coordinación de puertas.

Gate-Info es un mecanismo que el controlador de puerta utiliza para determinar cuál es el estado actual y los valores de parámetros de una puerta o conjunto de puertas existentes.

El CMTS TIENE QUE enviar periódicamente al GC un mensaje Mantener vigente (KA) para facilitar la detección de fallos de conexión TCP. El controlador de puerta registra cuándo se reciben los mensajes KA. Si el controlador de puerta no ha recibido del CMTS un KA en los plazos especificados en IETF RFC 2748, o bien si el controlador de puerta no ha recibido una indicación de error de la conexión TCP, TIENE QUE deshacer la conexión TCP e intentar restablecerla antes de que se produzca la siguiente solicitud de asignación de puerta de ese CMTS.

Gate-Delete permite en ciertas circunstancias (véanse las cláusulas siguientes) que un controlador de puerta suprima una puerta recién asignada.

El CMTS utiliza Gate-Open para informar al controlador de puerta que se han comprometido los recursos de la puerta. Gate-Open y el mensaje Gate-Close descrito a continuación constituyen un mecanismo de información del CMTS al CMS, que permite una gestión detallada de estados de la llamada en el CMS.

Gate-Close permite al CMTS informar al GC de que la puerta se ha suprimido por interacción o inactividad del MTA.

### 7.4.3 Procedimientos para la asignación de una nueva puerta

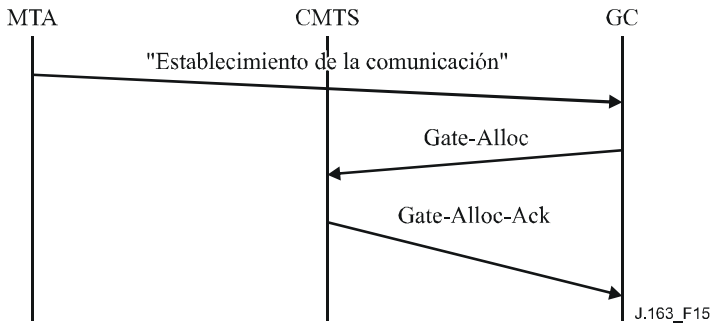
El controlador de puerta envía al CMTS un mensaje Gate-Alloc cuando el MTA de origen envía el mensaje "establecimiento de la comunicación" ("Call_Set-up"). Véase la figura 14.

La utilización de Gate-Alloc garantiza que no se solicitan simultáneamente demasiadas sesiones desde un MTA. Este mecanismo puede utilizarse para controlar un ataque de denegación de servicio procedente del MTA. En su respuesta al mensaje Gate-Alloc, el CMTS compara el número de puertas actualmente asignadas para el ID de abonado indicado, con el valor del campo Total en el objeto Total de actividad del mensaje Gate-Alloc. Si el número actual de puertas es igual al valor del campo Total de Gate-Alloc o mayor, el CMTS TIENE QUE devolver un mensaje Gate-Alloc-Err. En el primer caso (número de puertas superior al valor del campo Total de Gate-Alloc) probablemente se ha reconfigurado el abonado y su límite de puertas es inferior. Entonces las sesiones actuales del abonado no se ven afectadas, pero el CMTS rechazará cualquier nueva sesión de dicho abonado hasta que el total de sesiones del abonado sea inferior al valor especificado en el campo Total.

La determinación del valor efectivo del campo Total depende de criterios de funcionamiento. Ha de ser suficientemente alto (en cada MTA) para evitar el tratamiento negativo de situaciones de llamada legítimas, y suficientemente bajo para prevenir ataques de denegación de servicio.

Si el objeto Total de actividad no está presente, el CMTS no realiza la verificación de límite de puertas. Para reducir el tiempo de establecimiento de la comunicación, el GC PUEDE realizar la verificación de límite de puertas al recibir Gate-Alloc-Ack, en lugar de que sea el CMTS quien realice la verificación. Así el GC puede realizar simultáneamente las opciones de asignación de puerta (Gate-Alloc) y de análisis de políticas del abonado. Cuando los resultados de ambas operaciones están disponibles, el GC puede realizar la verificación del límite de puertas. Si la verificación tiene resultado negativo, el GC DEBERÍA enviar al CMTS un mensaje Gate-Delete para suprimir la puerta que fue asignada incorrectamente (véase 7.4.8). El GC PUEDE incluir el objeto Total de actividad en los siguientes mensajes Gate-Alloc para dicho abonado una vez que la política se ha almacenado en una memoria intermedia.

El diagrama siguiente (véase la figura 15) es un ejemplo de la señalización Gate-Alloc.




NOTA – Este ejemplo de mensaje "Establecimiento de la comunicación" se refiere al mensaje "Invite sin señal de llamada" con la señalización DCS.

**Figura 15/J.163 – Ejemplo de señalización de asignación de puerta (Gate-Alloc)**

El CMTS TIENE QUE responder al mensaje Gate-Alloc con un Gate-Alloc-Ack (resultado positivo) o Gate-Alloc-Err (resultado negativo). TIENE QUE existir concordancia entre los ID de transacción de la respuesta y la petición.

En una respuesta Gate-Alloc-Err se informa de todos los errores de asignación de puertas. El objeto IPCablecomError contiene una los siguientes códigos de error:

1 = No hay puertas disponibles en este momento

4 = El abonado ha rebasado el límite de puertas

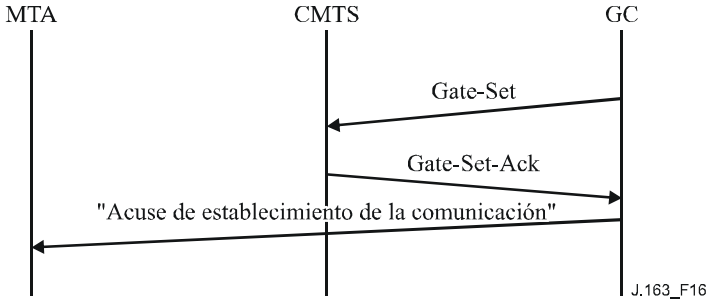
6 = Falta un objeto necesario

7 = Objeto no válido

127 = Otros, error no especificado

### 7.4.4 Procedimientos para la autorización de recursos a través de una puerta

El controlador de puerta envía al CMTS el mensaje Gate-Set para inicializar o modificar los parámetros operacionales de la puerta o puertas. La figura 16 es un ejemplo de la señalización Gate-Set.




NOTA – Este ejemplo de mensaje "Acuse de establecimiento de la comunicación" se refiere al mensaje "200 OK" que es la respuesta al mensaje "Invite sin señal de llamada" con la señalización DCS.

**Figura 16/J.163 – Ejemplo de señalización de establecimiento de puerta (Gate-Set)**

Si el mensaje Gate-Set contiene un objeto ID de puerta, se trata de una petición de modificación de una puerta existente. Si el mensaje Gate-Set no contiene este objeto ID, se trata de una petición para

asignar una nueva puerta, y SE PUEDE incluir el objeto Total de actividad para que el CMTS determine si el abonado ha superado el numero máximo de puertas simultáneas (véase 7.4.3).

El mensaje Gate-Set TIENE QUE contener exactamente uno o dos objetos especificación de puerta que pueden describir una puerta ascendente o ninguna, y una puerta descendente o ninguna.

El CMTS TIENE QUE responder a un mensaje Gate-Set con Gate-Set-Ack (resultado positivo) o Gate-Set-Err (resultado negativo). El ID de transacción de la respuesta TIENE QUE concordar con el ID de transacción de la petición.

En la respuesta Gate-Set-Err se informa de los errores en la asignación o autorización de puertas. El objeto Error de IPCablecom contiene uno de los códigos de error siguientes:

1 = No hay puertas disponibles en este momento

2 = ID de puerta desconocido

3 = Valor de clase de sesión no válido

4 = El abonado ha rebasado el límite de puertas

5 = Ya se estableció la puerta

6 = Falta un objeto necesario

7 = Objeto no válido

127 = Otros, error no especificado

En el tratamiento de una petición de reserva de un MTA, el CMTS TIENE QUE determinar la puerta adecuada, utilizando el TLV bloque de autorización. El CMTS TIENE QUE verificar que la petición de reserva se encuentra dentro de los límites autorizados especificados para la puerta.

El CMTS actualiza la petición de reserva por referencia a los parámetros de puerta. Si el conjunto de parámetros de QoS está admitido (2), el CMTS TIENE QUE asignar los parámetros de QoS admitidos al termporizador T7. El CMTS TIENE QUE registrar el valor del punto de código DiffServ o del Tipo de servicio (TOS) del objeto Gate-Spec en reemplazo del octeto Tipo de servicio IP, antes de transmitir los paquetes.

El CMTS TIENE QUE realizar una función de control de admisión por referencia a los parámetros de políticas configurados y al valor Clase de sesión de la puerta.

En lugar del mensaje Gate-Alloc se puede utilizar un mensaje Gate-Set para asignar (y establecer) una puerta. Entonces es posible que el número del puerto utilizado por la puerta distante para recibir mensajes de coordinación de puertas no esté disponible para el controlador de puerta. Si es así, el campo Puerto CMTS del objeto información de puerta distante (incluido en el mensaje Gate-Set) se pone a cero. Ello hace que el CMTS no tenga en cuenta el número del puerto para la coordinación de puertas. Sin embargo, cuando el controlador de puerta conoce (posteriormente) el número del puerto utilizado por la puerta distante, tiene que enviar otro mensaje Gate-Set (con el número del puerto en el objeto Remote-Gate-Info) para informar al CMTS sobre dicho puerto.

El principio del mensaje Gate-Set es utilizar los valores de parámetros más recientes para el control de admisión cuando se modifica el estado de una puerta de Autorizado a Reservado. Habiendo reservado los recursos, el MTA está seguro de que todas las peticiones de compromiso dentro de los límites de capacidad reservada serán aceptadas. Después (puerta en estado Reservado o Comprometido), la puerta TIENE QUE permanecer estática. El CMTS DEBE rechazar todo mensaje Gate-Set recibido para una puerta que esté reservada o comprometida. Si eventos externos (cambio de códec, de puerto RTP, de dirección IP, etc.) hacen que los parámetros de la puerta ya no sean suficientes para transportar un tren de medios previsto, el controlador de puerta TIENE QUE tratar de crear otra puerta adaptada al nuevo tren de medios.

### 7.4.5 Procedimientos para la interrogación de una puerta

Para conocer los valores de los parámetros de una puerta, el controlador de puerta envía al CMTS un mensaje Gate-Info. El CMTS TIENE QUE responder al mensaje Gate-Info con un Gate-Info-Ack (resultado positivo) o Gate-Info-Err (resultado negativo). El ID de transacción de la respuesta TIENE QUE concordar con el ID de transacción de la petición. ES OBLIGATORIO incluir los objetos GateSpec en la respuesta Gate-Info-Ack, si antes se habían comunicado al CMTS asociados a esa puerta.

En la respuesta Gate-Info-Err se informa de los errores en la interrogación de puertas. El objeto Error contiene uno de los códigos de error siguientes:

2 = ID de puerta desconocido

127 = Otros, error no especificado

### 7.4.6 Procedimientos para comprometer una puerta

Cuando el MTA realiza satisfactoriamente la operación Commit inicial para una puerta (procedimiento descrito en 6.2.1 para un MTA integrado), el CMTS TIENE QUE enviar un mensaje Apertura de puerta (Gate-Open).

### 7.4.7 Procedimientos para el cierre de una puerta

El CMTS TIENE QUE liberar todos los recursos asociados a la puerta, suprimir la puerta, suprimir los flujos de servicio asociados mediante un mensaje DOCSIS DSD y enviar un mensaje Gate-Close al recibir un mensaje explícito de liberación del cliente MTA (procedimiento descrito en 6.3.3 para MTA integrados), o al detectar que el cliente ya no está generando paquetes de forma activa ni mensajes de renovación del flujo asociado a la puerta.

### 7.4.8 Procedimientos para la supresión de una puerta

En un flujo de llamada normal, el CMTS suprime una puerta cuando recibe un mensaje DSD_REQ. El CMTS también suprime una puerta cuando recibe un mensaje Gate-Close.

Si las puertas en los sentidos ascendente y descendente están reservadas o comprometidas, el CMTS debe cumplir las siguientes reglas:

– Para una DSD-REQ iniciada por un E-MTA que incluye identificadores de flujo de servicio ascendente y descendente asociadas con una puerta válida, el CMTS tiene que suprimir los flujos de servicio en ambos sentidos, y liberar todos los recursos vinculados con la puerta.

– Para una DSD-REQ iniciada por un E-MTA que sólo incluye un identificador de flujo de servicio válido en sentido ascendente y ningun identificador para el sentido descendente asociado con una puerta válida, el CMTS DEBE suprimir los flujos de servicio en ambos sentidos. El CMTS debe enviar una DSD-REQ para el flujo de servicio descendente asociado con el E-MTA y liberar todos los recursos vinculados con la puerta.

– Para una DSD-REQ iniciada por un E-MTA que sólo incluye un identificador de flujo de servicio válido en sentido desscendente y ningun identificador para el sentido ascendente asociado con una puerta válida, el CMTS DEBE suprimir solamente el flujo de servicio en sentido descendente. El CMTS debe esperar que expire el correspondiente temporizador T8 en sentido ascendente, si está funcionando o para una DSD-REQ del flujo de servicio ascendente, o esperar antes de liberar todos los recursos vinculados con la puerta.

Normalmente un controlador de puerta no inicia una operación de supresión de puerta, pero en algunas situaciones excepcionales puede ser conveniente que un controlador de puerta suprima una puerta del CMTS. Por ejemplo, si el controlador de puerta es informado (por una respuesta Gate-Alloc-Ack) que un abonado ha rebasado su límite de puertas, puede ser conveniente suprimir la puerta recién asignada en el CMTS. En tal caso, DEBERÍA enviar al CMTS un mensaje

Gate-Delete (sin esperar a que expire la temporización de puerta). La funcionalidad de supresión puede ser útil en otras situaciones.

El CMTS TIENE QUE responder a un mensaje Gate-Delete con un Gate-Delete-Ack (resultado positivo) o Gate-Delete-Err (resultado negativo). El ID de transacción de la respuesta TIENE QUE concordar con el ID de transacción de la petición. En la respuesta Gate-Delete-Err se informa de los errores producidos en la supresión de puertas. El objeto Error incluye uno de los siguientes códigos de error:

2 = ID de puerta desconocido

127 = Otros, error no especificado

### 7.4.9 Secuencia de terminación

Cuando un CMTS cierra su conexión TCP con el GC, PUEDE enviar en primer lugar un mensaje DELETE-REQUEST-STATE (incluyendo el objeto alias utilizado en el mensaje REQUEST). El CMTS PUEDE enviar a continuación un mensaje CLIENT-CLOSE. Estos mensajes son opcionales porque el GC es un sistema sin contexto y porque el protocolo COPS requiere que el servidor COPS suprima automáticamente cualquier estado asociado con el CMTS al cerrar la conexión TCP.

Cuando el controlador de puerta va a hacer el cierre, DEBERÍA enviar al CMTS un mensaje COPS Cierre del cliente (*client-close*) (CC). En el mensaje COPS CC, el controlador de puerta NO DEBERÍA enviar el objeto Dirección de redireccionamiento PDP <PDPRedirAddr>. Si un CMTS recibe un mensaje COPS CC del controlador de puerta con un objeto <PDPRedirAddr> NO TENDRÁ EN CUENTA este objeto al procesar el mensaje.

### 7.4.10 Situaciones de fallo

Cuando un CMTS detecta la pérdida de conexión TCP o COPS con el GC, por ejemplo, en caso de fallo catastrófico del GC, TIENE QUE mantener todas las puertas establecidas. Un método de mantener el estado de la conexión TCP o COPS es utilizar mensajes de mantenimiento de actividad COPS. En este caso, si el CMTS no recibe una respuesta de mantenimiento de actividad procedente del CMS dentro del intervalo de tiempo de mantenimiento de actividad, el CMTS considerará perdida la conexión COPS y comenzará a leer el puerto 2126 para reinicializar el zócalo TCP.

Las puertas comprometidas seguirán estando comprometidas, y otras puertas conservarán el estado en que se encuentren hasta que se modifique de forma activa o expiren los temporizadores pertinentes. El mantenimiento de las puertas en caso de fallos GC/CMS permite preservar flujos críticos como una llamada de emergencia.

## 7.5 Utilización del protocolo de puertas en el CMS

El CMS TIENE QUE garantizar que es posible acomodar todos los códecs acordados durante la negociación en la capacidad máxima de recursos solicitada al CMTS en mensajes de puertas. El CMS TIENE QUE utilizar el algoritmo LUB descrito en 6.1.1 para determinar los valores b, r, p, m y M.

El CMS DEBERÍA comprobar si el mensaje de control de puerta enviado al CMTS contiene las direcciones y los puertos de punto extremo apropiados, para referenciar estos puntos extremo y evitar el robo del servicio.

El CMS TIENE QUE establecer un Término de inactividad de 800 µs en sentido ascendente cuando no comunica ningún parámetro de fluctuación de autorización en sentido ascendente al MTA. Si lo comunica, el valor utilizado en la puerta debería ser inferior o igual al valor enviado al MTA para el parámetro DOCSIS de fluctuación de autorización tolerada. En sentido descendente el CMS TIENE QUE utilizar el valor cero.

## 7.6 Coordinación de puertas

El controlador de puerta (GC) registra el estado de cada puerta y crea una puerta en el CMTS mediante los mensajes Asignación (Gate-Alloc) o Establecimiento (Gate-Set). El controlador de puerta puede suprimir una puerta mediante la instrucción Supresión (Gate-Delete) y solicitar al CMTS información asociada a una determinada puerta mediante el mensaje Información (Gate-Info). El CMTS informa al GC las modificaciones de estado originadas por mensajes del MTA o por inactividad, mediante mensajes Apertura (Gate-Open) y Cierre (Gate-Close).

El CMTS genera el mensaje Gate-Open, que inicia la llamada, cuando el MTA compromete recursos de QoS. El mensaje Gate-Close indica el cierre de la puerta en el CMTS y la liberación de los recursos de QoS asociados. Gate-Open y Gate-Close son mensajes informativos relativos a cambios de estado en el CMTS para una determinada puerta, y no requieren información de retorno del CMS.

Es obligatorio sincronizar los eventos Gate-Open y Gate-Close en los puntos extremo local y distante para evitar posibles situaciones de robo de servicio. Se sincronizan con una lógica interna del CMS o mediante una señalización CMS-a-CMS en el caso de múltiples CMS.

### 7.6.1 Conexión de una llamada

Para conectar satisfactoriamente una llamada normal son necesarios tres eventos que se suceden rápidamente:

- El CMS solicita el compromiso de recursos al MTA local.
- El CMTS indica que el MTA local ha comprometido los recursos.
- Coordinación en el plano de señalización del compromiso de recursos local y distante.

Véase la figura 17.

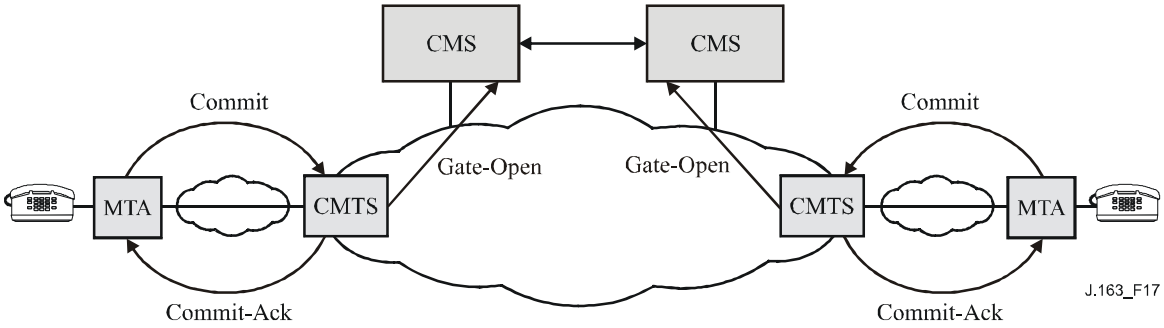



**Figura 17/J.163 – Coordinación de la conexión de llamada**

Si un CMS recibe un mensaje Gate-Open para una puerta a la que no se han comprometido recursos, TIENE QUE suprimirla y comunicar el código de motivo 'Gate-Open no previsto'.

### 7.6.2 Terminación de una llamada

Para terminar una llamada, como en el caso de la conexión, son necesarios tres eventos que se suceden rápidamente:

- El CMS solicita la liberación de recursos al MTA local.
- El CMTS indica que el MTA local ha liberado los recursos.
- Coordinación en el plano de señalización de la liberación de recursos local y distante.

Véase la figura 18.

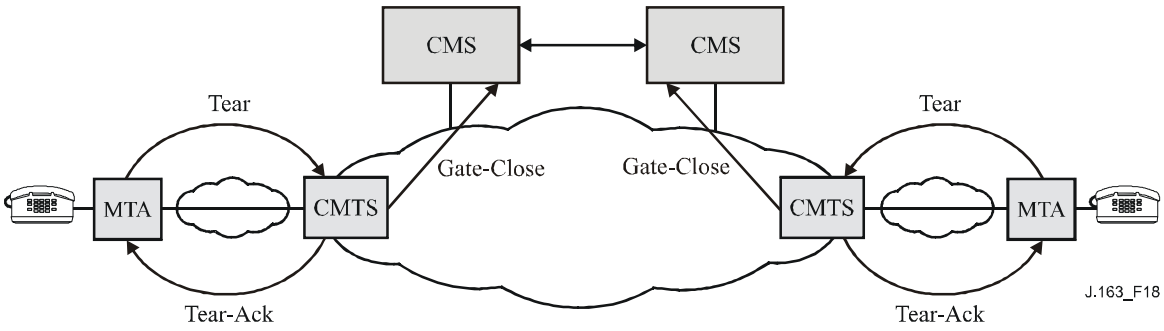



**Figura 18/J.163 – Coordinación de la terminación de llamada**

Cuando envía al MTA un mensaje para suprimir la conexión, el CMS TIENE QUE iniciar un temporizador para un periodo T5. Si al expirar este plazo el CMTS no ha comunicado el cierre de la puerta, el CMS TIENE QUE generar una instrucción Gate-Delete para suprimirla en el CMTS y señalar el código de motivo 'Cierre local de puerta no realizado'.

Cuando el CMS recibe un mensaje Gate-Close, tiene que actualizar el estado interno reflejando el cierre de la puerta en el CMTS.

# Anexo A

## Definición y valores de los temporizadores

En esta Recomendación se hace referencia a varios temporizadores. En este anexo figura una lista de temporizadores y sus valores recomendados.

**Temporizador T0**

Este temporizador se implementa en la máquina de estados de puertas del CMTS y limita el tiempo que una puerta puede estar asignada sin que se fijen sus parámetros. Ello permite al CMTS recuperar los recursos del ID de puerta cuando el sistema de gestión de llamada no consigue completar la secuencia de señalización para una nueva sesión.

Este temporizador arranca cuando se asigna la puerta.

Se pone a cero nuevamente cuando se fijan los parámetros de la puerta.

Al expirar este temporizador, el CMTS TIENE QUE considerar que el ID de puerta asignado ya no es válido.

El valor RECOMENDADO de este temporizador es 30 segundos.

**Temporizador T1**

Este temporizador se implementa en la máquina de estados de puertas del CMTS y limita el tiempo que puede transcurrir entre la autorización y la realización del compromiso.

Este temporizador se arranca cada vez que se establece una puerta.

Se pone a cero nuevamente cuando la puerta pasa al estado COMPROMETIDO.

Al expirar este temporizador, el CMTS TIENE QUE liberar todos los recursos reservados en el CMTS para esta puerta, revocar las reservas que hubiera hecho el MTA y autorizadas por esta puerta, enviando al CM un mensaje DSC o DSD para liberar los recursos que había reservado, e iniciar un mensaje Gate-Close para la puerta.

ES OBLIGATORIO definir el temporizador T1 con el valor indicado en el mensaje Gate-Set. Si el valor del mensaje Gate-Set es cero, ES OBLIGATORIO definir el temporizador T1 con un valor por defecto configurable. El valor por defecto RECOMENDADO es de 200-300 segundos.

Si el valor del temporizador T1 es 0 en Gate-Set, el CMTS TIENE QUE devolver el valor de T1 configurado en el CMTS o cero en el objeto GateSpec del mensaje Gate-Info-Ack. En este caso es preferible el valor configurado para T1.

**Temporizador T2**

Este temporizador ya no se utiliza.

**Temporizador T3**

Este temporizador ya no se utiliza.

**Temporizador T4**

Este temporizador ya no se utiliza.

**Temporizador T5**

Este temporizador se implementa en el CMS y controla la sincronización entre la liberación de recursos en el MTA local y la verificación de cierre de la puerta local en el CMTS.

Cuando el CMS envía al MTA un mensaje para suprimir la conexión, el CMS TIENE QUE cerrar la puerta en el CMTS en el plazo de T5. Se pone a cero nuevamente cuando el CMS recibe el mensaje Gate-Close que confirma el cierre de la puerta local.

Al expirar este temporizador el CMS suprime la puerta en el CMTS, enviando el mensaje Gate-Delete con el código de motivo 'Cierre de puerta local no realizado'.

El valor RECOMENDADO de este temporizador es 5 segundos.

**Temporizador T6**

Este temporizador ya no se utiliza.

**Temporizador T7**

El CMTS TIENE QUE fijar a la temporización para los parámetros de QoS admitidos para el flujo de servicio el valor especificado de este temporizador. En el caso de que un flujo con múltiples subflujos, la temporización para parámetros de QoS en estado Admitido para dicho flujo se pone al valor del temporizador T7 especificado en el último mensaje Gate-Set recibido para cualquier subflujo del flujo. Es el tiempo durante el cual es obligatorio retener los recursos en el CMTS para un conjunto de parámetros de QoS de estado Admitido para un flujo de servicio, mientras hay otro conjunto de parámetros de QoS de estado Activo. Otras explicaciones sobre la utilización de los parámetros de QoS Plazo de estado Admitido en el anexo C al anexo B/J.112.

Para que el E-MTA pueda renovar este temporizador, el CMTS TIENE QUE comunicar al E-MTA los parámetros de QoS Plazo de estado Admitido, en la respuesta a su petición de reserva (DSA-RSP).

El valor RECOMENDADO de este temporizador es 200 segundos.

**Temporizador T8**

El CMTS TIENE QUE fijar la temporización para los parámetros de QoS activos para el flujo de servicio el valor especificado para este temporizador. En el caso de in flujo con múltiples subflujos, la temporización del flujo para parámetros de QoS en Activo se pone al valor del temporizador T8 especificado en el último mensaje Gate-Set recibido para cualquier subflujo del flujo. Es el tiempo durante el cual pueden permanecer no utilizados los recursos en un flujo de servicio activo. Otras explicaciones sobre la utilización de los parámetros de QoS Plazo de estado Activo en el anexo C al anexo B/J.112.

Para que el E-MTA pueda renovar este temporizador, el CMTS TIENE QUE comunicar al E-MTA los parámetros de QoS Plazo de estado Activo, en la respuesta a su petición de reserva (DSA-RSP).

El valor por defecto de este temporizador es 0, que significa que el CMTS no debe sondear si hay actividad en el flujo de servicio.

## Apéndices I a VIII y XI

Ningún texto.

# Apéndice IX

# Casos de robo de servicio

Se presentan a continuación algunos casos de robo de servicio para destacar la necesidad de procesos de autorización dinámica, de un protocolo de reserva de recursos en dos fases, de puertas y de una coordinación entre puertas. En este sistema, gran parte de la inteligencia de control de la sesión se asigna a los clientes, que pueden adaptarse más fácilmente a la tecnología y proporcionar servicios nuevos e innovadores. Si bien este enfoque, destinado a garantizar la perdurabilidad, es un objetivo de diseño, debe reconocerse que deja la puerta abierta a muchas posibilidades de fraude. En este apéndice se analizan algunas de dichas posibilidades y las medidas de prevención en la arquitectura de señalización de QoS.

El supuesto básico es que el MTA no es inmune a los intentos de manipulación fraudulenta del cliente, y que se intentarán las manipulaciones más elaboradas para burlar los controles de red sobre el MTA y conseguir un servicio gratuito. Las posibles formas de manipulación fraudulenta del cliente son, entre otras, la apertura de la caja y la sustitución de memorias ROM, la sustitución de circuitos integrados, el sondeo y la reproducción del diseño del MTA, incluso la sustitución total del MTA por una versión ilegal del mercado negro. Existen soluciones técnicas para la seguridad física del MTA (por ejemplo, una trampa de gas nocivo para la apertura de la caja) pero no son aceptables.

Como el MTA sólo puede distinguirse por la comunicación sobre la red DOCSIS, es posible y bastante probable que se va a intentar emular el comportamiento de un MTA mediante un soporte lógico particular. Un ordenador con ciertos programas no se podría distinguir del verdadero MTA. En este caso, el comportamiento del soporte lógico se encuentra bajo el control total del cliente.

Además, se pretende implementar los nuevos servicios en el MTA y permitir la utilización de programas informáticos de distintos proveedores para el control de estos servicios. Dicho soporte lógico actualizado se descargará en el MTA, y los clientes podrán descargar versiones especiales ilegales que proporcionen un acceso fraudulento. No hemos incluido en este análisis los "caballos de Troya" incluidos en soporte lógico descargado, por tratarse del mismo tipo de problema que supone la comunicación del número de tarjeta de crédito y/o el número PIN de un cliente actualmente. Sólo consideramos el caso de un cliente que descarga soporte lógico intencionadamente para conseguir un beneficio ilícito.

## IX.1 Escenario N.º 1: Los clientes establecen por sí mismos conexiones con alta QoS

Un MTA que disponga de inteligencia suficiente puede recordar destinos marcados anteriormente y la dirección de los mismos, o utilizar otros mecanismos para determinar la dirección IP de un destino. Entonces puede ser él mismo quien intercambie señalización con el destino (con una cierta colaboración por parte del otro cliente) para negociar una conexión con alta calidad de servicio mediante la interfaz DOCSIS para un cliente integrado. Dado que no se utiliza ningún agente de red para iniciar la sesión, no se genera un registro de facturación. La solución es exigir una autorización dinámica en el CMTS; sin dicha autorización, fracasará cualquier intento de disponer de una calidad de servicio elevada.

Este proceso se ha realizado con la cooperación de dos MTA que han sido modificados, pero también se puede conseguir un robo de servicio similar modificando únicamente el iniciador. Si el MTA de origen utiliza el agente de red para establecer la sesión, informando al destino en la forma normalizada de una sesión de entrada, pero la alta calidad de servicio la ha negociado consigo mismo como en el caso anterior, no habrán registros de facturación y el iniciador podría obtener así una sesión gratis. En este caso también la solución consiste en exigir el uso de puertas en los CMTS.

## IX.2 Escenario N.º 2: Los clientes utilizan la QoS configurada para aplicaciones que no son de voz

Una QoS configurada de forma estática sólo indica que un cliente está autorizado para disponer de una elevada calidad de servicio, sin restricciones para la utilización del servicio. En concreto, un cliente que se haya suscrito a un servicio de comunicación vocal de calidad comercial y que por lo tanto esté autorizado para activar conexiones de gran anchura de banda y bajo retardo sobre la red DOCSIS, puede utilizar esta capacidad para navegación en la web y otras aplicaciones con un ordenador. La solución es exigir la autorización dinámica en el CMTS; sin dicha autorización fracasará cualquier intento de disponer de una calidad de servicio elevada.

## IX.3 Escenario N.º 3: El MTA modifica la dirección de destino de los paquetes vocales

Otra posibilidad es que dos MTA, distantes entre sí, establezcan cada uno una sesión local. Una vez que la anchura de banda y la conexión se han establecido, los MTA cambian las direcciones IP en los trenes del protocolo en tiempo real (RTP) para direccionarse mutuamente. El sistema de contabilidad sigue facturando a cada uno por sus sesiones locales, cuando en realidad los clientes están en una sesión de larga distancia. Por eso tenemos que instalar en los CMTS mecanismos que proporcionen acceso a una QoS superior exclusivamente por referencia a filtros de paquetes previamente autorizados. Así pues, además de la gestión de los recursos en dos fases, esta situación obliga a instalar filtros de paquetes en las puertas.

## IX.4 Escenario N.º 4: Utilización de medias conexiones

Es un ejemplo de robo de servicio que podría ocurrir si no se hiciera una coordinación de puertas. Supóngase que un cliente en una sesión compromete los recursos de sesión y que el otro no lo hace. Por ejemplo, supóngase que el cliente terminación compromete sus recursos, pero no el mensaje de señalización adecuado, de forma que el origen no compromete los suyos. En este caso sólo se abre una puerta y tanto los usuarios como la red quedan con media conexión. Como el iniciador no comprometió sus recursos, la red no puede legítimamente facturar al usuario por la media conexión. Dos clientes pueden ponerse de acuerdo para establecer cada uno media conexión, por la que no serán facturados, que pueden combinarse para crear una conexión completa entre las dos partes. Sería una sesión gratuita. Los fraudes de este tipo sólo pueden evitarse mediante la sincronización del funcionamiento de ambas puertas.

## IX.5 Escenario N.º 5: Terminación prematura manteniendo media conexión

La coordinación de puertas también es necesaria para dar por terminada una llamada. Supóngase que $MTA_O$ llama a $MTA_T$ y paga por la sesión. Dado que la sesión se factura a $MTA_O$, éste tiene claramente un incentivo para enviar al $CMTS_O$ un mensaje Release para cerrar su puerta y detener la facturación. Sin embargo, si $MTA_T$ no envía a $CMTS_T$ el mensaje Release para cerrar la puerta, se mantiene una media conexión. En este caso, $MTA_T$ puede seguir enviando voz y/o datos a $MTA_O$ sin ser facturado por la sesión. Por lo tanto, la puerta de la parte iniciadora en el $CMTS_O$ debe emitir un mensaje GATE-CLOSE (cierre de puerta) para cerrar la puerta del lado de terminación en el $CMTS_T$.

## IX.6 Escenario N.º 6: Mensajes de coordinación de puertas falsificados

Cada MTA conoce la identidad de su CMTS y la quíntupla que éste utiliza para el identificador de puerta (GateID). Los MTA pueden realizar varios tipos de negociación extremo a extremo antes de solicitar recursos; en particular, pueden intercambiar fácilmente información acerca de sus ID de puerta. Entonces el MTA puede imitar fraudulentamente el mensaje Gate-Open enviado al extremo que no paga y obtener una conexión unidireccional no facturada. Hacerlo dos veces permite disponer de una conexión completa no facturada. Para evitarlo el controlador de puerta puede

comunicar al CMTS una clave que se ha de emplear en los mensajes CMTS-CMTS para cada sesión (o para cada puerta).

### IX.7 Escenario N.º 7: Fraude contra llamantes indeseados

Las particularidades de la secuencia de establecimiento de la comunicación permiten que se autorice una anchura de banda en el destino más grande que en la fuente. En estas circunstancias, la parte llamada podría reservar y asignar una anchura de banda muy superior a la cantidad finalmente negociada, y la factura de la parte llamante sería superior a lo esperado. Si fuera posible, este mecanismo se podría utilizar en perjuicio de las empresas de telemarketing, como una retaliación contra las llamadas indeseadas que hacen durante la cena.

Dado que el CMS autoriza los recursos de sesión antes de que el MTA los solicitara, se tienen más garantías de que el CMTS no permitirá más solicitudes de recursos que las autorizadas.

## Apéndice X

## Servicio común de política abierta (COPS)

### X.1 Procedimientos y principios del servicio común de política abierta

Este apéndice es una breve descripción de los procedimientos y principios del servicio común de política abierta (COPS) y de la relación entre el COPS y otros protocolos tales como LDAP.

El servicio común de política abierta (COPS, *common open policy service*) es un protocolo cliente/servidor definido para ser utilizado en el control de admisión de redes del tipo RSVP/IntServ y DiffServ con QoS. COPS se ejecuta sobre TCP/IP utilizando un número de puerto conocido (3288). Las entidades COPS residen en un dispositivo situado en el límite de la red y en un servidor de políticas. En el marco de RAP se definen tres entidades funcionales:

- Punto de decisión de política (PDP, *policy decision point*) – Es la entidad servidora COPS que toma la decisión final sobre la admisión o rechazo de la sesión, basándose en la información disponible sobre políticas. Es previsible que se implemente como una aplicación en un dispositivo servidor autónomo.
- Punto de imposición de política (PEP, *policy enforcement point*) – Entidad cliente en COPS que consulta al PDP para tomar decisiones de política o informarse sobre las políticas antes de tomar decisiones de control de admisión. El PEP puede recibir peticiones de servicio y luego interrogar al PDP, que podrá responder de forma afirmativa o negativa, o bien el PEP puede informar al PDP que desea recibir información relativa a las decisiones y a la política sin tener que solicitarlo.
- Punto de decisión local (LDP, *local decision point*) – Es una versión local del PDP que puede tomar decisiones basadas en información local o en información relativa a decisiones anteriores que se conserva en un elemento de almacenamiento intermedio. Una decisión del PDP siempre tiene prioridad respecto a una decisión del LDP.

La figura X.1 es una ilustración de la secuencia COPS en un entorno RSVP/IntServ.

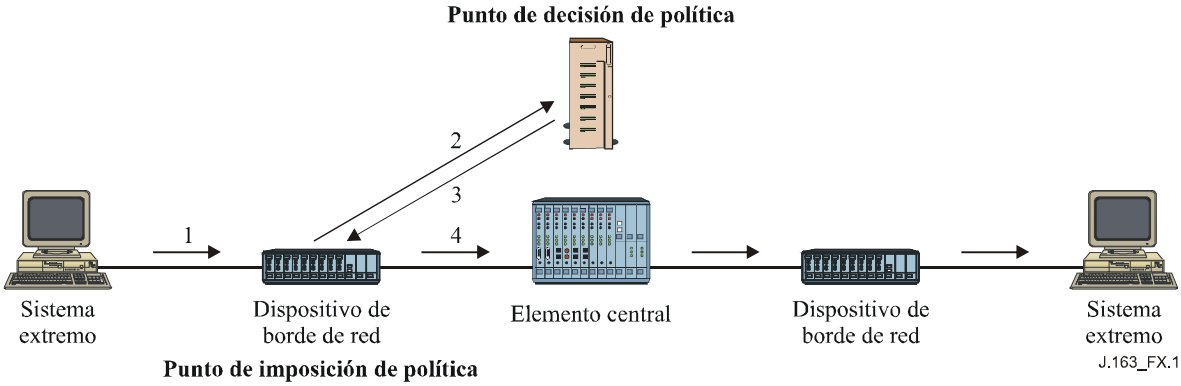



**Figura X.1/J.163 – Protocolo COPS**

En la secuencia COPS, el PEP cliente es la entidad encargada de establecer inicialmente una sesión con el PDP utilizando información que está configurada en el PEP o que se obtiene por algún otro medio. Una vez que la sesión se ha establecido, el dispositivo del borde de red que recibe un mensaje RSVP (1) generará una petición de tratamiento al PDP (2) que describe el contexto y contiene información sobre la misma petición. El PDP responde (3) con la decisión de aceptar o rechazar la petición, y si ésta es aceptada, el dispositivo del borde de la red retransmite el mensaje RSVP hacia la red (4).

Cada sesión se mantiene mediante un mensaje mantener vigente: mantiene la sesión activa si no se han recibido mensajes recientemente. Cada petición RSVP o de cualquier otro tipo se identifica mediante un alias que puede utilizarse para asociar la respuesta, respuestas ulteriores no solicitadas y la cancelación.

Los mensajes de protocolo pueden utilizarse también para otras tareas. Constan de un código de operación que identifica si es una petición, una respuesta u otro tipo de mensaje, seguido de objetos que se identifican por sí mismos, cada uno de los cuales contiene una clase de objeto y un identificador de versión. Cada objeto incluye un número de clase que determina su naturaleza, por ejemplo de objeto temporizador u objeto decisión, y de un tipo de clase que identifica el subtipo o versión de la clase utilizada.

Otras clases de objetos incluyen los datos de asignación de anchura de banda necesarios para identificar los recursos que solicita el usuario, y los objetos de política que pueden ser enviados desde el PDP para ser incluidos en el mensaje RSVP cuando éste se envía a la red.

## X.2 Comparación en términos de política entre COPS y LDAP

El protocolo COPS y el protocolo simplificado de acceso al directorio (LDAP, *lightweight directory access protocol*) se han considerado para la gestión basada en políticas, pero las funciones de uno y otro son muy distintas.

En COPS, el cliente solicita al punto de decisión de política (PDP) que tome una decisión y mantiene comunicaciones con el PDP para participar activamente en la gestión de la política y en asuntos relacionados con la misma. Es posible que el PEP que hace la petición no conozca las políticas y se apoye en el PDP para tomar decisiones en función del conocimiento que éste tiene de las políticas. El protocolo permite que el PEP informe al PDP sobre la petición, y que éste devuelva una decisión para aceptar o rechazar la petición.

En LDAP, el cliente solicita un registro de un directorio. La función que utiliza el registro depende del cliente, el cual debe ser capaz de entender el registro leído y decidir como utilizar dicha información. El servidor debe ser capaz de encontrar el registro correcto sobre la base de la

información incluida en la propia petición, lo cual puede implicar utilizar una función de búsqueda, o de recuperación de múltiples registros.

Tanto COPS como LDAP pueden utilizarse en el contexto del control de admisión RSVP. COPS se utilizaría entre el PEP y el PDP para enviar una petición de análisis basado en la política. LDAP se utilizaría entre el PDP y un servidor de directorio para recuperar registros de política asociados con las direcciones de origen y de destino para la petición RSVP. El PDP tomaría entonces una decisión basada en la información sobre política que se ha recuperado y utilizaría el COPS para devolver esa decisión al PEP. Véase la figura X.2.

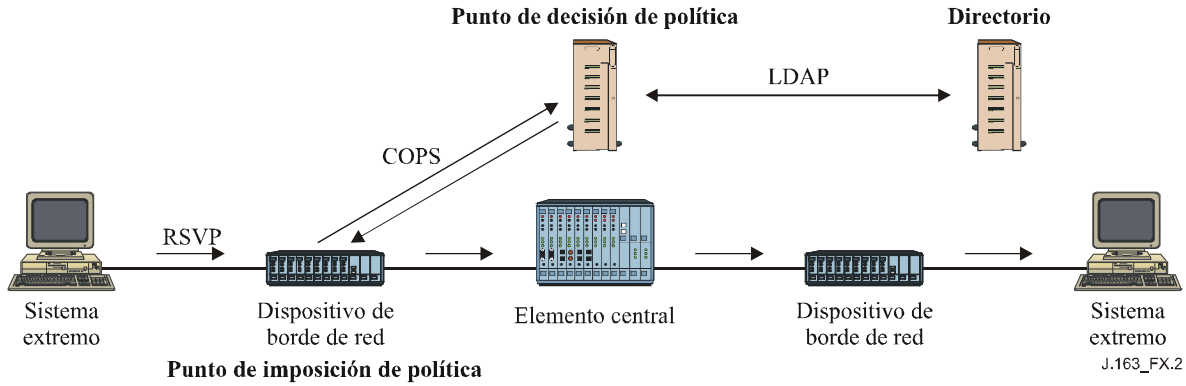



**Figura X.2/J.163 – Modelo con COPS y LDAP**

# Apéndice XII

# Consideraciones sobre el TCP

En esta Recomendación se define una interfaz entre un controlador de puerta (GC) y un sistema de terminación de módem de cable (CMTS) que se utiliza para la autorización de puerta y que, fundamentalmente, soporta un protocolo basado en transacciones independientes entre sí. El mecanismo de transporte de estos mensajes puede ser el protocolo de control de transmisión (TCP, *transmission control protocol*). Sin embargo, la utilización del TCP podría suponer algunos problemas de calidad de funcionamiento. En este apéndice se examinan algunos de estos problemas y se proponen soluciones que permiten un transporte aceptable mediante optimizaciones de la implementación y un ajuste de la implementación del TCP.

El diseño de la red debe soportar el grado deseado de fiabilidad y funcionamiento en tiempo real.

## XII.1 Requisitos

Requisitos del protocolo de transporte para las comunicaciones entre el GC y el CMTS:

1) Transporte fiable de mensajes entre el GC y el CMTS.

2) El intercambio normal de mensajes (sin pérdida de paquetes) debe hacerse con poco retardo (del orden de milisegundos). También es necesario que el retardo sea razonablemente bajo en una situación de pérdida de paquetes (del orden de decenas de milisegundos).

3) Podrá haber numerosas peticiones en curso simultáneamente, porque es probable que se produzcan a la vez numerosos establecimientos de comunicación.

4) Deberá evitarse un posible bloqueo de cabeza de línea (HOL, *head-of-the-line*).

5) La asociación entre el GC y el CMTS puede prolongarse (al menos varios minutos), pero el proceso de establecimiento de una nueva conexión con el CMTS en caso de fallo de un GC no debe requerir un tiempo excesivo. Hay que considerar con especial atención el caso de creación de una nueva conexión durante el establecimiento de una comunicación.

## XII.2 Modificaciones recomendadas

Recomendaciones de modificaciones de una implementación estándar del protocolo TCP:

1) Modificar los mecanismos de temporización para el establecimiento de la conexión (hacerlo más agresivo).
2) Permitir una ventana mayor después del establecimiento de la conexión.
3) Tener múltiples conexiones TCP por cada pareja GC-CMTS para paliar posibles problemas de cabeza de línea (HOL) (por ejemplo, utilizarlas en forma cíclica).
4) Utilizar una granularidad de la temporización inferior a 500 ms.
5) Inhabilitar el algoritmo de Nagle en el extremo transmisor para reducir el retardo.
6) Disponer de una interfaz sin bloqueo entre la aplicación y la pila TCP.

En el resto de este apéndice se describe la implementación de estas modificaciones.

## XII.3 Efecto del establecimiento de la conexión TCP en el retardo postmarcación

El establecimiento de la conexión TCP necesita tres señales de toma de contacto, tal como se indica a continuación (véase la figura XII.1).

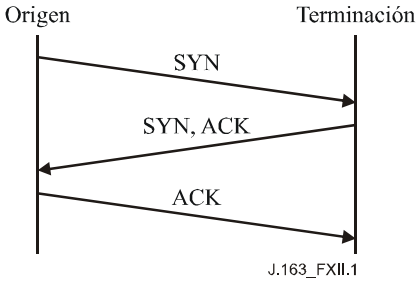



**Figura XII.1/J.163 – Establecimiento de una conexión TCP**

El protocolo TCP retransmite los segmentos que se suponen perdidos, tomando como criterios determinantes la estimación del tiempo de ida y vuelta (A) y una desviación típica respecto al valor de A (D). El valor de la temporización de retransmisión (RTO, *retransmission timeout value*) se calcula generalmente utilizando la fórmula siguiente:

$$RTO = A + 4D$$

pero la RTO inicial se calcula utilizando la fórmula siguiente:

$$RTO = A + 2D$$

donde A y D se inicializan con los valores de 0 y 3 segundos respectivamente. Cuando tiene lugar una retransmisión, se aplica una variación exponencial con un multiplicador de 2 al valor vigente de RTO. Así, el RTO del primer segmento se calcula de la forma siguiente:

$$RTO = 0 + 2 \times 3 = 6$$

Por lo tanto, si el segmento SYN inicial se pierde, la retransmisión no se produce hasta transcurridos 6 segundos. En ese instante, el RTO sería:

$$RTO = 0 + 4 \times 3 = 12$$

y aplicando una variación de potencia 2 se obtiene un nuevo valor de temporización de 24 segundos para la retransmisión. Por lo tanto, si también se pierde la retransmisión, habrán transcurrido 30 segundos antes de que se produzca la tercera retransmisión.

La importancia de este problema depende enteramente de la frecuencia de fallo del establecimiento de la conexión GC → CMTS durante el retardo posmarcación. En las situaciones actualmente previsibles, esta circunstancia es mucho más una excepción que la regla. El efecto de un retardo de establecimiento de la conexión en el retardo posmarcación es un motivo suficiente para no crear una conexión durante el periodo de retardo posmarcación. El retardo de creación de conexión debido a la pérdida de paquetes podría reducirse utilizando el principio de marcación de paquetes Diffserv al objeto de reducir el retardo y la probabilidad de pérdidas, similar al principio utilizado actualmente para encaminamiento de tráfico.

### XII.4 Necesidad de un retardo reducido de los paquetes entre el GC y el CMTS, incluso en situaciones de pérdidas

El requisito de recuperación de paquetes perdidos (2) supone determinadas soluciones para que el TCP se recupere rápidamente de una situación de pérdida. Cuando se transmiten pocos paquetes y el receptor no puede generar un número suficiente de acuses de recibo duplicados, se trata de la recuperación de un estado de temporización de retransmisión. El algoritmo de retransmisión TCP se basa en la media redondeada del tiempo de ida y vuelta (RTT, *round-trip time*), A, y la media redondeada de la desviación típica de RTT. Tal como se ha descrito anteriormente, el valor del temporizador de retransmisión es:

$$RTO = A + 4D$$

y si este tiempo expira el segmento en cuestión se retransmite y se ajusta exponencialmente RTO con un multiplicador de 2[8] hasta que el RTO alcanza un límite superior de 64 segundos. Los segmentos tratados por el TCP se transmiten satisfactoriamente al destino o bien se cierra la conexión después de transcurrido un determinado periodo de tiempo (generalmente largo, por ejemplo de 2 a 9 minutos).

Es conveniente adoptar esta estrategia de retransmisión, pero hay dos problemas (conexos) para la interfaz considerada:

1) Si el segmento no se entrega satisfactoriamente en poco tiempo, es muy probable que se abandone la llamada que se encuentra en fase de establecimiento y se interrumpa la transacción.

2) El límite máximo de 64 segundos del temporizador de retransmisión no es adecuado para las comunicaciones en tiempo real, para las cuales debiera ser mucho menor.

Un problema distinto pero relacionado es la granularidad del RTO. Si bien la especificación de TCP no incluye la granularidad del RTO, un valor de 500 ms es habitual en los sistemas de explotación comerciales. Por lo tanto, un segmento perdido no será en general detectado en menos de 500 ms, y dos segmentos perdidos no serán detectados en menos de 500 ms + 1000 ms = 1,5 segundos.

Para que el sistema se recupere rápidamente de una situación de paquetes perdidos en una secuencia (sin recurrir a la solución de múltiples acuses de recibo duplicados para retransmitir rápidamente ni tener que esperar la activación del temporizador RTO), puede ser conveniente implementar TCP-SACK, que ayuda a realizar la recuperación incluso cuando no se ha alcanzado el umbral de retransmisión rápida. También se recomienda reducir la granularidad de temporizador en la implementación TCP (posiblemente inferior a 500 milisegundos).

---

[8] TCP utiliza mensajes ACK duplicados para provocar la retransmisión de segmentos que pueden estar perdidos, pero no tendremos en cuenta esta función en esta parte del análisis.

## XII.5 Bloqueo de cabeza de línea

El bloqueo de cabeza de línea resulta del servicio de distribución de datos en orden del TCP y del hecho de que un segmento perdido puede bloquear la entrega de segmentos posteriores a la aplicación. Si los segmentos 1 y 2 se envían desde A hasta B, y el segmento 1 se pierde, el segmento 2 no puede entregarse a la aplicación hasta que el segmento 1 se haya retransmitido satisfactoriamente.

Para la interfaz considerada, este bloqueo de cabeza de línea puede superarse relativamente bien si se dispone de múltiples conexiones TCP establecidas entre el GC y el CMTS que serán todas utilizadas para realizar las transacciones, por ejemplo utilizándolas de forma cíclica. Por tanto, la pérdida de un segmento en una conexión no afectará a otros segmentos pues las transacciones se envían por conexiones diferentes.

El inconveniente de este procedimiento es que no es probable que los segmentos perdidos sean retransmitidos antes de la activación del temporizador de retransmisión (es distinto cuando se recibe un ACK duplicado), ya que hasta entonces no habría ningún segmento adicional que transmitir.

## XII.6 Arranque lento de TCP

El mecanismo de arranque lento de TCP puede limitar la capacidad del TCP de iniciar la transmisión de un tren de paquetes de datos, especialmente cuando el tren consta de un número pequeño (mayor que 1) de paquetes de datos. Es conveniente elegir una ventana inicial de tamaño superior a uno (tanto al activar la conexión como después de recuperarse de la congestión producida por la pérdida de un solo paquete). Se considera conveniente elegir un tamaño de ventana de 2 a 4 veces el valor del tamaño máximo de un segmento (MSS, *maximum segment size*). No obstante, esta ventana inicial no ha de ser superior a 4 MSS para evitar un nuevo riesgo de congestión.

## XII.7 Retardo de paquetes: algoritmo de Nagle

El TCP/IP se diseñó inicialmente para soportar múltiples sesiones de usuario sobre una red lenta. El algoritmo de Nagle se introdujo al objeto de optimizar la utilización de la red para el caso de usuarios que realizaban la entrada de datos directamente desde un teclado. En esencia, este algoritmo retarda la transmisión de paquetes hasta que se haya acumulado un número suficiente de ellos en una memoria intermedia o hasta que haya transcurrido un determinado tiempo (normalmente alrededor de 200 milisegundos).

Tratándose de tráfico en tiempo real, es conveniente inhabilitar el algoritmo de Nagle para la comunicación entre GC y CMTS. En la mayoría de las plataformas basadas en Unix es posible inhabilitar el algoritmo Nagle utilizando la siguiente llamada del sistema en el descriptor de ficheros del conector:

Ejemplo 1: Establecimiento de la opción TCP_NODELAY

```
/* set TCP No-delay flag (disable Nagle algorithm) */
int flag = 1;
setsockopt(fd, IPPROTO_TCP, TCP_NODELAY, &flag,
   sizeof(flag));
```

La mayoría de los otros lenguajes y plataformas tienen una facilidad similar que permite invalidar el algoritmo de Nagle (se conoce generalmente como la opción TCP_NODELAY).

## XII.8 Interfaz sin bloqueo

Por defecto, la mayoría de los sistemas de explotación proporciona una interfaz con bloqueo para los conectores TCP/IP, que puede mejorar el esquema de recuperación de errores, pero también afecta la calidad de funcionamiento del canal de comunicación.

En esencia, en un sistema de interfaz con bloqueo una instrucción de sistema tal como enviar() no vuelve a producirse hasta que el sistema operativo confirma que el mensaje ha sido almacenado satisfactoriamente en la memoria de almacenamiento intermedio de transmisión.

Tal vez convendría emplear una interfaz sin bloqueo para mejorar la calidad de funcionamiento y soportar eventos asíncronos que utilizan la instrucción función seleccionar() de una arquitectura UNIX. Puede establecerse una interfaz de conector sin bloqueo utilizando esta instrucción para el conector recién creado.

Ejemplo 2: Establecimiento de la opción O_NONBLOCK

```
/* set the socket to non blocking */
fcntl( fd, F_SETFL, O_NONBLOCK );
```

La mayoría de los otros lenguajes y plataformas tienen una facilidad similar.

## SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2006