UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.163

(03/2004)

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

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

Numerosos operadores de televisión por cable están mejorando la calidad de sus sistemas a fin de disponer de capacidad de transporte bidireccional y utilizar dicha capacidad para la prestación de servicios de datos IP de alta velocidad conformes a las Recomendaciones UIT-T J.83 y J.112. Ahora desean incrementar la capacidad de esta plataforma de distribución para poder ofrecer telefonía. Esta Recomendación pertenece a una serie de Recomendaciones destinadas a conseguir dicho objetivo. Proporciona los mecanismos para conseguir la calidad de servicio dinámica necesaria en muchas aplicaciones en tiempo real.

La presente Recomendación se ha revisado para adaptarla a la evolución de la industria desde su publicación y ajustarse a la actual especificación del sistema PacketCable™ de CableLabs.

El anexo A se ha retirado porque ya no es necesario para las nuevas condiciones de la tecnología en Europa. En línea con esta evolución, el anexo B se ha integrado en el texto principal de esta Recomendación, y se ha reemplazado el término "AN" (Nodo de acceso) por "CMTS" (Sistema de terminación de módem de cable) en toda la Recomendación.

Orígenes

La Recomendación UIT-T J.163 fue aprobada el 15 de marzo de 2004 por la Comisión de Estudio 9 (2001-2004) 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

En esta Recomendación se presentan 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 las peticiones de una calidad de servicio específica de la red J.112 en dispositivo de cliente. Numerosos ejemplos ilustran la utilización de esta Recomendación. Esta Recomendación pretende definir una arquitectura de calidad de servicio (QoS, *quality of service*) para la parte de "acceso" de una red de comunicaciones por cable que utiliza el protocolo IP (IPCablecom), que se pone a disposición de cada uno de los flujos de las aplicaciones que la solicitan.

2 Referencias

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

2.1 Referencias normativas

- 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 (2002), *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 1321 (1992), *The MD5 Message-Digest Algorithm*.
- IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*. (Updated by RFC 2750.)
- IETF RFC 2210 (1997), *The Use of RSVP with IETF Integrated Services*.
- IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.

– IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

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 (2004), *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 (2001), *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 (2002), *Especificación de la seguridad de IPCablecom*.

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

– IETF RFC 1890 (1996), *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 2543 (1999), *SIP: Session Initiation Protocol*.

– IETF RFC 2749 (2000), *COPS usage for RSVP*.

– IETF RFC 2750 (2000), *RSVP Extensions for Policy Control*.

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

– IETF RFC 2866 (2000), *RADIUS Accounting*.

– IETF RFC 2961 (2001), *RSVP Refresh Overhead Reduction Extensions*.

– IETF RFC 2996 (2000), *Format of the RSVP DCLASS Object*.

– IETF RFC 3006 (2000), *Integrated Services in the Presence of Compressible Flows*.

– IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

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

– *PacketCable Distributed Call Signalling Specification,* PKT-SP-DCS-D03-000428, 28 April 2000.

– *PacketCable Dynamic Quality-of-Service Specification,* PK-SP-DQOS-I07-03-08-15.

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 J.112: 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

En esta Recomendación se utilizan las siguientes siglas.

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 adaptor*)
NCS	Señalización de llamada basada en la red (*network-based call signalling*)
PHS	Supresión de cabecera 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:

Obligación firme (TIENE QUE, HAY QUE, futuro)	La obligación firme se indica mediante estas expresiones, el empleo del verbo principal en futuro simple o la expresión "ES OBLIGATORIO".

Prohibición firme (negación)	La prohibición firme se expresa mediante la negación del verbo principal en futuro simple o la expresión "ESTÁ PROHIBIDO".
Conveniencia (DEBERÍA)	Se utiliza el verbo modal en condicional "DEBERÍA" y otros verbos con significado de conveniencia (aconsejar, recomendar) o los adjetivo "RECOMENDADO" "CONVENIENTE". Significa que algo no tiene que hacerse necesariamente, pero es importante darse cuenta de todas las consecuencias y considerarlo detenidamente antes de hacer otra cosa.
Inconveniencia (NO DEBERÍA)	Se utiliza el verbo modal en condicional y con negación "NO DEBERÍA". Significa que algo podría ser aceptable o útil en algunos casos, pero es importante darse cuenta de todas las consecuencias y considerarlo detenidamente antes de hacerlo.
Opción (PODER)	Este verbo, los adjetivos "FACULTATIVO" y "OPCIONAL" y la expresión "ES POSIBLE" indican que existe la posibilidad de elegir entre varias alternativas. Por ejemplo, un proveedor puede incluir un elemento porque lo exige el mercado o para mejorar el producto, pero no necesariamente todos los proveedores.

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 multimedios (MTA, *multimedia terminal adapter*) y el sistema de terminación de módem de cable (CMTS, *cable modem termination system*), incluyendo la red J.112. 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 J.112 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.

Se han definido dos protocolos de señalización de llamadas IPCablecom: la señalización de llamada basada en la red (Rec. UIT-T J.162) y la señalización de llamada distribuida (SIP, RFC 2543 del IETF). 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 J.112 cercana a la parte iniciadora) y en el segmento "distante" (la red J.112 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 activación 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* PK-SP-DQOS-I07-03-08-15.

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 J.112. Por lo tanto, es necesario identificar información que permita asociar la utilización de recursos de QoS J.112 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 J.112, los recursos que están reservados pero no comprometidos están disponibles para su asignación temporal a otros flujos J.112 (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, y para la activación en dos fases en el caso de MTA autónomos. La activación en una fase para MTA autónomos queda para ulteriores versiones de esta Recomendación.

3) *Proporcionar políticas definidas de IPCablecom destinadas a controlar la QoS en la red J.112 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 J.112 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 J.112*

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

6) *Utilizar mecanismos de QoS de la capa MAC J.112*

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 J.112. Además, se deben soportar varios modelos de correspondencia de flujos (asociar una sesión IPCablecom o múltiples sesiones IPCablecom a un único flujo J.112).

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 J.112*

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 J.112. Por ejemplo, si un módulo de cliente IPCablecom falla durante una sesión IPCablecom, deberían liberarse todos los recursos de QoS J.112 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 postselección*

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 postselección.

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 J.112). 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 el caso de un MTA integrado, el único trayecto de señalización que se soporta es el que se especifica aquí utilizando el protocolo RSVP. En el caso de un MTA integrado, son posibles tanto el RSVP como el acceso directo a la señalización MAC J.112.

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 (MTA) pueden ser diferentes. Se encuentran en la instalación del usuario y están conectados a la red a través del canal J.112. 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 J.112 con la red J.112.

2) **MTA autónomo**: Es un dispositivo de cliente que implementa la funcionalidad multimedia sin incorporar una interfaz de capa MAC J.112. 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 J.112.

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. 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) es el elemento de red IPCablecom que tiene funciones centralizadas para procesar los flujos de información. El CMTS corresponde al punto de imposición de políticas (PEP, *policy enforcement point*) definido en el protocolo de asignación de recursos del IETF (RAP, *resource allocation protocol*).

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

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*)]. Un CMS que utilice el modelo de señalización de llamada controlado por la red implementa un agente de llamada que controla directamente la sesión y mantiene el estado de cada llamada. Un CMS que utilice el modelo de señalización de llamada distribuida puede actuar como "representante o proxy DCS" y realizar servicios solamente durante el establecimiento inicial de la sesión. 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.

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 J.112 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 J.112 se considera que los flujos J.112 son unidireccionales o bidireccionales. En cada sentido, los flujos J.112 están sujetos a las operaciones que se identifican a continuación.

Funciones del módem de cable (CM) a través del cual el tráfico accede a la red J.112 con capacidad de QoS:

- Clasificar el tráfico IP en flujos J.112 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 las cabeceras de los paquetes IP ascendentes conforme a la política del operador de red.
- Obtener del CMTS la QoS J.112 requerida.
- Aplicar adecuadamente los mecanismos de QoS J.112.

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 J.112 para garantizar la aplicación de los valores definidos en las políticas del operador de red.
- Modificar el campo TOS de las cabeceras 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 J.112 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 IETF 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 J.112). 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 J.112.

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.

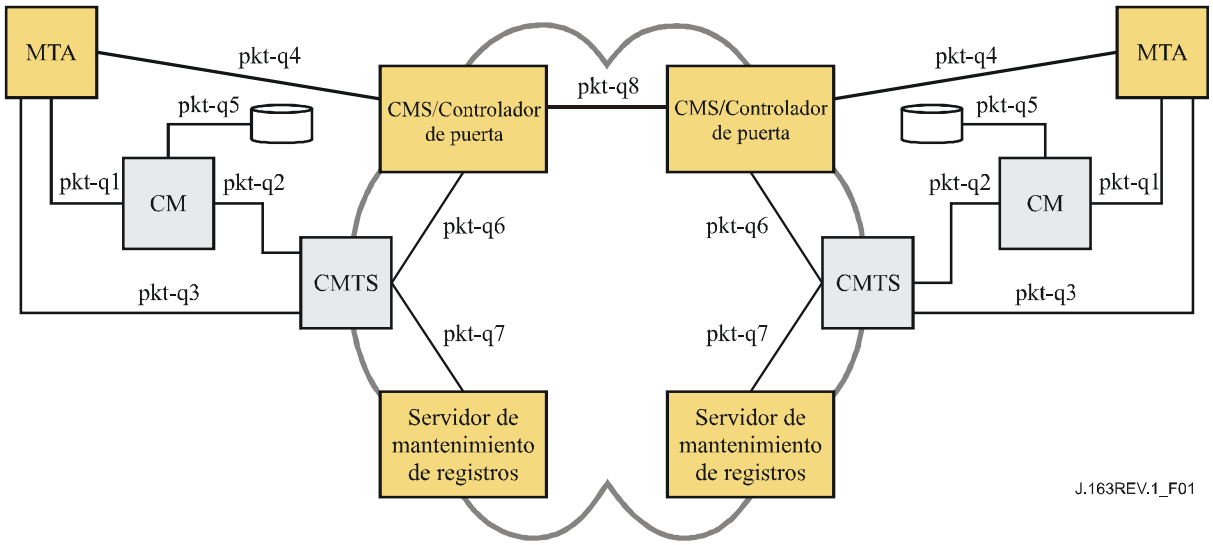


Figura 1/J.163 – Interfaces de señalización de QoS en una red IPCablecom

Las interfaces pkt-q1 a pkt-q8 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. Se muestran dos alternativas para esta especificación: una interfaz general que puede utilizarse para MTA integrados o autónomos, y una interfaz facultativa que sólo está disponible para MTA integrados.

Cuadro 1/J.163 – Interfaces DQoS

Interfaz	Descripción	DQoS de MTA integrado/autónomo	DQoS dinámica de MTA integrado (opcional)
pkt-q1	MTA-CM	No disponible	Interfaz de capa MAC J.112
pkt-q2	CM-CMTS	QoS J.112, iniciada por el CMTS	QoS J.112, iniciada por el CM
pkt-q3	MTA-CM TS	RSVP+	No disponible
pkt-q4	MTA-GC/CMS	NCS/DCS	NCS/DCS
pkt-q5	CM-Servidor de configuración	No disponible	No disponible
pkt-q6	GC-CMTS	Gestión de puerta	Gestión de puerta
pkt-q7	CMTS-RKS	Facturación	Facturación
pkt-q8	CMS-CMS	Señalización CMS a 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 J.112 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 J.112 entre CM y CMTS

Es la interfaz de QoS J.112 (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 J.112. Esta interfaz se define en la Rec. UIT-T J.112.

pkt-q3: Interfaz de la capa de red entre MTA y CMTS

Esta interfaz se utiliza para solicitar anchura de banda y QoS en términos de retardo, utilizando el RSVP normalizado y las extensiones al mismo que se especifican en esta Recomendación. Como resultado del intercambio de mensajes entre el MTA y el CMTS, los flujos J.112 se activan utilizando la señalización originada en CMTS sobre la interfaz pkt-q2.

pkt-q4: 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-q5: Señalización entre el sistema de configuración J.112/IPCablecom y el CM

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

pkt-q6: 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. En relación con la admisión y la autorización, y en el contexto de IPCablecom, debe existir una relación de confianza mutua entre el GC/CMS y el CMTS.

pkt-q7: 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-q8: 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.
- 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 ha 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

---

[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.

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 un superconjunto del protocolo de reserva de recursos (RSVP) del IETF.

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 J.112 se gestionan sobre la base de flujos J.112 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.

En la figura 2 se muestra gráficamente este modelo. Esta Recomendación incluye un entorno de cliente en el que un MTA autónomo puede conectarse al CM mediante una red de enlaces y de encaminadores normalizados con capacidad RSVP.

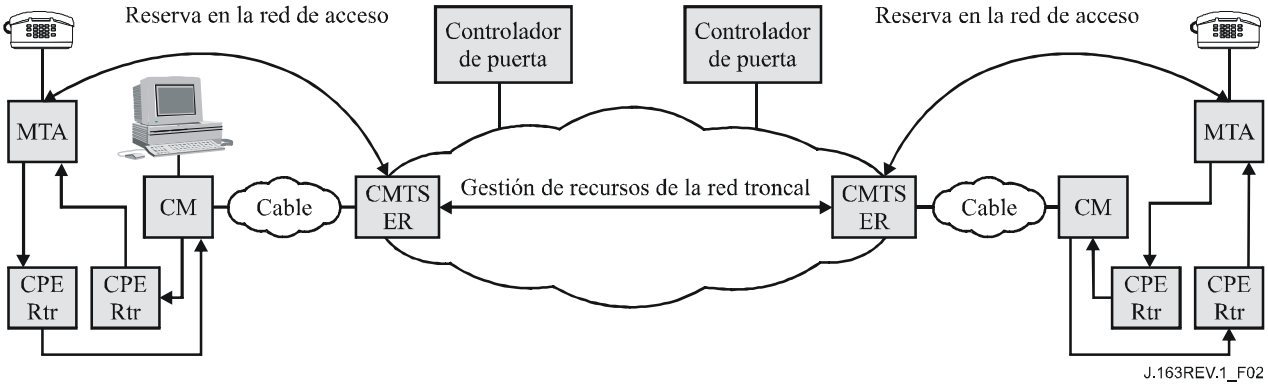


Figura 2/J.163 – Marco de referencia de una sesión

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 J.112). 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 J.112 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. En la especificación de configuración se indica cómo configurar el flujo de señalización dedicado (véase la nota). 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.

NOTA – Los atributos de número de clase de servicio (SCN, *service class number*) para señalización de llamada en sentido ascendente (*call signalling SCN up*) y en sentido descendente (*call signalling SCN down*), y de máscara de red (*call signalling network mask*) definen el flujo de señalización dedicado para un MTA integrado, si han sido definidos en el archivo de configuración del MTA.

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 J.112 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.

Se ha planteado una arquitectura muy general para permitir el desarrollo de nuevos servicios y la ulterior evolución de las arquitecturas de red. Este objetivo impone diversos requisitos para una arquitectura de QoS viable, que se describen en las cláusulas siguientes.

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 estas normas. De 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 el protocolo RSVP, que pueden interpretarse tramo a tramo en la red local (del usuario) y de acceso (en el caso de clientes integrados, puede ser la interfaz de capa MAC J.112). 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, Rec. UIT-T J.112).

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 J.112. En la red J.112, que no permite trayectos diferentes hacia adelante y hacia atrás, este protocolo añade varios objetos nuevos al RSVP que permiten que el CMTS reduzca el retardo actuando como representante (proxy) del cliente del extremo lejano.

Los mensajes RSVP, los mensajes de gestión J.112 y los mensajes de señalización de llamada (denominados en general mensajes de señalización) son todos transportados por la red J.112 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 J.112 separado en el CM, con

QoS mejorada, destinado a transportar tráfico de señalización. Este flujo J.112 separado se configura de la misma forma que otros trenes de medios J.112 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 (por ejemplo, al transmitir el primer mensaje INVITE si se trata de un sistema DCS).

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 J.112 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 J.112, 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 de varios códecs, es importante asignar los recursos adecuados para que los cambios ulteriores de códec funcionen correctamente. Es necesario asignar los siguientes recursos:

- Ancho de banda autorizado: el CMS/GC TIENE QUE autorizar el mínimo valor superior (LUB, *least-upper-bound*) de ancho de banda del códec que se podrá utilizar en la conexión durante la asignación de la puerta.
- Ancho de banda reservado: el MTA TIENE QUE reservar el mínimo valor superior de ancho 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 el ancho de banda reservado es superior al ancho de banda comprometido, habrá que renovar el primero enviando un mensaje de cambio de servicio dinámico (DSC) J.112 al CMTS.
- Ancho de banda comprometido: el MTA COMPROMETERÁ sólo el códec utilizado en sentido ascendente. Así, el ancho de banda adicional no utilizado (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 ancho 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.

5.7 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. 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.

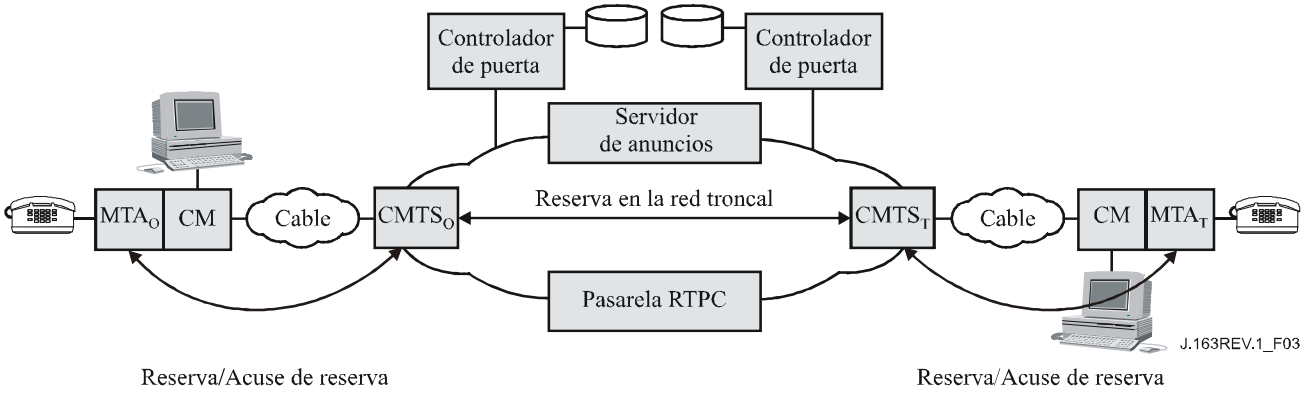


Figura 3/J.163 – Fase 1 de la gestión de recursos

La figura 3 muestra la primera fase del protocolo de gestión de recursos para una aplicación multimedia. En esta descripción, los subíndices "O" y "T" designan los puntos de origen y terminación de la llamada. El MTA puede ser un anfitrión de VoIP autónomo o un MTA integrado (este último se muestra en la figura 3). MTA_O y MTA_T hacen una petición de reserva de recursos (mensaje PATH de RSVP o mensaje J.112 de la interfaz facultativa 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. En el contexto de RSVP, el mensaje RESV enviado por el CMTS (donde reside la puerta) constituye el acuse de recibo dirigido al MTA.

La figura 4 muestra la segunda fase. Después de determinar que los recursos están disponibles, MTA_O envía a MTA_T un mensaje RING (activación de señal de llamada del teléfono). MTA_T envía una indicación RINGING (tono de llamada activado) al MTA_O para señalar que los recursos están disponibles y que se ha recibido el mensaje RING. Cuando la parte llamada descuelga el teléfono, MTA_T envía un mensaje ANSWERED (contestado) al MTA_O y un mensaje COMMIT (compromiso) al $CMTS_T$. Al recibir el mensaje ANSWERED, el MTA_O envía al $CMTS_O$ un mensaje COMMIT. El mensaje COMMIT hace que los recursos se asignen para la llamada en las redes J.112. 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).

Los mensajes RING, RINGING y ANSWERED de esta figura y de la descripción anterior son equivalentes lógicos de los mensajes de señalización intercambiados por los protocolos J.162 y SIP IETF RFC 2543.

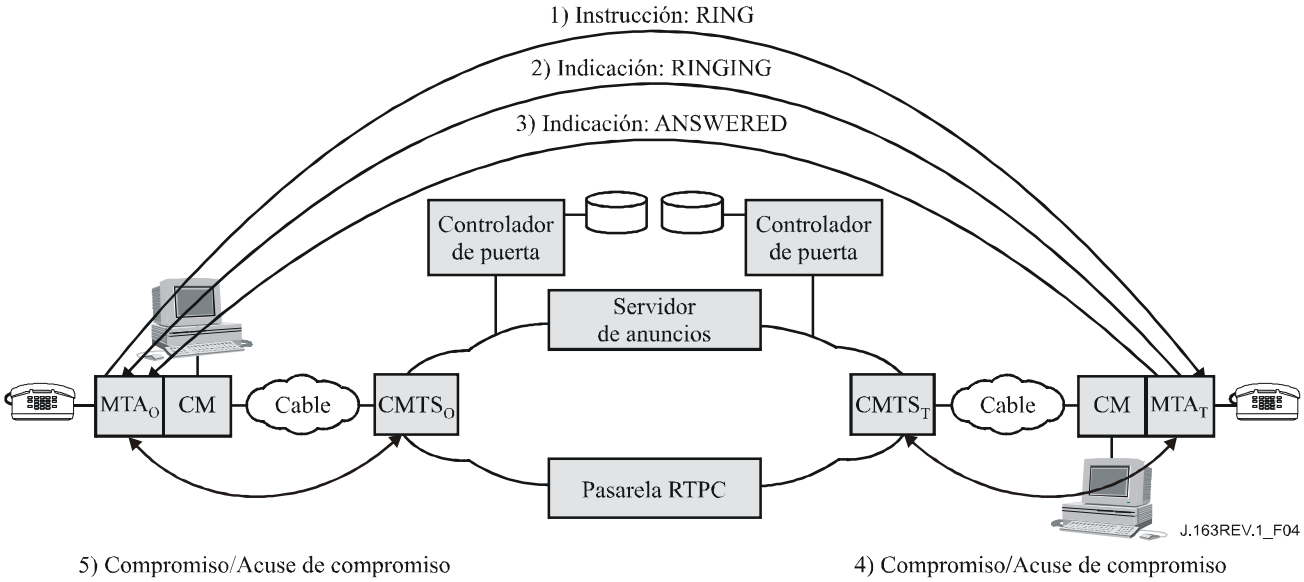


Figura 4/J.163 – Fase 2 de la gestión de recursos

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.

5.7.4 Recursos de la sesión

En la figura 5 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

---

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

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.

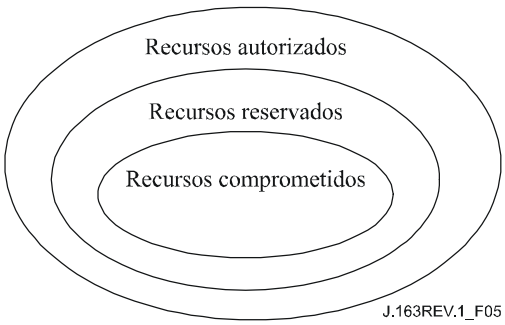


Figura 5/J.163 – Recursos autorizados, reservados y comprometidos

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 posibles políticas de control de admisión que pueden implementarse 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 RESERVA.

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 J.112.

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: establecer estados temporales mediante mensajes de renovación en la gestión de recursos (transmitir periódicamente mensajes RSVP-PATH durante una sesión activa), 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 J.112 (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 J.112, 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 de la cabecera 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, utilizando el objeto DCLASS propuesto por el IETF en el RSVP. 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 1890). 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 1890 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 ancho de banda para dicho CÓDEC.

En el caso de códecs menos conocidos, no es posible determinar los requisitos de ancho 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 ancho de banda (b) para especificar estos requisitos del códec desconocido. Estructura de la línea parámetro de ancho de banda (b):

b= <modifier>: <bandwidth-value>

Por ejemplo:

b= AS:99

Es OBLIGATORIO utilizar este parámetro de ancho 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 el ancho de banda solicitado en el SDP es una decisión de políticas del CMS/CMTS.

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

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

6 Protocolo de calidad de servicio entre el MTA y el CMTS (pkt-q3)

Para cumplir los requisitos previamente descritos, el RSVP y la arquitectura de servicios integrados IETF RFC 2210 se utilizan como bases del mecanismo de señalización para proporcionar la QoS local. La versión actual de la especificación del RSVP debe ser mejorada a fin de cumplir los requisitos de la arquitectura de QoS dinámica. En algunos documentos se utiliza el término RSVP+ para referirse al RSVP con estas extensiones.

El RSVP y la arquitectura de servicios integrados especifican los parámetros de QoS en términos genéricos independientes de la tecnología de la capa 2 subyacente. Es necesario precisar la forma de reflejar estas especificaciones de tráfico generales en especificaciones específicas de flujos J.112. Dicha correspondencia existe para otros protocolos de la capa 2 (por ejemplo, ATM, LAN IEEE 802.XX); en esta cláusula se describen las correspondencias establecidas para redes J.112.

La arquitectura de QoS dinámica utiliza un superconjunto de RSVP con las diferencias siguientes:

- Dado que las reservas de recursos se inician de forma independiente para cada red J.112 (modelo de asignación de recursos segmentados), esta Recomendación no exige que los mensajes de gestión de recursos se transmitan de extremo a extremo.
- El intercambio relativo a la gestión de recursos entre el MTA y el CMTS reserva recursos en ambos sentidos en la red de área local (controlada por el cliente) y en las redes J.112. Ello permite que un CMTS actúe como representante (o proxy) del punto extremo distante, una solución interesante porque reduce al mínimo el número de mensajes necesarios para la gestión de recursos en las redes J.112 de anchura de banda limitada, y reduce el retardo posterior a la marcación y después de descolgar.
- En la parte de área local de la red (controlada por el cliente) puede haber encaminadores RSVP. En este entorno es necesario hacer reservas unidireccionales. Para permitir ambas

funciones (reservas bidireccionales en la red J.112 y reservas unidireccionales en la red del cliente), el MTA envía a la puerta un mensaje PATH (trayecto) mejorado.

- La capacidad de vincular un único conjunto de recursos a un grupo de varias reservas, considerando que el MTA informa que en un momento dado sólo estará activa una de las reservas del grupo.
- Soporte de la función de activación de recursos en dos fases disponible en J.112, que permite garantizar que los recursos estarán disponibles antes de que se genere la señal de llamada en el teléfono del extremo lejano. El intercambio RSVP con el CMTS realiza la primera fase (control de admisión) y el MTA envía al CMTS un mensaje diferente para que se realice la activación.

Un sistema con calidad de servicio dinámica puede o no soportar el protocolo RSVP estándar, pero este protocolo no es suficiente. Los mensajes del protocolo RSVP estándar no activarán las operaciones de QoS dinámica que se especifican en esta Recomendación.

6.1 Descripción general de las extensiones del RSVP

6.1.1 Operación segmentada

Tal como se define en IETF RFC 2205, el RSVP está diseñado para ser ejecutado entre dos sistemas anfitriones. Sin embargo, el modelo de QoS de IPCablecom requiere que la señalización se realice de forma segmentada, entendiendo por segmento el comprendido entre un MTA y un CMTS. En esta cláusula se describe el soporte de un modelo segmentado en el RSVP.

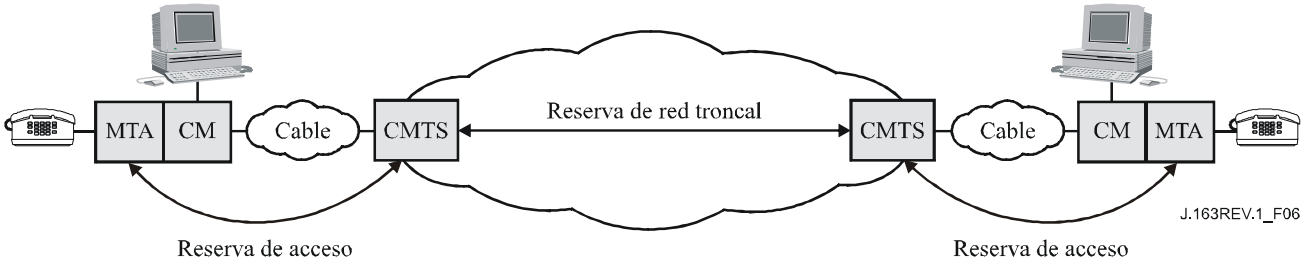


Figura 6/J.163 – Modelo de señalización segmentada

En el modelo segmentado un MTA comunica con el CMTS. Además de la situación simple ilustrada en la figura 6, esta Recomendación permite situaciones más complejas, por ejemplo la presencia de una red de cliente entre el cliente y el CM, que puede incluir diversos elementos de red, incluyendo conmutadores o encaminadores con capacidad RSVP. La presencia de una red de cliente significa que la solución funciona incluso si el cliente y el CMTS no son inmediatamente adyacentes en la capa IP. La red de cliente puede proporcionar múltiples trayectos entre el cliente y el CM, pudiendo existir en esta red rutas asimétricas.

El CMTS intercepta los mensajes RSVP enviados desde el MTA de origen hacia el MTA en el lado de terminación de la sesión a fin de implementar el modelo segmentado. Entonces sólo habrá que hacer modificaciones mínimas en el RSVP, manteniendo la dirección de destino de los mensajes PATH igual a la dirección de destino de los datos.

6.1.2 Reservas bidireccionales

El RSVP tradicional realiza reservas unidireccionales. Los mensajes PATH circulan en el mismo sentido que los datos, y los mensajes RESV circulan en sentido opuesto. Para realizar una reserva bidireccional es necesario añadir nuevos objetos RSVP para definir ambos sentidos. El CMTS responde a la petición estableciendo reservas en ambos sentidos del enlace J.112. Si existen

encaminadores RSVP entre el MTA de origen y el CM, el CMTS inicia un mensaje PATH que tiene la apariencia de un mensaje procedente del cliente distante.

6.1.3 Compresión y supresión de la cabecera y detección de actividad vocal (VAD)

Si el CMTS y el CM están configurados para realizar la compresión o la supresión de la cabecera, puede reducirse la anchura de banda necesaria para el flujo J.112. El cliente debe informar al CMTS que puede haber compresión o supresión antes de realizar una reserva, con el fin de garantizar que se ha reservado la anchura de banda apropiada. La solución general a este problema se describe en el documento del IETF sobre servicios integrados en presencia de flujos comprimibles [IETF RFC 3006].

El MTA completa la especificación del tráfico (Tspec) de emisor con un parámetro de compresión (Compression_Hint), descrito en [IETF RFC 3006] que identifica el tipo o tipos de compresión o supresión de cabecera que pueden aplicarse a los datos. Este parámetro de compresión contiene una campo de indicación que precisa el tipo o los tipos de compresión o supresión posibles, y aclara si el usuario utiliza sumas de control UDP o IP y/o IP-Ident (identificación IP); cuando no se utilizan, también se pueden comprimir o suprimir dichos campos. Si no se comprime ni se suprime ninguno de los campos de la cabecera IP, NO SE COMPRIMIRÁ NI SE SUPRIMIRÁ la suma de control IP.

Para señalar a la red J.112 la supresión de la cabecera, el CMTS utiliza los datos que proporciona el campo indicación del parámetro de compresión, para indicar el esquema de la supresión de cabecera que se realiza en este flujo J.112. Esta información se utiliza para reducir la tasa o velocidad efectiva y la profundidad o capacidad del contador de testigos del MTA. Si un enlace no soporta la supresión de cabecera, no se tiene en cuenta el parámetro indicación de compresión y se utiliza la especificación completa Tspec.

Cuando se suprime la cabecera en un enlace J.112, es necesario comunicar al CMTS el *contenido* de esta cabecera antes de la transmisión del primer paquete de datos, de forma que el contexto de la supresión pueda establecerse en el CM y el CMTS. Esta información puede ser enviada mediante el mensaje RSVP utilizado para realizar la reserva o mediante los mensajes de capa MAC enviados antes del primer paquete de datos. Como los mensajes PATH se procesan en todos los tramos intermedios entre el cliente y el CMTS, el valor de tiempo de vida (TTL, *time to live*) de un mensaje PATH entrante será el mismo de los paquetes de datos, siempre que los mensajes PATH y los paquetes de datos tengan el mismo TTL inicial cuando los envíe el MTA. Por tanto, el CMTS puede utilizar el contenido de PATH para conocer los valores de los campos que serán suprimidos. El CMTS utiliza mensajes MAC J.112 para indicar al CM que se aplica la supresión a un determinado flujo y ordenar la supresión de determinados campos dependiendo de que se incluyan o no sumas de control UDP.

El CMTS puede asimismo ordenar al CM la supresión del campo identificación IP, que sólo se utiliza cuando se realiza la fragmentación. Dado que este campo cambia en cada paquete, su valor no puede comunicarse mediante el RSVP ni enviando mensajes MAC. La supresión de este campo dependerá de la posibilidad de fragmentar ulteriormente el paquete. No es necesario que el MTA envíe al CMTS información alguna sobre la supresión de este campo; el CMTS puede decidir suprimirlo o no en función de una política local.

El mismo enfoque básico permite soportar la detección de actividad vocal (VAD, *voice activity detection*). Un CMTS puede utilizar distintos algoritmos de planificación para flujos que utilicen VAD y, por tanto, necesita saber qué flujo puede ser tratado con VAD. En el objeto de compresibilidad transportado en Tspec SE TIENE QUE incluir un valor que indique que se puede aplicar VAD al flujo de datos para el que se solicita esta reserva (no se ha hecho la detección de silencio para ese flujo en el MTA y se trata de voz, no facsímil ni datos).

6.1.4 Vinculación dinámica de recursos

El modelo de QoS dinámica exige poder modificar dinámicamente la vinculación entre recursos y flujos. Para la llamada en espera por ejemplo, puede ser conveniente retener suficientes recursos para una única sesión en la red J.112 transfiriendo la asignación de tales recursos de un llamante a otro. Aunque se había propuesto esta capacidad, no se incluyó en la versión 1 del protocolo RSVP.

En RSVP, el "alias" para un conjunto de recursos reservados es el objeto Sesión. Dado que la sesión contiene la dirección de destino del flujo, habrá que modificar el objeto Sesión para reasignar recursos a un flujo con una dirección de destino distinta. La dirección de fuente del flujo puede modificarse mediante una nueva especificación de filtro en el mensaje RESV.

Esta funcionalidad se ha integrado añadiendo un objeto identificador de recurso (Resource-ID) a los mensajes RSVP. Los encaminadores, que entienden el significado de este objeto, intentan utilizar los recursos asociados con dicho identificador. El objeto ID de recurso es un identificador opaco generado por el nodo que controla los recursos (en este caso el CMTS).

Véase la figura 7. Si el MTA incluye el ID de recurso en la petición de reserva para un nuevo flujo, está indicando al CMTS que la sesión puede compartir recursos para esta nueva puerta (puerta 2) con una puerta creada anteriormente (puerta 1). Si la QoS solicitada para la nueva puerta puede conseguirse con una asignación de anchura de banda igual o inferior a la de la puerta existente, no se reserva anchura de banda adicional en la red J.112. No obstante, puede ser necesario reservar anchura de banda en la red troncal dependiendo del trayecto extremo a extremo de la nueva sesión. El acceso a la reserva compartida es mutuamente excluyente: un MTA debe emitir un mensaje de compromiso para indicar al CMTS cuál es el flujo activo, y dicho compromiso elimina explícitamente los recursos comprometidos para el otro. En el ejemplo de la llamada en espera, el cliente envía un mensaje de compromiso al CMTS para identificar el flujo actualmente activo cuando el usuario pasa de una sesión a otra.

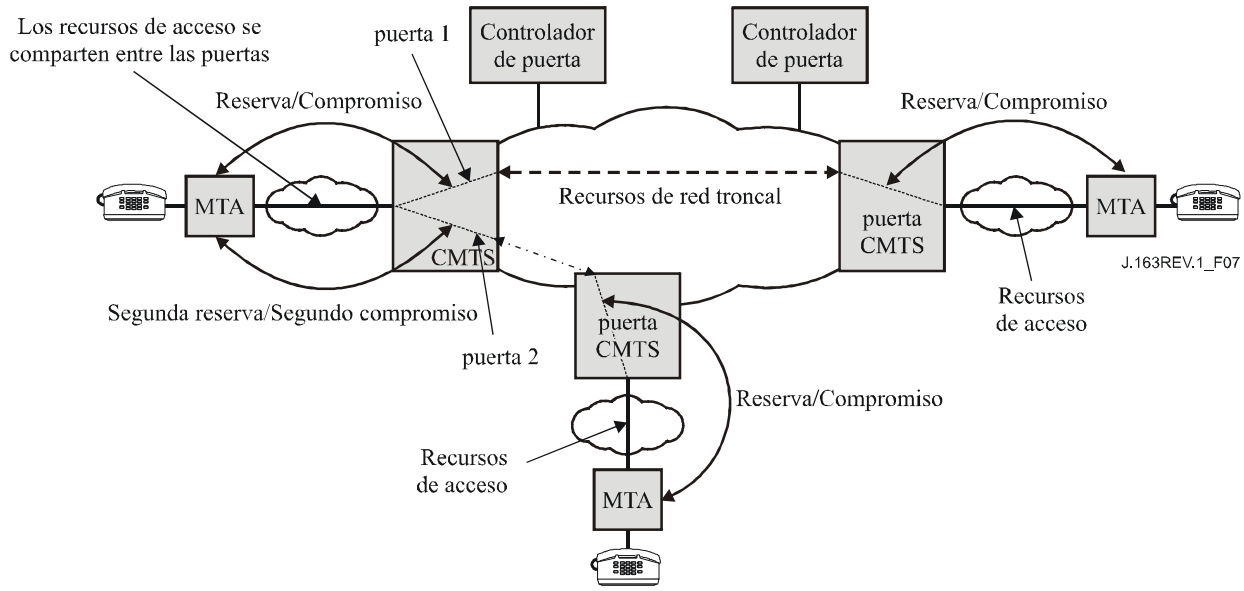


Figura 7/J.163 – Compartición de las reservas de recursos entre puertas

En el modelo segmentado, el CMTS incluye el ID de recurso en el primer mensaje RESV que envía al MTA, y el MTA puede incluir este ID en los siguientes mensajes que hagan referencia a los recursos en cuestión. Lo que es más importante, el MTA que desea establecer una nueva sesión y reutilizar los recursos de una sesión existente incluye el ID de recurso asociado con la sesión anterior en el mensaje PATH que envía al CMTS. Un mensaje PATH que contenga el identificador de un conjunto de recursos actualmente asignado añade una nueva vinculación entre un flujo

(definido en los objetos Sesión y Plantilla de emisor) y dichos recursos. Facultativamente, puede modificar la cantidad de recursos atribuidos mediante la inclusión de Tspec y Rspec distintas a las previamente recibidas por el CMTS para este conjunto de recursos. Puede añadir un nuevo conjunto de Tspec y de Rspec para incluir múltiples códecs tal como se describe en 6.2.

El RSVP permite modificar la magnitud de una reserva con el tiempo. Una reserva que no sea mayor que otra que ya se encuentre instalada (es decir, que no requiera un mayor nivel de recursos para algunos de los dos sentidos de la sesión) NO SERÁ RECHAZADA en el control de admisión. La misma regla se aplica cuando se utiliza el objeto ID de recurso. Si la cantidad de recursos solicitada en la nueva reserva no es superior a la previamente instalada, la reserva NO SERÁ RECHAZADA en el control de admisión.

Un encaminador que no pueda interpretar este nuevo objeto (por ejemplo, en la red del cliente) intentará simplemente instalar lo que parece ser una nueva reserva sin reutilizar recursos previamente atribuidos. Probablemente no habrá problemas porque la anchura de banda disponible en la red propia local seguramente no será inferior a la anchura disponible en la red J.112. La reserva anterior expira si no se renueva. En caso de insuficiencia de recursos en la red del cliente habrá que actualizar los encaminadores en la red propia para que soporten este nuevo objeto. Obsérvese que siempre es recomendable intentar realizar reservas en la red del cliente, aunque la anchura de banda en la misma sea relativamente abundante, ya que la reserva proporciona a los dispositivos de la red del cliente la información necesaria para evitar que determinados flujos sufran un retardo y una fluctuación excesivos que podrían experimentar si se combinaran en una cola común con tráfico de servicios manejados con el criterio del mejor esfuerzo (o con flujos reservados que tengan características de tráfico muy diferentes).

6.1.5 Proceso de reserva/compromiso en dos etapas

Un aspecto significativo del modelo de QoS dinámica de IPCablecom es el proceso de reserva en dos fases: la reserva y el compromiso. El protocolo RSVP se utiliza para la fase de reserva, de forma que el CMTS no proporciona realmente los recursos hasta la segunda etapa del proceso.

Debido a que en la fase de compromiso sólo participan un MTA y una puerta local, se realiza mediante un mensaje unidifusión desde el MTA al CMTS. El MTA conoce cuál es el ID de puerta gracias al protocolo de señalización.

6.1.6 Autenticación

El proveedor puede garantizar que las partes no reservan recursos de red no autorizados. El RSVP proporciona una serie de mecanismos para ello, tales como los objetos integridad de RSVP y datos de políticas incluidos en otros mensajes RSVP. La especificación de QoS dinámica incluye un ID de puerta entre los datos de políticas, que ES OBLIGATORIO incluir en los mensajes RSVP-PATH.

6.2 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 J.112, 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 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 las cabeceras 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.

6.2.1 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.

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 6.2 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

6.2.2 Reflejar los códecs PacketCable en peticiones DQoS RSVP

Es necesario utilizar el siguiente perfil DQoS del mecanismo DOCSIS 1.1 de QoS para soportar servicios vocales. Dado que los códecs IPCablecom definidos (conforme a la Rec. UIT-T J.161) se transportan en trenes de datos de velocidad binaria constantes, ES OBLIGATORIO aplicar las siguientes reglas de creación de mensajes DQoS:

Los parámetros del *RSVP Capacidad del contador* (b), *Tamaño máximo del datagrama* (M) y *Mínima unidad supervisada* (m) TIENEN QUE ser iguales.

Los parámetros del *RSVP Tasa del contador* (r), *Tasa máxima* (p) y *Tasa reservada* (R) TIENEN QUE ser iguales.

El *término de inactividad del RSVP* TIENE QUE ser un valor proporcionado por el CMS. Si el CMS no lo proporciona, se TIENEN QUE utilizar los valores de 800 microsegundos para el flujo ascendente y cero para el flujo descendente.

El *Protocolo RSVP* SE TIENE QUE definir como UDP.

La *dirección de destino del RSVP* TIENE QUE ser la dirección IP a la que se van a enviar los paquetes del tren de datos, si se conoce esta dirección en el sentido de utilización del parámetro. Si se desconoce, SE TIENE QUE utilizar el valor cero en este campo.

El *puerto de destino del RSVP* TIENE QUE ser el puerto UDP al que se van a enviar los paquetes del tren de datos, si se conoce esta dirección en el sentido de utilización del parámetro. Si se desconoce, SE TIENE QUE utilizar el valor cero en este campo.

La *dirección de fuente del RSVP* TIENE QUE ser la dirección IP desde la que se van a enviar los paquetes del tren de datos, si se conoce esta dirección en el sentido de utilización del parámetro. Si se desconoce, SE TIENE QUE utilizar el valor cero en este campo.

El *puerto de fuente del RSVP* TIENE QUE ser el puerto UDP desde el que se van a enviar los paquetes del tren de datos, si se conoce esta dirección en el sentido de utilización del parámetro. Si se desconoce, SE TIENE QUE utilizar el valor cero en este campo.

Si una entidad recibe un mensaje DQoS que no es conforme a las reglas de esta especificación, TIENE QUE rechazarlo de forma definitiva.

6.2.3 Reflejar las especificaciones de flujo RSVP en parámetros de QoS J.112

Al recibir una petición de reserva, el CMTS decide:

- el tipo de servicio J.112 que se ha de utilizar; por ejemplo, autorización sin petición, interrogación en tiempo real, etc.;
- los parámetros de QoS que se han de asociar al flujo de servicio correspondiente.

Condiciones que se aplican a los objetos del RSVP en los dos sentidos:

Tspec del emisor y *Tspec del emisor hacia atrás*:

Capacidad del contador (b), bytes = tamaño del datagrama VoIP, inclusive la tara de cabecera IP/UDP/RTP.

Tasa del contador (r), bytes/segundo = tasa de datos efectiva, inclusive la tara de cabecera IP/UDP/RTP.

Tamaño máximo del datagrama (M), bytes = capacidad del contador (b).

Mínima unidad supervisada (m), bytes = capacidad del contador (b).

Tasa máxima (p), bytes/segundo = tasa del contador (r).

RSpec del emisor y *Rspec del emisor hacia atrás*:

- *Tasa reservada (R)*, bytes/segundo = tasa del contador (r).

- *Término de inactividad (s),* microsegundos = fluctuación de autorización tolerada para el flujo ascendente y tiempo de espera tolerado para el flujo descendente[3]. Es un valor $0 \leq s \leq 2 \times$ intervalo de paquetización o un valor por defecto de 800 microsegundos para flujos ascendentes, y $50 \leq s \leq 2 \times$ intervalo de paquetización o un valor por defecto de cero para flujos descendentes, si el CMTS no especifica estos valores al MTA. En el sentido descendente, cero significa que no hay limitación de tiempo de espera.

Sesión y *Sesión hacia atrás*:

Protocolo = UDP.

Dirección de destino = dirección IP a la que se han de enviar los paquetes del tren de datos.

Puerto de destino = puerto UDP al que se han de enviar los paquetes del tren de datos.

Plantilla de emisor y *Plantilla de emisor hacia atrás*:

Dirección de fuente = dirección IP desde la que se han de enviar los paquetes del tren de datos.

Puerto de fuente = puerto UDP desde el que se han de enviar los paquetes del tren de datos.

ES OBLIGATORIO utilizar los mismos valores cuando se comprometen los recursos.

6.2.3.1 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.

El parámetro *DOCSIS Autorizaciones por intervalo* TIENE QUE ser 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 $2 \times$ intervalo de paquetización. Si el CMS no lo especifica, se utilizará un valor por defecto de 800 microsegundos.

---

[3] Este valor depende del tiempo de espera extremo a extremo previsto para una llamada; el CMS puede especificar un valor basado en información de encaminamiento (por ejemplo, tiempo de transmisión hasta el destino).

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) de la cabecera MAC de DOCSIS hasta el final de la verificación de redundancia cíclica (CRC). Este valor incluye una tara de 18 bytes de cabecera 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 cabecera MAC DOCSIS, que se compone de la cabecera básica DOCSIS (6 bytes), la cabecera ampliada UGS (3 bytes) y cabecera ampliada BPI+ (5 bytes). Si se ha activado la supresión de cabecera de cabida útil (PHS), NO SE INCLUIRÁ el número de bytes suprimidos. La cabecera ampliada suprimida PHS (2 bytes) NO SE INCLUIRÁ para flujos de servicio UGS o UGS/AD porque la información pertinente aparece en la cabecera ampliada UGS.

Tamaño de autorización sin petición DOCSIS^8,9 = M + 32-PHS[4,5]

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.

6.2.3.2 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.

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.

---

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

5 La supresión de cabecera (PHS) de este ejemplo está definida en la especificación DOCSIS RFI, cláusula B.C.2.2.10.4 del anexo B a J.112.

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.

6.2.3.3 Codificación para supresión de cabecera de cabida útil

Peticiones DOCSIS para supresión de cabecera de cabida útil (PHS)

La supresión de cabecera 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 cabecera de cabida útil* indica los bytes de las cabeceras que la entidad emisora TIENE QUE suprimir, y la entidad receptora TIENE QUE restablecer.

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

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

El parámetro *DOCSIS Verificación supresión de cabecera 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 cabecera 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 cabecera 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 cabecera" en los códigos DOCSIS de supresión de cabecera de cabida útil, así como el parámetro de error DOCSIS descrito más adelante. NO SE UTILIZARÁ el mensaje de error DOCSIS.

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

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

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

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

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

Al recibir un código de confirmación "rechazar supresión de cabecera" que tiene un parámetro con errores DOCSIS que incluye la máscara de supresión de cabecera de cabida útil DOCSIS, el E-MTA PUEDE hacer una nueva petición sin supresión de cabecera de cabida útil DOCSIS, o

PUEDE redefinir la máscara de supresión de cabecera 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 cabecera" que tiene un parámetro con errores DOCSIS que incluye el tamaño de supresión de cabecera de cabida útil DOCSIS, el E-MTA PUEDE hacer una nueva petición de ancho de banda sin supresión de cabecera de cabida útil DOCSIS.

Cómo utiliza el E-MTA la cabecera ampliada DOCSIS UGS

El parámetro DOCSIS Índice de supresión de cabecera de cabida útil TIENE QUE ser el índice predefinido de PHS, o cero cuando no se ha definido ninguna supresión de cabecera 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 parámetro DOCSIS Autorizaciones activas SE TIENE QUE poner a uno cuando el E-MTA no está en supresión de silencio, y SE TIENE QUE poner a cero cuando el E-MTA está en supresión de silencio para el códec que se utiliza para el tren de datos asociado con este flujo de servicio.

6.2.3.4 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 de la cabecera 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:

$$\text{Tamaño mínimo previsto de paquetes a la velocidad reservada DOCSIS} = m + 18 - PHS$$

El parámetro *DOCSIS Velocidad de tráfico máxima sostenida*[6] 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 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:

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

El parámetro DOCSIS *Velocidad de tráfico mínima reservada*[6] 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).

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

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.

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

---

6 Los valores con cifras decimales se redondean.

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.

6.2.3.5 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 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 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.

6.2.3.6 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.

6.2.3.7 Supresión de la cabecera de la cabida útil y detección de actividad vocal

Si el CMTS y el CM suprimen la cabecera puede reducirse la anchura de banda necesaria para un flujo de servicio. Antes de hacer una reserva el cliente TIENE QUE informar al CMTS que es posible suprimir la cabecera, para determinar correctamente la anchura de banda reservada. La solución general a este problema se describe en IETF RFC 3006. El emisor (cliente) añade a la Tspec del emisor un parámetro indicación de compresión (*Compression_Hint*) descrito en IETF RFC 3006, que identifica el tipo de compresión o supresión de cabecera que puede aplicarse a los datos. El parámetro Compression_Hint contiene un campo que informa del tipo o tipos de compresión posibles.

Si un MTA quiere que el CM suprima la cabecera, TIENE QUE incluir en la Tspec el parámetro Compression_Hint IETF RFC 3006. En el campo Factor de compresión, un porcentaje entre 1 y 100 inclusive, SE TIENE QUE dar un valor que suponga un ahorro de anchura de banda cuando se utilice la supresión de cabecera (42 bytes). El valor del factor de compresión varía en relación con el perfil de tráfico del CÓDEC. El valor de la indicación TIENE QUE ser uno de los siguientes, dependiendo del tipo o tipos de compresión/supresión que desee el MTA:

0x40090001 No se suprime la suma de control del UDP ni el campo identificación IP ni el campo suma de control IP.

0x40090002 No se suprime la suma de control del UDP, pero sí los campos identificación IP y suma de control IP.

0x40090003 Se suprime la suma de control del UDP, pero no el campo identificación IP ni el campo suma de control IP.

0x40090004 Se suprime la suma de control del UDP y los campos identificación IP y suma de control IP.

Téngase presente que la supresión del campo identificación IP generará problemas si el paquete se fragmenta ulteriormente en la red IP. Para paquetes de longitud inferior a 576 bytes (valor por defecto de MAX-MTU en Internet), puede suponerse que no habrá fragmentación. El MTA NO DEBERÍA solicitar la supresión del campo identificación IP si va a enviar paquetes de longitud superior a 576 bytes.

Un CMTS que esté conectado a un CM capaz de realizar la supresión de cabecera utiliza el parámetro Compression_Hint [IETF RFC 3006] para reducir la velocidad efectiva y la capacidad del contador de testigos que suministra el emisor. Si un enlace no soporta la supresión de cabecera, se ignora el parámetro Compression_Hint y se utiliza la Tspec completa.

Cuando se suprime la cabecera en un enlace J.112 también es necesario comunicar al CMTS, antes de la transmisión del primer paquete de datos, el contenido de la cabecera que se va a suprimir para poder establecer el contexto de supresión en el CM y el CMTS. Toda esta información se presenta en el mensaje RSVP utilizado para establecer la reserva, incluyendo los puertos y las direcciones IP de fuente y de destino. Dado que los mensajes PATH se procesan en los tramos intermedios entre el cliente y el CMTS, el valor de tiempo de vida (TTL) de un mensaje PATH entrante será el mismo de los paquetes de datos, siempre que el TTL inicial de los mensajes PATH y los paquetes de datos sea el mismo cuando son enviados por el cliente. El CMTS TIENE QUE utilizar el contenido de PATH para conocer los valores de los campos que serán suprimidos. El CMTS TIENE QUE utilizar mensajes MAC J.112 para señalar al CM que debe aplicarse la supresión a un determinado flujo y

darle indicaciones para suprimir determinados campos en función de la presencia o ausencia de la suma de control del UDP y de los números de secuencia IP.

Si el MTA inicia un mensaje PATH especificando libertad de elección del emisor, no puede determinarse con exactitud el contenido del campo PHS. El CMTS TIENE QUE especificar el tamaño de PHS para que el CM pueda evaluar con precisión las necesidades de recursos del flujo de servicio.

El mismo principio básico permite soportar la detección de actividad vocal (VAD). Como un CMTS puede utilizar diferentes algoritmos de planificación para flujos que utilicen VAD, necesita saber cuáles son los flujos que deben tratarse con VAD. El parámetro Indicación de compresión incluido en la Tspec TIENE QUE incluir el bit bandera que indica que el flujo de datos para el que se ha solicitado esta reserva puede ser tratado con VAD.

6.2.4 Autorización y comportamiento de UGS y UGS/AD

Como el controlador de puerta (GC) no especifica el tipo de planificación de flujos de servicio J.112 en el caso de la DQoS, se han establecido directrices específicas para su utilización.

Para una sesión normal:

- El CMTS debería seleccionar el tipo de planificación del flujo de servicio UGS o UGS/AD para un MTA autónomo, utilizando el RSVP y basándose en el parámetro Indicación de compresión VAD. Puede definir parámetros que se configuran para controlar la decisión.

Si la reserva abarca distintas especificaciones de flujo (mínimo valor superior):

- Si se indica VAD en los mensajes RSVP, el CMTS debería crear un tipo de planificación del flujo de servicio UGS/AD. El CMTS también puede definir parámetros que se configuran para controlar la decisión.

Si los recursos se han de compartir entre los flujos:

- El CMTS tiene que utilizar el mismo tipo de planificación del flujo de servicio para todos los recursos compartidos en los mensajes RSVP. Por tanto, el MTA tiene que solicitar los mismos valores para VAD. El CMTS rechazará las peticiones de compartición de recursos si los valores VAD no coinciden con el flujo existente.

6.2.5 Autorización y comportamiento del CMTS

Al recibir una solicitud de reserva o compromiso de ancho 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 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).

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 ancho de banda sin bloque de autorización, el CMTS TIENE QUE rechazarla con el código de error "Autorización denegada definitivamente".

Si el CMTS no encuentra ninguna puerta asociada al GateID, TIENE QUE transmitir un código de error para indicar que se ha denegado la autorización y la petición será rechazada definitivamente.

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 6.2.

Tspec de emisor y *Tspec de emisor hacia atrás*:

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.

La mínima unidad supervisada en 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.

Rspec de emisor y *Rspec de emisor hacia atrás*:

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.

Sesión y *Sesión hacia atrás*:

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.

Plantilla de emisor y *Plantilla de emisor hacia atrás*:

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.

6.3 Definición de objetos RSVP adicionales

ES OBLIGATORIO añadir varios objetos RSVP nuevos al mensaje PATH original enviado por el MTA. Todos los objetos nuevos tienen un número de clase con los dos bits de orden superior puestos a uno, lo que significa que los nodos RSVP que no reconozcan estos objetos deben reenviarlos sin modificación. En esta cláusula se define el formato de varios objetos nuevos que se deben transportar en los mensajes RSVP. Todos los objetos utilizan el esquema de codificación TLV de RSVP (RFC 2205 del IETF).

6.3.1 Rspec hacia atrás (Reverse Rspec)

Objeto de Rspec hacia atrás: Clase = 226, Tipo C = 1.

Longitud (= 24)		Clase (= 226)	Tipo C (= 1)
0 (a)	Reservado	4 (b)	
2 (c)	0 Reservado	3 (d)	
130 (e)	0 (f)	2 (g)	
Velocidad [R] (número IEEE de 32 bits con coma flotante)			
Término de inactividad [S] (entero de 32 bits)			

(a) – Número de versión del mensaje (0).

(b) – Longitud total (4 palabras sin contar la cabecera).

(c) – Cabecera de servicio, número de servicio 2 (Garantizado).

(d) – Longitud de datos del servicio 1 (tres palabras sin contar la cabecera).

(e) – ID del parámetro, parámetro 130 (Rspec de servicio garantizado).

(f) – Banderas de parámetro 130 (ninguna puesta a uno).

(g) – Longitud del parámetro 130 (dos palabras sin contar la cabecera).

Véase la explicación de los campos en el documento IETF RFC 2210.

Las especificaciones hacia atrás (Reverse-Rspec) son para datos enviados por el cliente (sentido ascendente en una red J.112). Se indica en el mensaje PATH enviado por el cliente y se convierte en el objeto de especificaciones hacia adelante (Forward-Rspec) en el mensaje RESV que el CMTS produce actuando como representante del punto extremo distante.

6.3.2 Sesión hacia atrás (Reverse-Session)

Objeto sesión hacia atrás IPv4:

Longitud (= 12)		Clase (= 226)	Tipo C (= 2)
Dirección de destino IPv4 (4 bytes)			
ID Protocolo	Banderas	Puerto de destino	

El objeto sesión hacia atrás describe la información de destino del tren de datos que debe recibir el MTA (en sentido descendente en la red J.112) y se convierte en el objeto sesión del mensaje PATH que el CMTS produce actuando como representante del punto extremo distante.

6.3.3 Plantilla de emisor hacia atrás (Reverse-Sender-Template)

Objeto plantilla de emisor hacia atrás IPv4:

Longitud (= 12)	Clase (= 226)	Tipo C (= 3)
Dirección de fuente IPv4 (4 bytes)		
Reservado	Reservado	Puerto fuente

El objeto plantilla de emisor hacia atrás describe la información de fuente del tren de datos que debe recibir el MTA (descendente en la red J.112). Se convierte en el objeto plantilla de emisor del mensaje PATH que el CMTS produce actuando como representante del punto extremo distante.

6.3.4 Tspec de emisor hacia atrás (Reverse-Sender-Tspec)

Objeto Tspec de emisor hacia atrás: son los mismos campos de Tspec de emisor, descritos en RFC 3006.

Longitud (= 48)		Clase (= 226)	Tipo C (= 4)
0 (a)	Reservado	10 (b)	
1 (c)	0 Reservado	9 (d)	
127 (e)	0 (f)	5 (g)	
Tasa del contador de testigos [r] (número IEEE de 32 bits con coma flotante)			
Tamaño del contador de testigos [b] (número IEEE de 32 bits con coma flotante)			
Máxima velocidad de datos [p] (número IEEE de 32 bits con coma flotante)			
Mínima unidad supervisada [m] (entero de 32 bits)			
Tamaño máximo de paquete [M] (entero de 32 bits)			
126 (h)	banderas (i)	2 (j)	
Indicación (número asignado) (k)			
Factor de compresión (entero de 32 bits) (l)			

(a) – Número de versión del formato del mensaje (0).

(b) – Longitud total (10 palabras, sin incluir la cabecera).

(c) – Cabecera de servicio, número del servicio 1 (información por defecto/global).

(d) – Longitud de los datos del servicio 1 (nueve palabras sin incluir la cabecera).

(e) – ID del parámetro, parámetro 127 (Token_Bucket_Tspec).

(f) – Banderas del parámetro 127 (ninguna puesta a uno).

(g) – Longitud de parámetro 127 (cinco palabras sin incluir la cabecera)

(h) – ID del parámetro, parámetro 126 (Compression_Hint).

(i) – Banderas del parámetro 126 (ninguna puesta a uno).

(j) – Longitud del parámetro 126 (dos palabras sin incluir la cabecera)

(k) – Valor de indicación definido para la supresión de cabecera J.112 (por determinar).

0x????0001 No suprimir la suma de control UDP NI el campo identificación IP NI el campo suma de control IP.

0x????0002 No suprimir la suma de control UDP Y suprimir los campos identificación IP y suma de control IP.

0x????0003 Suprimir la suma de control UDP Y no suprimir el campo identificación IP ni el campo suma de control IP.

0x????0004 Suprimir la suma de control UDP Y los campos identificación IP y suma de control IP

NOTA – ???? significa número por determinar; asignación de numeración del IANA para IPCablecom.

(l) – Valor del factor de compresión – porcentaje de reducción en el tamaño de los paquetes como consecuencia de la supresión de la cabecera J.112. Nótese que varía en función del CÓDEC utilizado. Véase la explicación de los campos en IETF RFC 2210.

El objeto Tspec de emisor hacia atrás describe el flujo de datos que debe enviar el MTA (ascendente en la red J.112). Se convierte en el objeto Tspec de emisor del mensaje PATH que el CMTS produce actuando como representante del punto extremo distante.

6.3.5 Rspec hacia adelante (Forward-Rspec)

Objeto Forward-Rspec hacia adelante:

Longitud (= 24)		Clase (= 226)	Tipo C (= 5)
0 (a)	Reservado	4 (b)	
2 (c)	0 Reservado	3 (d)	
130 (e)	0 (f)	2 (g)	
Velocidad [R] (número IEEE de 32 bits con coma flotante)			
Término de inactividad [S] (entero de 32 bits)			

Véase la definición de estos campos en Rspec hacia atrás, véase 6.3.1.

Rspec hacia adelante se aplica a los datos transmitidos hacia el cliente (sentido descendente en la red J.112). Este objeto aparece en un mensaje PATH enviado por el cliente, y su contenido se incorpora en el objeto especificación de flujo (Flowspec) del mensaje RESV devuelto.

6.3.6 Identificador de recurso (Resource-ID)

Objeto identificador de recurso:

Longitud (= 8)	Clase (= 226)	Tipo C (= 7)
ID de recurso (entero de 32 bits)		

El objeto ID de recurso se devuelve al MTA en un mensaje RESV y contiene el identificador que se utilizará para ulteriores modificaciones de recursos. También se incluye en los mensajes PATH enviados por el MTA para solicitar la compartición de recursos entre varias sesiones.

6.3.7 Identificador de puerta (Gate-ID)

Objeto identificador de puerta:

Longitud (= 8)	Clase (= 226)	Tipo C (= 8)
ID de puerta (entero de 32 bits)		

El objeto ID de puerta se incluye en los mensajes PATH del MTA para identificar la autorización del recurso adecuado en el CMTS.

6.3.8 Entidad para compromiso (Commit-Entity)

Objeto entidad para compromiso IPv4:

Longitud (= 12)	Clase (= 226)	Tipo C (= 9)
Dirección de destino IPv4 (4 bytes)		
Reservado	Puerto de destino	

El objeto entidad para compromiso se comunica en un mensaje RESV de retorno del CMTS para indicar la dirección de destino y el número de puerto al que el MTA debe enviar el mensaje COMMIT.

6.3.9 Clase D (DClass)

Objeto Clase D:

Longitud (= 8)		Clase (= 225)	Tipo C (= 1)
No utilizado	No utilizado	No utilizado	DSCP

El objeto Clase D se comunica en un mensaje RESV de retorno del CMTS para indicar el DSCP que el MTA DEBERÍA utilizar cuando envíe al CMTS paquetes de datos en relación con esta reserva. La utilización del objeto Clase D se describe en un documento específico sobre utilización y formato del objeto DCLASS con señalización RSVP [IETF RFC 2996].

6.4 Definición de mensajes RSVP

En esta cláusula se definen los mensajes RSVP mejorados que el MTA TIENE QUE generar y que el CMTS TIENE QUE soportar.

Los mensajes RSVP SE TIENEN QUE enviar como datagramas IP "indeterminados" (*raw*) con número de protocolo 46. El mensaje RSVP-PATH TIENE QUE tener la opción Aviso de encaminador (RouterAlert) IETF RFC 2113 en la cabecera IP. Cada mensaje RSVP TIENE QUE ocupar exactamente un datagrama IP.

Todos los mensajes RSVP TIENEN QUE constar de una cabecera común, seguida de un número variable de objetos de longitud variable. La cabecera común TIENE QUE tener la siguiente estructura:

Versión	Banderas	Tipo de mensaje	Suma de control RSVP
TTL enviado		(Reservado)	Longitud del mensaje RSVP

Los valores de cada campo TIENE QUE ser los especificados en IETF RFC 2205.

Todos los objetos SE TIENEN QUE formar con una o más palabras de 32 bits, con una cabecera de una palabra y el formato siguiente:

Longitud en bytes	Número de clase	Tipo C
Contenido del objeto …		

Los valores de cada campo TIENE QUE ser los especificados en IETF RFC 2205.

El formato del mensaje RSVP-PATH y del mensaje RSVP-RESV conformes a esta Recomendación TIENE QUE contener los objetos siguientes (los elementos en cursiva se definen en esta Recomendación, los restantes en IETF RFC 2205 y/o IETF RFC 2210). En el caso de los objetos

que no se definen en esta Recomendación, SE TIENEN QUE aplicar las reglas de ordenación de objetos de IETF RFC 2205. No existen requisitos de ordenación para los objetos <Resource-ID>, <Gate-ID>, y <Commit-Entity>. <Reverse-Rspec> y <Downstream-Flowspec> TIENEN QUE aparecer después del objeto <Sender-Tspec>. Para los objetos definidos en <Downstream-Flowspec> y <Component-Item> SE TIENE QUE aplicar el siguiente orden de lenguaje BNF:

<PATH-Message> ::=Common-Header> [<Integrity-Object>]
<Session-Object> <RSVP-Hop> <Time-Values>
<Policy-Data> …] <Sender-Template>
Sender-Tspec> <*Reverse-Rspec*>
Downstream-Flowspec> [<*Resource-ID*>]
Gate-ID>

<*Downstream-Flowspec*> *::=* <*Reverse-Session*> <*Reverse-Sender-Template*>
<*Reverse-Sender-Tspec*><*Forward-Rspec*>

<RESV-Message> ::= <Common-Header> [<Integrity-Object>]
<Session-Object> <RSVP-Hop> [<DClass>]
Time-Values> [<RESV-Confirm>] [<Scope>]
<Policy-Data> …] <*Resource-ID*>
Commit-Entity> <Style> <Flowspec>
Filter-Spec>

Las componentes de estos mensajes se describen en las cláusulas siguientes.

6.4.1 Objetos de mensajes para hacer una reserva en sentido ascendente

Un mensaje RSVP-PATH estándar contiene, como mínimo, los objetos siguientes:

<Session> <RSVP-Hop> <Time-Values> <Sender-Template> <Sender-Tspec>

Sin embargo, en el modelo segmentado hay que proporcionar al CMTS toda la información que necesita para hacer una reserva bidireccional en el enlace J.112. También hay que permitirle enviar al MTA un mensaje RSVP-RESV. Un mensaje RSVP-RESV estándar contiene, como mínimo, los objetos siguientes:

<Session> <RSVP-Hop> <Time-Values> <Style> <Flowspec> <Filter-Spec>

El CMTS TIENE QUE enviar este mensaje al MTA después de recibir de él un mensaje RSVP-PATH. El único objeto que no puede obtenerse a partir de RSVP-PATH o de información local es la especificación de flujo (Flowspec). El objeto especificación de filtro (Filter-Spec), que consta de la dirección IP y el puerto de fuente que debe utilizar el MTA, aparece en la plantilla de emisor (Sender-Tspec) del mensaje PATH. Casi todos los elementos de Flowspec aparecen en Sender-Tspec en el mensaje PATH. Las excepciones son los valores de velocidad reservada (R) e inactividad (S), que conjuntamente constituyen Rspec. Por lo tanto, el MTA proporciona una Rspec adecuada que incluye los valores de R y S para el servicio garantizado, y que se codifica conforme a IETF RFC 2210. Se comunica en un objeto Rspec hacia atrás (Reverse-Rspec) descrito en 6.3.1.

6.4.2 Objetos del mensaje para reserva descendente

El MTA TIENE QUE proporcionar suficiente información para permitir que el CMTS construya un mensaje RSVP-PATH para el flujo de datos descendente, habiendo recibido un mensaje RSVP-PATH para el flujo de datos ascendente. Esto significa que el MTA DEBE proporcionar los objetos siguientes relacionados con el flujo de datos descendente (CMTS→MTA).

<Session> <Sender-Template> <Sender-Tspec>

Estos objetos tienen definiciones RSVP normales y se aplican al tren de datos símplex que se transmite desde el punto extremo distante hacia el MTA. En el mensaje RSVP-PATH que envía el MTA se les asignan nuevos códigos de objeto (tal como se ha señalado anteriormente) y nuevos nombres: sesión hacia atrás, plantilla de emisor hacia atrás, Tspec de emisor hacia atrás. El objeto sesión hacia atrás TIENE QUE incluir la dirección IP del MTA, el tipo de protocolo y el puerto (en su caso) en el que va a recibir los datos de este flujo. La plantilla de emisor hacia atrás TIENE QUE incluir la dirección IP del punto extremo distante, o bien todos ceros para indicar elección libre de la fuente. La plantilla de emisor hacia atrás TIENE QUE incluir el número de puerto (en su caso y si se conoce), o cero. Tspec de emisor hacia atrás TIENE QUE incluir la información Tspec que describe el flujo de datos desde el punto extremo distante. El CMTS TIENE QUE utilizar su propia dirección como valor de tramo RSVP y elegir un valor en el campo de tiempo para indicar la frecuencia de renovación del mensaje RSVP-PATH. Aunque el CMTS no necesite generar el mensaje RSVP-PATH y enviarlo al MTA, esa información es necesaria para poder realizar una reserva y crear clasificadores de paquetes en sentido descendente.

Además de esta información, el único elemento de información adicional que el CMTS necesita para hacer una reserva en el sentido descendente es Rspec. Como en los otros casos, se le asigna un nuevo objeto y un nuevo nombre: Rspec hacia adelante (Forward-Rspec). Contiene los mismos elementos de información y se codifica de la misma forma que una Rspec convencional.

Obsérvese que Forward-Rspec se aplica a los datos transmitidos hacia el MTA, lo cual significa que el MTA lo envía en el mismo sentido que el mensaje RSVP-RESV que normalmente transportaría esta información. Se incluye en el mensaje RSVP-PATH como una forma de optimización que reduce el retardo de establecimiento. El MTA envía Reverse-Rspec en el sentido opuesto al RSVP-RESV que normalmente transportaría esta información.

6.5 El procedimiento de reserva

En esta cláusula se describen las acciones del MTA y el CMTS para reservar recursos conjuntamente.

Para los fines de este análisis, el punto extremo que se encuentra en comunicación directa con el CMTS es el cliente, y el otro punto extremo de la sesión se denomina punto extremo distante. No se precisa el tipo de dispositivo (pasarelas, computadoras, clientes integrados). Se supone que el cliente utiliza RSVP para comunicar sus peticiones de QoS al CMTS, y no se precisan las capacidades del punto extremo distante. El flujo de datos desde el cliente hacia el CMTS se denomina ascendente, y el flujo de datos desde el CMTS al cliente descendente.

6.5.1 Establecimiento de la reserva

Procedimiento RSVP en el caso del modelo segmentado:

El cliente TIENE QUE enviar un mensaje RSVP-PATH hacia el punto extremo distante de la sesión y ese mensaje TIENE QUE ser interceptado por el CMTS. Así se inicia el proceso de reserva de anchura de banda en sentido ascendente y descendente. Cuando es necesario hacer reservas en ambos sentidos, el mensaje RSVP-PATH TIENE QUE incluir información sobre las necesidades de recursos en sentido ascendente (Reverse-Rspec) y descendente (Reverse-Sender-Tspec, Forward-Rspec).

El CMTS TIENE QUE comprobar si la cantidad de recursos solicitados está dentro de los límites autorizados para la sesión, y si dispone de suficientes recursos locales para aceptar la reserva. Si el resultado es positivo hace la reserva de los recursos ascendentes y descendentes y TIENE QUE emitir los mensajes de nivel MAC J.112 para asignar los recursos adecuados en el enlace J.112.

El CMTS TIENE QUE establecer clasificadores para los flujos ascendente y descendente. El clasificador ascendente TIENE QUE incluir la dirección IP de fuente del cliente y el número de puerto del objeto Plantilla de emisor. El clasificador ascendente TIENE QUE incluir el tipo de

protocolo, la dirección IP de destino y el número de puerto del objeto Sesión. Si se incluye el objeto Plantilla de emisor hacia atrás (Reverse-Sender-Template) y contiene una dirección distinta de 0.0.0.0, el clasificador descendente TIENE QUE incluirla como dirección IP de fuente. Si se incluye la plantilla de emisor hacia atrás y contiene un número de puerto distinto de 0, el clasificador descendente TIENE QUE incluir dicho valor como puerto de fuente. El clasificador descendente TIENE QUE incluir el tipo de protocolo, la dirección IP de destino y el número de puerto del objeto Sesión hacia atrás.

ES OBLIGATORIO que el CMTS haga las reservas de recursos de red troncal necesarias, tomando como referencia el algoritmo definido para la configuración de la red troncal específica.

Si el resultado de las reservas en los niveles de acceso y troncal es positivo, el CMTS TIENE QUE enviar al cliente un mensaje RSVP-RESV. El contenido de RSVP-RESV SE TIENE QUE determinar a partir de RSVP-PATH: el objeto Sesión se copia de RSVP-PATH, el valor de Estilo es Filtro fijo (Fixed-Filter), la especificación de flujo (Flowspec) se constituye a partir de Tspec de emisor y Rspec hacia adelante, la especificación de filtro (Filter-Spec) es la definida en la plantilla de emisor, y se genera un identificador de recurso (Ressource-ID) que incluye el identificador asignado a los recursos atribuidos. ES OBLIGATORIO incluir el objeto Entidad para compromiso (Commit-Entity) que especifica la dirección y el número del puerto en los que el CMTS aceptará el mensaje COMMIT (tal como se describe en 6.6). SE DEBERÍA incluir el objeto DCLASS con un valor determinado en función del campo punto de código Diffserv (DSCP) de la puerta.

Si la dirección del tramo anterior difiere de la dirección de fuente incluida en el mensaje RSVP-PATH, el CMTS TIENE QUE generar un RSVP-PATH para reservas en sentido descendente. El contenido de RSVP-PATH SE TIENE QUE determinar a partir del RSVP-PATH recibido del cliente. El objeto Sesión TIENE QUE corresponder al objeto Sesión hacia atrás (Reverse-Session-Object) del mensaje RSVP-PATH. Si la dirección que aparece en la plantilla de emisor hacia atrás es 0.0.0.0, o el número de puerto es 0, en el RSVP-PATH no se envía ni Tspec de emisor (Sender-Tspec) ni una plantilla de emisor (Sender-Template). En otros casos, la Tspec de emisor se determina a partir de la Tspec de emisor hacia atrás (Reverse-Sender-Tspec), la Rspec hacia adelante (Forward-Rspec) a partir de la Rspec hacia atrás (Revese-Rspec) y la plantilla de emisor (Sender-Template) a partir de la plantilla de emisor hacia atrás(Reverse-Sender-Template). Se genera un objeto Identificador de recurso (Resource-ID) que incluye el identificador asignado a los recursos atribuidos. El MTA PUEDE utilizar la Tspec de emisor hacia atrás (Reverse-Sender-Tspec) enviada en el mensaje RSVP-PATH, para calcular la especificación de filtro que devuelve en su respuesta RSVP-RESV, o bien, PUEDE generar una respuesta filtro de libre elección (Wildcard-Filter).

Al recibir el mensaje RSVP-RESV el cliente sabe que se han reservado los recursos necesarios. Sabe que dispone de una reserva en ambos sentidos, si el resultado del proceso de reserva es positivo, y puede iniciar la señalización para enviar la señal de llamada al teléfono en el extremo distante.

Si el resultado del proceso de reserva es negativo, el CMTS TIENE QUE enviar al cliente un mensaje RSVP-PATH-ERR indicando el motivo (por ejemplo, no tiene autorización, recursos insuficientes, etc.). Si se trata de las políticas de tratamiento, ES OBLIGATORIO incluir en el mensaje RSVP-PATH-ERR un objeto RSVP-ERROR-SPEC con los siguientes códigos de error y valores de error:

- Si RSVP-PATH no incluía el objeto Identificador de puerta (Gate-ID) o este objeto no concuerda con ninguna de las puertas que conoce el CMTS, contesta con el código de error = 2 (resultado negativo de control de políticas) y el valor de error = 3 (rechazo por políticas genéricas).
- Si RSVP-PATH se rechaza porque no hay recursos adicionales para el nivel de prioridad de la puerta, se devuelve el código de error = 1 (resultado negativo del control de admisión) y el valor de error = 2 (anchura de banda solicitada no disponible). El MTA PUEDE enviar al

usuario una indicación especial del error específico. Si los motivos del resultado negativo de RSVP-PATH no son de políticas, DEBE incluirse un objeto RSVP-ERROR-SPEC con un código de error y un valor de error definidos en el apéndice B de IETF RFC 2205.

El emisor de un RSVP-PATH (MTA o CMTS) es la entidad encargada de hacer una reserva fiable. El emisor de un RSVP-PATH TIENE QUE recibir un mensaje RSVP-RESV o RSVP-PATH-ERR dentro del intervalo de temporización configurado del temporizador T3 (véase el anexo A).

Cuando un MTA o un CMTS transmite un mensaje RSVP que requiere acuse de recibo, ES OBLIGATORIO incluir un objeto RSVP-MESSAGE-ID en dicho mensaje y validar la bandera de solicitud de acuse de recibo (ACK_Desired) del objeto RSVP-MESSAGE-ID. El MTA y el CMTS TIENEN QUE validar la bandera "capacidad de reducción de renovación" en la cabecera común de cada mensaje RSVP. El MTA o el CMTS que recibe un mensaje RSVP con un objeto RSVP-MESSAGE-ID TIENE QUE responder con un mensaje RSVP que contenga un objeto RSVP-MESSAGE-ACK o RSVP-MESSAGE-NACK. El objeto RSVP-MESSAGE-(N)ACK PUEDE ser transportado en mensajes RSVP estándar, pero también puede transmitirse en un mensaje RSVP-ACK si el receptor del objeto RSVP-MESSAGE-ID no tiene ningún otro mensaje RSVP que enviar en ese momento. Por ejemplo, aunque el CMTS NO DEBERÍA retardar el procesamiento de un mensaje RSVP-PATH recibido, si lo retarda TIENE QUE responder inmediatamente con un mensaje RSVP-ACK y ulteriormente un mensaje RSVP-RESV.

Los mensajes RSVP-ACK transportan uno o más objetos RSVP-MESSAGE-(N)ACK. NO SE INCLUIRÁ ningún otro objeto RSVP, exceptuando un objeto facultativo RSVP-INTEGRITY. El objeto RSVP-MESSAGE-(N)ACK (en su caso) TIENE QUE ser el primero del mensaje, salvo que esté presente un objeto RSVP-INTEGRITY (en cuyo caso el objeto RSVP-MESSAGE-(N)ACK TIENE QUE colocarse inmediatamente después del objeto RSVP-INTEGRITY). El CMTS o el MTA PUEDEN utilizar objetos RSVP-INTEGRITY.

Los objetos RSVP-MESSAGE-ID y RSVP-MESSAGE-(N)ACK pueden utilizarse para asegurar una entrega fiable de mensajes RSVP en caso de pérdidas en la red. Dado que el MTA o el CMTS validan la bandera solicitud de acuse de recibo, TIENEN QUE retransmitir los mensajes para los que no han recibido acuse de recibo a intervalos más breves que el intervalo de renovación estándar RSVP, hasta que se acuse recibo del mensaje o expire la temporización T3 (véase el anexo A). ES OBLIGATORIO utilizar una velocidad de retransmisión alta basada en las funciones habituales de variación exponencial. ES OBLIGATORIO utilizar el periodo de retransmisión inicial del temporizador T6 (véase el anexo A) y una variación de potencia de 2. El proceso de retransmisión rápido termina al recibir un objeto RSVP-MESSAGE-(N)ACK o cuando expira el temporizador T3. Si el emisor de RSVP-PATH no recibe un mensaje RSVP-RESV, RSVP-PATH-ERROR, o RSVP-MESSAGE-(N)ACK antes de la siguiente retransmisión, TIENE QUE considerar que se han perdido su mensaje RSVP-PATH original o la respuesta desde el otro extremo, debiendo reenviar el RSVP-PATH. No hay duplicación de reserva porque todos los mensajes RSVP son idempotentes.

En IPCablecom, los mensajes RSVP-PATH son los únicos que TIENEN QUE incluir objetos RSVP-MESSAGE-ID con la bandera ACK_Desired validada. Los objetos RSVP-MESSAGE-ID PUEDEN ser utilizados en otros mensajes RSVP.

Los objetos RSVP-MESSAGE-ID se utilizan en un esquema de RSVP por tramos. Cada uno de los tramos del trayecto que utilizan RSVP y soportan la reducción de renovación realiza su propia retransmisión rápida hasta que recibe un acuse de recibo procedente del siguiente nodo en sentido ascendente. Por lo tanto, si un MTA autónomo situado tras un CM con capacidad RSVP recibe un objeto RSVP-MESSAGE-ACK del CM para un RSVP-PATH, y el CM espera un RSVP-MESSAGE-ACK del CMTS para dicho RSVP-PATH, el CM lleva a cabo la retransmisión rápida mientras el MTA autónomo espera a que expire su temporización de renovación RSVP-PATH normal (30 s). (El MTA ha cesado la retransmisión rápida al recibir un acuse de recibo.) Si un CM con capacidad de RSVP cesa la retransmisión rápida, devuelve hacia atrás al

MTA autónomo un RSVP-PATH-ERROR. De esta forma, la retransmisión no afecta al trayecto completo, sino a los tramos con tendencia a sufrir pérdidas.

En IETF RFC 2961 se define y se describe con mayor detalle un procedimiento de entrega fiable de mensajes RSVP. En IETF RFC 2961 también se describen mecanismos para reducir el número de mensajes de señalización RSVP necesarios para renovar el estado RSVP. Condiciones para las implementaciones de MTA y CMTS conformes a IETF RFC 2961:

- TIENEN QUE validar el bit de capacidad de reducción de renovación en la cabecera RSVP.
- TIENEN QUE soportar la extensión MESSAGE_ID.
- TIENEN QUE soportar la extensión de renovación simplificada para sesiones de unidifusión.
- PUEDEN soportar la extensión de renovación simplificada para sesiones de multidifusión.
- TIENEN QUE soportar la recepción de mensajes agrupados.
- PUEDEN soportar la transmisión de mensajes agrupados.

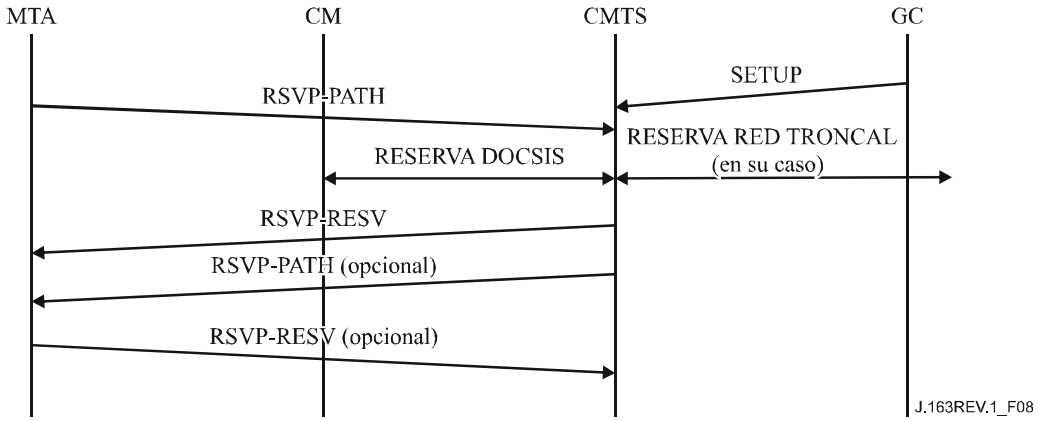


Figura 8/J.163 – Establecimiento de reserva

El CMTS TIENE QUE aplicar filtros de clasificación de paquetes en sentido ascendente para los flujos J.112, para descartar los paquetes que no concuerden con el conjunto de clasificadores de paquetes en sentido ascendente del flujo J.112. La aplicación de filtros de clasificación de paquetes en sentido ascendente es un requisito opcional del CMTS en las redes J.112, pero esta Recomendación exige su implementación en los flujos J.112 utilizados para transportar trenes de medios IPCablecom. Si un CMTS sólo aplica los filtros de clasificación en sentido ascendente a los flujos J.112 (a ningún otro tipo de flujo), es el proveedor del CMTS quien debe decidir como se determinan los flujos J.112.

6.5.2 Modificación de la reserva

Además de reservar una cierta cantidad de recursos puede ser necesario modificar los recursos asignados, aumentando o disminuyendo los recursos utilizados. Para modificar los recursos utilizados se modifica el objeto FLOWSPEC (especificación de flujo) de un mensaje RSVP-RESV y/o la Tspec de emisor de un mensaje RSVP-PATH. Para modificar una reserva ES OBLIGATORIO seguir el mismo proceso de establecimiento de una nueva reserva. Cuando se trate de la modificación de los recursos de una sesión sin aumentar los recursos previamente reservados, el resultado del control de admisión siempre DEBERÍA ser positivo. Debido a que los recursos se describen mediante vectores multidimensionales, una modificación de reserva que aumente los recursos en un sentido y los disminuya en otro SE TIENE QUE someter al control de admisión. Para que el resultado del control de admisión sea positivo, ES OBLIGATORIO que los recursos se

mantengan dentro de los márgenes de recursos autorizados para la sesión y de recursos disponibles para el CMTS.

En el caso de interrupción de una reserva para establecer una sesión con una puerta de mayor prioridad, cuando la anchura de banda es insuficiente, el CMTS TIENE QUE enviar un mensaje RSVP-PATH-ERR y/o RSVP-RESV-ERR para la sesión que se interrumpe. Este mensaje DEBERÍA enviarse cuanto antes. Como respuesta, el MTA DEBERÍA deshacer la reserva y PUEDE notificar la interrupción al usuario (por ejemplo, puede enviar al usuario un tono especial). En este caso, el mensaje RSVP-PATH-ERR (o RSVP-RESV-ERR) TIENE QUE contener un objeto RSVP-ERROR-SPEC con un código de error 2 (resultado negativo de control de políticas) y un valor de error 5 (flujo interrumpido por prioridad).

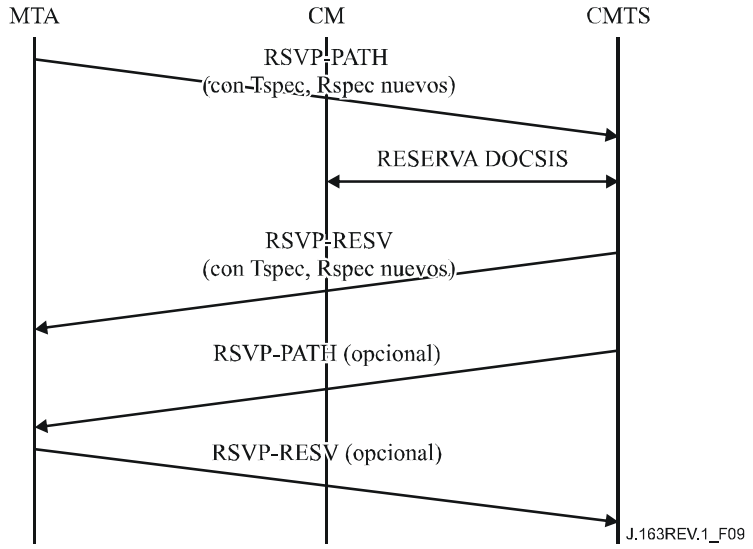


Figura 9/J.163 – Modificación de una reserva

6.5.3 Supresión de una reserva

En RSVP hay dos mensajes para la supresión explícita del estado Trayecto y Reserva: RSVP-PATH-TEAR y RSVP-RESV-TEAR. Para suprimir una reserva en el CMTS, el MTA DEBERÍA enviar un mensaje RSVP-PATH-TEAR. Para suprimir una reserva en dispositivos que utilizan RSVP entre el MTA y el CMTS, el MTA PUEDE enviar un mensaje RSVP-RESV-TEAR. El formato de estos mensajes TIENE QUE ser conforme a IETF RFC 2205 y TIENE QUE incluir el objeto Sesión y la plantilla de emisor para permitir que el CMTS identifique la puerta correspondiente.

Los estados Trayecto y Reserva expiran OBLIGATORIAMENTE si no se renuevan periódicamente. Es adecuado, por ejemplo, cuando falla el MTA. Véanse los mecanismos de renovación en 6.5.4.

Cuando el CMTS recibe un RSVP-PATH-TEAR TIENE QUE responder enviando al MTA un RSVP-RESV-TEAR. El formato de estos mensajes TIENE QUE ser conforme a IETF RFC 2205.

En la versión 1 de RSVP no hay mecanismos para garantizar la entrega fiable de mensajes RSVP-PATH-TEAR y RSVP-RESV-TEAR porque se ha considerado que de estos estados van a expirar de todas formas. Sin embargo, para evitar retardos en la supresión (que suponen una utilización innecesaria de recursos y pueden producir una facturación excesiva), puede utilizarse la ampliación de fiabilidad de RSVP descrita en [IETF RFC 3209].

6.5.4 Mantenimiento de la reserva

El RSVP utiliza un modelo de estado temporal, es decir, de reservas que es necesario renovar periódicamente para que no expiren. Esta característica se mantiene en el modelo segmentado aquí descrito. Dado que el proceso de reserva en este modelo lo inicia el MTA, ES OBLIGATORIO que el MTA renueve periódicamente toda la información de estado RSVP. El MTA TIENE QUE enviar mensajes RSVP-PATH tal como se describe en 6.5.1 en el plazo indicado por el CMTS en el objeto Tiempo de RSVP-RESV. Cuando el CMTS recibe el mensaje RSVP-PATH TIENE QUE generar mensajes RSVP-RESV hacia el MTA (también un mensaje RSVP-PATH si se han detectado nodos con capacidad RSVP tal como se describe en 6.5.1). Así se mantiene el estado temporal del RSVP, lo cual permite garantizar su correcto funcionamiento frente a cambios de encaminamiento y fallos de nodos.

El MTA (o el CMTS) PUEDE asimismo implementar el modo RSVP de renovación simplificada como otra forma de conservar la anchura de banda ascendente cuando se renueva el estado de reserva. En este modo, los nodos RSVP pueden "comprimir" sus estados Trayecto (o Reserva) de múltiples reservas en un único mensaje. En el documento que trata de extensiones de RSVP de reducción de tara para renovación [IETF RFC 2961] se describe así el proceso de renovación simplificada:

"La extensión de renovación simplificada permite renovar el estado RSVP sin transmitir los mensajes estándar de trayecto (Path) o reserva (Resv). Es interesante porque permite disminuir la cantidad de información que debe transmitirse y procesarse para mantener la sincronización de estados de RSVP. Otro aspecto importante de esta extensión es que mantiene la capacidad del RSVP para el tratamiento de los tramos situados más adelante que no sean RSVP y adaptarse a los cambios de encaminamiento. Esta extensión no puede utilizarse con mensajes Path o Resv que sean diferentes de los mensajes anteriormente transmitidos, es decir, si se trata de mensajes de activación.

La extensión de renovación simplificada se basa en la extensión MESSAGE_ID previamente definida. La extensión de renovación simplificada sólo puede aplicarse a un estado previamente anunciado en mensajes Path y Resv que contengan objetos MESSAGE_ID.

La extensión de renovación simplificada utiliza los objetos y el mensaje ACK definido previamente como parte de la extensión MESSAGE_ID, y un nuevo mensaje Srefresh. El nuevo mensaje transporta una lista de campos identificador de mensaje (Message_Identifier) correspondientes a los mensajes de activación Path y Resv que establecieron el estado. Los campos Message_Identifier se transportan en uno de los tres objetos Srefresh relacionados: MESSAGE_ID LIST, MESSAGE_ID SRC_LIST y MESSAGE_ID MCAST_LIST.

El objeto MESSAGE_ID LIST (lista de identificadores de mensaje) se utiliza para renovar todos los estados Resv y el estado Path de sesiones unidifusión. Se compone de una lista de campos Message_Identifier que fueron anunciados inicialmente en objetos MESSAGE_ID. Los otros dos objetos se utilizan para renovar el estado Path de las sesiones multidifusión. Un nodo que recibe una renovación simplificada de un estado Trayecto en multidifusión necesitará información de fuente y de grupo en determinados momentos. Estos dos objetos proporcionan esta información. Los objetos difieren en la información que contienen y en la forma de transmisión. Ambos transportan campos Message_Identifier y las correspondientes direcciones IP de fuente. El objeto MESSAGE_ID SRC_LIST (lista SRC de identificadores de mensaje) se envía en mensajes dirigidos a la dirección IP multidifusión de la sesión. El objeto MESSAGE_ID MCAST_LIST (lista multidifusión de identificadores de mensaje) añade la dirección de grupo y se envía en mensajes dirigidos al siguiente tramo RSVP.

El objeto MESSAGE_ID MCAST_LIST se utiliza normalmente en enlaces punto a punto.

Un nodo RSVP que reciba un mensaje Srefresh compara cada campo Message_Identifier de la lista con el estado Path o Resv instalado. Todos los estados de concordancia se actualizan como si se

hubiese recibido un mensaje normal de renovación RSVP. Cuando no hay concordancia se notifica al emisor del mensaje Srefresh mediante un acuse negativo de renovación (NACK).

Para enviar un acuse negativo de renovación se utiliza el objeto MESSAGE_ID_NACK. Tal como se describe en la cláusula anterior, las reglas para el envío de los objetos MESSAGE_ID_NACK y MESSAGE_ID_ACK son las mismas. Una de estas reglas establece que el objeto MESSAGE_ID_NACK se puede enviar en mensajes RSVP no relacionados o en mensajes ACK RSVP."

Véase una descripción completa del proceso de renovación simplificada en la sección 5 de la especificación de extensiones de RSVP de reducción de tara para renovación [IETF RFC 2961].

6.6 Definición de mensajes de compromiso

En esta cláusula se definen los mensajes de compromiso que el MTA TIENE QUE generar y que el CMTS TIENE QUE soportar.

ES OBLIGATORIO enviar los mensajes de compromiso (Commit) como datagramas UDP/IP con número de protocolo 17 (UDP). Cada mensaje Commit TIENE QUE ocupar exactamente un datagrama UDP/IP. La dirección IP de destino y el número de puerto que se indican en la cabecera UDP TIENEN QUE ser los mismos que se especifican en el objeto entidad para compromiso (Commit-Entity) que se comunica con el mensaje RSVP-RESV. El número de puerto de fuente TIENE QUE ser el puerto en el que el MTA aceptará el mensaje de acuse de recibo.

ES OBLIGATORIO formar los mensajes de compromiso con una cabecera común seguida de un número variable de objetos de longitud variable. La cabecera común TIENE QUE tener el formato siguiente:

Versión	Banderas	Tipo de mensaje	Suma de control del mensaje
TTL enviado		(Reservado)	Longitud del mensaje

ES OBLIGATORIO utilizar la especificación IETF RFC 2205 para los valores de cada campo. ES OBLIGATORIO utilizar los siguientes tipos de mensajes:

COMMIT	240
COMMIT-ACK	241
COMMIT-ERR	242

Cada objeto TIENE QUE constar de una o más palabras de 32 bits, con una cabecera de una palabra que tiene el formato siguiente:

Longitud en bytes	Número de clase	Tipo C
Contenido del objeto ...		

ES OBLIGATORIO utilizar la especificación IETF RFC 2205 para los valores de cada campo.

El formato de los mensajes COMMIT y COMMIT-ACK conformes a esta Recomendación TIENE QUE ser el siguiente (los elementos en cursiva se definen en 6.3 de esta Recomendación, y todos los demás en IETF RFC 2205 y/o IETF RFC 2210):

<COMMIT-Message> ::= <Common-Header> <Session>
Sender-Template> <*Gate-ID*>
<Flowspec>] [<*Downstream-Flowspec*>]
<COMMIT-ACK-Message> ::= <Common-Header> <Session>
Sender-Template><*Gate-ID*>

<COMMIT-ERR-Message> ::= <Common-Header> <Session>
<Sender-Template><*Gate-ID*><Error-Spec>

Véase la definición de <*Downstream-Flowspec*> en lenguaje BNF en 6.4, Definición de mensajes RSVP.

ES OBLIGATORIO incluir los objetos Sesión (Session) y Plantilla de emisor (Sender-Template) que identifican las direcciones IP y los puertos del emisor y del destino. Dado que los recursos comprometidos PUEDEN ser inferiores a los recursos totales reservados (especialmente en una situación de llamada en espera o de modificación de códec), un mensaje Commit (compromiso) también PUEDE contener un objeto <Flowspec> (especificación de flujo) para cada sentido de la sesión. Ello proporciona un mecanismo para aumentar o reducir los recursos comprometidos, siempre que la cantidad de dichos recursos comprometidos no supere a los recursos reservados. Obsérvese que ES POSIBLE retener (congelar) un conjunto de recursos reduciendo los recursos comprometidos a cero, sin modificar los recursos reservados. Si se omite una de las especificaciones de flujo (Flowspec), el CMTS TIENE QUE hacer que la cantidad de recursos comprometidos en dicho sentido sea igual a la cantidad de recursos reservados.

6.7 El procedimiento de compromiso

Un aspecto significativo del modelo de QoS dinámico es el proceso de reserva en dos fases: reserva y compromiso. En la cláusula 6.5 anterior se describe la fase de reserva, y en ésta se describe la fase de compromiso y su relación con la fase de reserva.

Un CMTS conforme TIENE QUE realizar todas las funciones de control de admisión y de asignación de recursos cuando recibe el mensaje RSVP-PATH original, pero NO PODRÁ permitir que el MTA acceda a dichos recursos hasta que se reciba un mensaje COMMIT, a no ser que en los parámetros GATE-SET se indique lo contrario.

Para realizar la operación de COMPROMISO (COMMIT) el MTA TIENE QUE enviar al CMTS un mensaje unidifusión. Se hace así porque la fase de compromiso sólo implica al MTA y a una puerta. El objeto entidad para compromiso en el mensaje RSVP-RESV permite al MTA conocer la dirección del CMTS y el número de puerto.

Obsérvese que un mensaje COMMIT difiere sustancialmente de un mensaje RSVP normalizado. Se envía directamente del MTA al CMTS y no tramo a tramo como el mensaje RSVP. Sin embargo, sus objetos tienen la misma sintaxis que los objetos RSVP.

El CMTS TIENE QUE verificar el valor del identificador de puerta (GateID) y comprobar si el contenido de los objetos Sesión y Plantilla de emisor concuerdan con la reserva anterior para el mismo valor de GateID, y si los objetos Sesión hacia atrás y Plantilla de emisor hacia atrás (en su caso) concuerdan con la reserva anterior para el mismo valor de GateID. El CMTS TIENE QUE acusar recibo de un mensaje COMMIT con un mensaje COMMIT-ACK o un mensaje COMMIT-ERR.

Se enviará un mensaje COMMIT-ACK después de realizar satisfactoriamente el intercambio de mensajes DSC J.112 entre el CMTS y el CM. Si el resultado de los mensajes J.112 es negativo, se enviará en su lugar un mensaje COMMIT-ERR. Cuando un MTA no recibe el acuse de recibo en el plazo del temporizador T4 (véase el anexo A), TIENE QUE volver a enviar el mensaje COMMIT (se harán hasta siete intentos).

Si el MTA desea modificar la cantidad de recursos comprometidos dentro de los límites de la capacidad máxima reservada, ES OBLIGATORIO realizar otra secuencia COMMIT/COMMIT-ACK.

Si el MTA desea modificar la cantidad de recursos reservados, ES OBLIGATORIO repetir el intercambio de mensajes RSVP-PATH/RSVP-RESV.

7 Protocolo de QoS entre un MTA integrado y el CM (pkt-q1)

En lugar de utilizar la interfaz pkt-q3 como se indica en la cláusula 6, un MTA integrado PUEDE hacer una reserva dinámica de recursos locales de QoS utilizando únicamente los mecanismos definidos en la Rec. UIT-T J.112. Cuando se utiliza esta alternativa, el MTA integrado transmite directamente las señales de QoS del acceso local a través de la interfaz del servicio de control MAC definida en el anexo E al anexo B/J.112. A diferencia del proceso descrito en la cláusula 6, la señalización QoS a través de la interfaz J.112 (interfaz pkt-q2) la inicia el CM (no el CMTS). En las otras interfaces no cambia nada. Véase un ejemplo de este método en los apéndices VII y VIII.

Un MTA integrado utiliza los protocolos de señalización (SIP IETF RFC 2543 y Rec. UIT-T J.162) para indicar sus requisitos de QoS para la sesión. Después de determinar los recursos de QoS que es necesario reservar o comprometer, el MTA integrado TIENE QUE iniciar una señalización de flujo de servicio dinámico J.112 para crear, modificar y/o suprimir flujos de servicio, y asignar recursos J.112. En todos los casos, que la sesión la haya iniciado el MTA integrado, un dispositivo par o un nodo de red, el MTA comunica los requisitos de QoS al MAC de la Rec. UIT-T J.112 a través de la interfaz de control del servicio MAC. Así se crean o modifican los flujos de servicio necesarios para la sesión, utilizando los mecanismos de la Rec. UIT-T J.112 de intercambio de mensajes para flujo de servicio dinámico. En las siguientes cláusulas se precisa la correspondencia entre los requisitos de QoS para la sesión del MTA y de la Rec. UIT-T J.112, el soporte del mecanismo en dos fases reserva/compromiso en la especificación J.112 y la utilización de la interfaz de control del servicio MAC J.112.

7.1 Reflejar las especificaciones (Flowspecs) en parámetros QoS J.112

En la cláusula 6.2.3 se describe en detalle el proceso de transcripción de parámetros DOCSIS que se ha de utilizar para establecer y mantener los flujos de servicio ascendente y descendente. El MTA TIENE QUE tener en cuenta los requisitos de esa cláusula para reflejar las condiciones de QoS de la sesión en parámetros QoS DOCSIS.

Además, los MTA integrados TIENEN QUE incluir su dirección y puerto de emisión (fuente en sentido ascendente) y recepción (destino en sentido descendente) en todos los TLV de clasificadores comunicados en mensajes DSx. SE PUEDEN asignar valores de elección libre a las direcciones de extremo distante y los puertos de recepción si no se ha proporcionado el SDP del extremo distante ni otros valores mediante la opción de conexión local (LCO). Cuando se proporcionan estos valores en uno de los formatos, ES OBLIGATORIO incluirlos en los TLV de clasificadores. En todos los casos SE TIENEN QUE asignar valores de elección libre a los puertos fuente de extremo distante, dado que este parámetro no se comunica mediante el SDP.

Obsérvese que los ejemplos de la cláusula 8 incluyen la tara asociada a la cabecera ampliada DOCSIS BPI+ conforme a la especificación de seguridad (Rec. UIT-T J.170). Si se inhabilita BPI+ (para hacer pruebas, por ejemplo), hay que actualizar los valores de estos ejemplos, retirando cinco bytes de la tara de capa de enlace en los cálculos del tamaño de autorización en sentido ascendente.

7.2 Soporte de J.112 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) J.112 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.

Véase un ejemplo de utilización del bloque de autorización en los mensajes DSA-REQ del apéndice VII.

7.2.1 Reserva/Compromiso de QoS en dos fases

Hay tres conjuntos de parámetros de calidad de servicio asociados a un flujo de servicio: 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 J.112, 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 10.

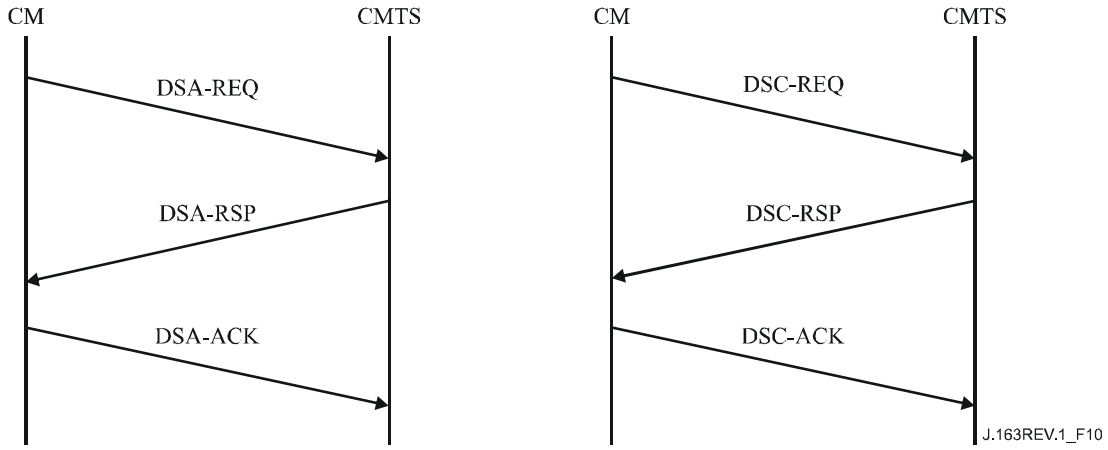


Figura 10 – Mensajes DSA y DSC entre el CM y el CMTS

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 J.112.

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

DSA-REQ

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 J.112.

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
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. Véanse otros ejemplos en el apéndice VII.

7.2.2 Reserva con múltiples especificaciones de flujo de servicio

En algunos casos hay que incluir varias especificaciones posibles al hacer una reserva. Por ejemplo, en algunas aplicaciones se desea disponer de una reserva que admita el cambio de una especificación de flujo a otra en plena sesión sin tener que pasar el control de admisión cada vez que se produce dicho cambio. Para poder modificar el conjunto de parámetros de QoS Activo (ActiveQoSParameterSet) de un flujo de servicio durante una sesión, debe especificarse un valor apropiado de conjunto de parámetros de QoS Autorizado (AuthorizedQoSParameterSet) mediante políticas en el controlador de puerta. Para ello se utiliza el método del mínimo valor superior (véase 6.2.1). Conforme a las disposiciones de 6.2.4, el mínimo valor superior de flujos con dos tipos de planificación J.112 diferentes es nulo. Véase la información de la Rec. UIT-T J.112 sobre el cálculo del mínimo valor superior para flujos de mensajes DSx.

7.2.3 Mantenimiento de la reserva

El RSVP utiliza un modelo temporal descrito en 6.5.4, pero la Rec. UIT-T J.112 sólo proporciona un mecanismo de temporización en las interfaces J.112. Los parámetros de QoS "Temporización de actividad" (TimeoutForActiveQoSParameters) y "Temporización de admisión" (TimeoutForAdmittedQoSParameters) del flujo de servicio 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.

7.2.4 Soporte de la vinculación dinámica de recursos

La vinculación dinámica de recursos (cláusulas 5.7.7 y 6.1.4) 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 incluir el identificador de recursos asociado a esta última sesión en el mensaje DSA-REQ que envía al cliente.

7.2.5 Concordancia de parámetros de QoS para la autorización

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

Los parámetros *RSVP Capacidad de contador* (b), *Tamaño máximo del datagrama* (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[7] (en sentido ascendente), y el valor *DOCSIS Tamaño mínimo previsto de paquete a la velocidad reservada* menos la tara DOCSIS descendente[8] (en sentido descendente).

---

7 En esta tara deberían incluirse los 18 bytes de tara de cabecera 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: cabecera básica DOCSIS (6 bytes), cabecera ampliada UGS (3 bytes) y cabecera ampliada BPI+ (5 bytes). Si se ha validado la supresión de cabecera de cabida útil (PHS, *payload header suppression*) hay que añadir el número de bytes suprimidos al valor DOCSIS Tamaño de autorización sin petición.

8 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 cabecera 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*.

En sentido descendente, los parámetros *RSVP Velocidad del contador* (r) y *Velocidad 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 datagrama* calculado antes. En sentido ascendente, los parámetros *RSVP Velocidad del contador* (r) y *Velocidad 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 *RSVP Velocidad reservada* (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 *RSVP Mínima unidad supervisada* calculado antes. En sentido ascendente, el parámetro *RSVP Velocidad reservada* (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 RSVP* SE TIENE QUE configurar con el valor *DOCSIS Fluctuación de autorización tolerada* en sentido ascendente. El término de inactividad RSVP TIENE QUE ser cero para el flujo descendente, para indicar que este parámetro no será especificado por el MTA.

El *Protocolo RSVP* TIENE QUE ser el *Protocolo IP DOCSIS*.

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

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

El *Puerto de fuente RSVP* 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 RSVP 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 RSVP* 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 cabecera IP/UDP/RTP

160 + 42 = 202 bytes en total por paquete

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

$10{,}1 \times 8$ = 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 cabecera 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 cabecera 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.

Cabecera básica DOCSIS (FC hasta HCS, ninguna cabecera ampliada): 6 bytes

Cabecera ampliada UGS: 3 bytes

Cabecera ampliada BPI+: 5 bytes

Cabecera 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.

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

7.2.6 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	gate-id

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

7.3 Utilización de la interfaz de servicio de control MAC J.112

Los parámetros de QoS J.112 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 J.112 (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 J.112:

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.

7.3.1 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 11.

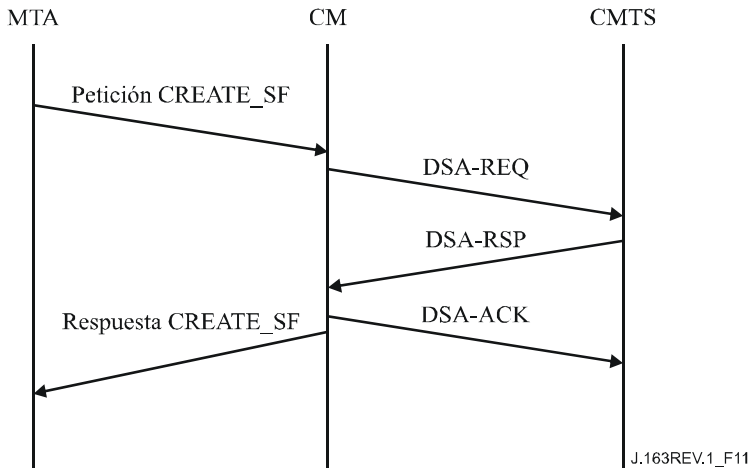


Figura 11/J.163 – Establecimiento de la reserva

7.3.2 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 12.

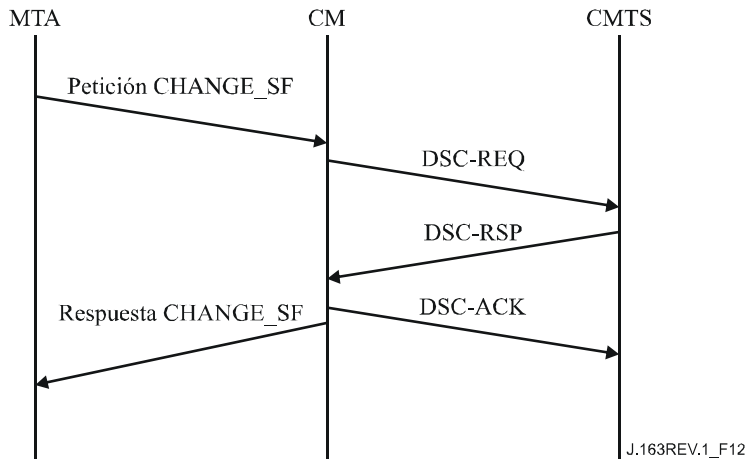


Figura 12/J.163 – Modificación de la reserva

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.

7.3.3 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 13.

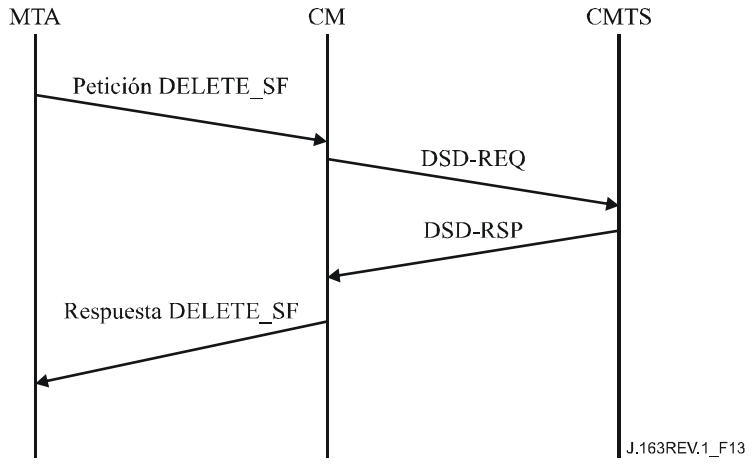


Figura 13/J.163 – Supresión de la reserva

8 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.

8.1 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 J.112 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 J.112 que, a su vez, controlan el encaminamiento de paquetes a flujos J.112.

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 J.112 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 un intercambio de mensajes MAC J.112, 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 J.112 para cada flujo unidireccional establecido.

8.1.1 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 el mensaje RSVP de 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 RSVP.

8.1.2 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 multimedios. [No obstante, ello no impide que puedan existir implementaciones bidireccionales.]

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 J.112, 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 multimedios 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 PATH o en el mensaje MAC J.112 equivalente) 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.

8.1.3 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 [sería la implementación bidireccional habitual].
- 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.

8.1.4 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 14, 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 14, 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 14 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 MTA intente reservar recursos. El MTA lo hace mediante un mensaje RSVP-PATH o mediante la interfaz de 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 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 MTA 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 MTA comprometa los recursos (los active). La instrucción de compromiso (Commit) del MTA es un mensaje UDP unidifusión o una petición equivalente a través de la interfaz de capa MAC. Si la puerta aún se encuentra en el estado "Reservado" y el temporizador T1 expira (el MTA 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.

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 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) 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 comprometidos hasta que el MTA local emita 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 MTA una instrucción de liberación, ya sea en la forma de mensaje RSVP-PATH-TEAR o a través de la interfaz de capa MAC, porque un cliente no ha renovado una reserva o debido a mecanismos internos J.112 que detectan un fallo de cliente, el CMTS TIENE QUE desactivar todos los recursos comprometidos para el MTA, 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 MTA inicie una modificación de la reserva o el compromiso de recursos, dentro de los límites de la autorización y el control de admisión local.

8.1.5 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.

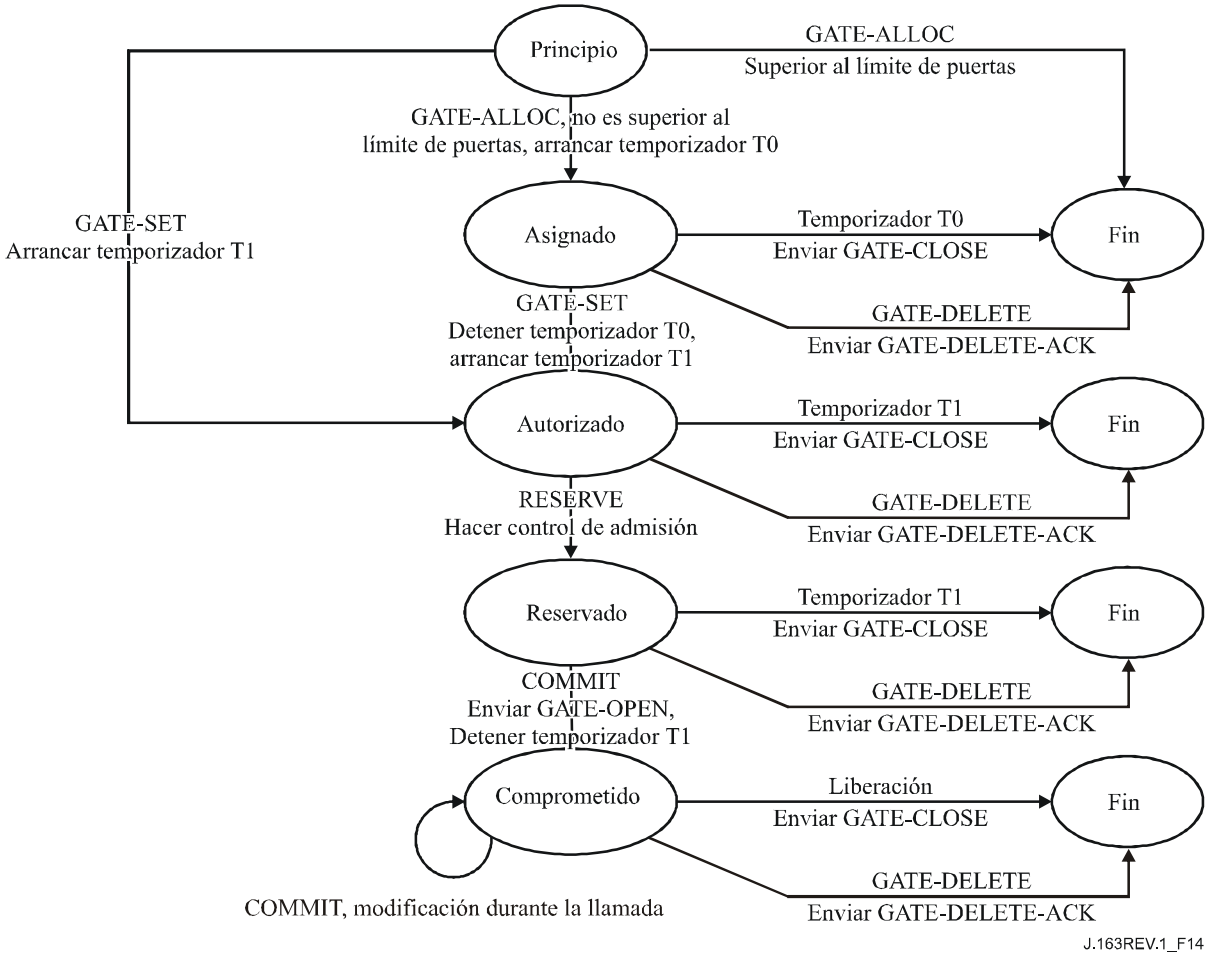


Figura 14/J.163 – Diagrama de transición de estados de una puerta

8.2 Perfil COPS para IPCablecom

El control de admisión de QoS de IPCablecom 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 15 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.

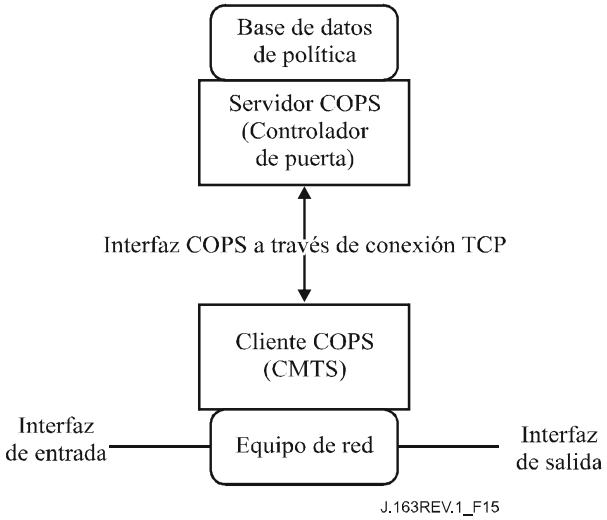


Figura 15/J.163 – Esquema del control de admisión de QoS

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 del ancho 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.

8.3 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 utilizará los mecanismos las normas actualmente en estudio para garantizar la seguridad del trayecto de comunicación.

8.3.1 Formato común de los mensajes COPS

Todos los mensajes COPS constan de una cabecera COPS seguida de un número de objetos tipificados. El GC y el CMTS TIENEN QUE soportar los mensajes COPS definidos a continuación (véase la figura 16):

<table>
<tr><td colspan="2">0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>Versión</td><td>Banderas</td><td>Código Op</td><td colspan="2">Tipo de cliente</td></tr>
<tr><td colspan="5">Longitud de mensaje</td></tr>
</table>

Figura 16/J.163 – Cabecera 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).

A la cabecera común COPS sigue un número variable de objetos. Todos los objetos tienen el mismo formato: una o más palabras de 32 bits con una cabecera de cuatro octetos de acuerdo con el formato siguiente (véase la figura 17).

0	1	2	3
Longitud		Número C	Tipo C
(Contenido del objeto)			

Figura 17/J.163 – Formato común de objetos COPS

Longitud es un valor de dos octetos que TIENE QUE indicar el número de octetos del objeto (incluida la cabecera). 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)

8.3.2 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:

8.3.2.1 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

8.3.2.2 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)		

8.3.2.3 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)		

8.3.2.4 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)		

8.3.2.5 Especificación de puerta (Gate-spec)

Longitud = 60		Número S = 5	Tipo S = 1	
Sentido	ID de protocolo	Banderas, abajo definidas	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)				Alt #1 de espec de flujo
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)				
Otros conjuntos de valores r, b, p, m, M, R y S que sean necesarios para describir la autorización.				Alt #2 de espec de flujo, etc.

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 la cabecera IP o cero si no hay requisito de concordancia.

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 son dos valores de 16 bits, o cero si no hay requisito de concordancia.

Los valores de r, b, p, m, M, R y S se describen en 6.2. 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 8.5 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 del ancho 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

Para que el nuevo sistema sea compatible con las implementaciones de sistemas actuales y poder utilizar 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. Las redes DiffServ no soportan 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 8.1.4. 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.

8.3.2.6 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)		

8.3.2.7 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.

8.3.2.8 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.

8.3.2.9 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 RSVP)

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

8.3.2.10 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

6 = Falta un objeto necesario

7 = Objeto no válido

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.

8.3.2.11 Parámetros de vigilancia electrónica (Electronic-Surveillance-Parameters)

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)		

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*).

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.

8.3.2.12 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

8.3.3 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 la cabecera COPS. En todos los mensajes decisión (DEC), excepto el

primero, se debería poner a uno el bit de la bandera del mensaje solicitado en la cabecera 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.

8.4 Procesos del protocolo de control de puerta

8.4.1 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 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 18.

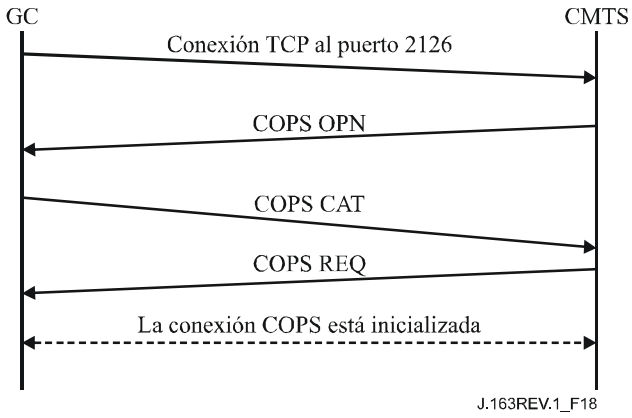


Figura 18/J.163 – Establecimiento de conexión COPS

El CMTS TIENE QUE enviar periódicamente al GC un mensaje COPS KEEP-ALIVE (KA). Cuando recibe el mensaje COPS KA, el GC TIENE QUE devolver al CMTS el mensaje COPS KA. Esta transacción, representada en la figura 19, 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.

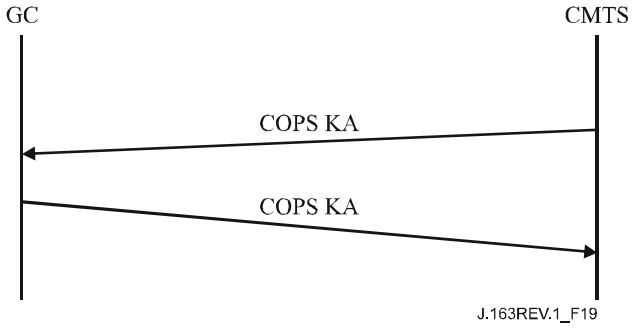


Figura 19/J.163 – Intercambio del mensaje COPS mantener vigente (KA)

8.4.2 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.

8.4.3 Procedimientos para la asignación de una nueva puerta

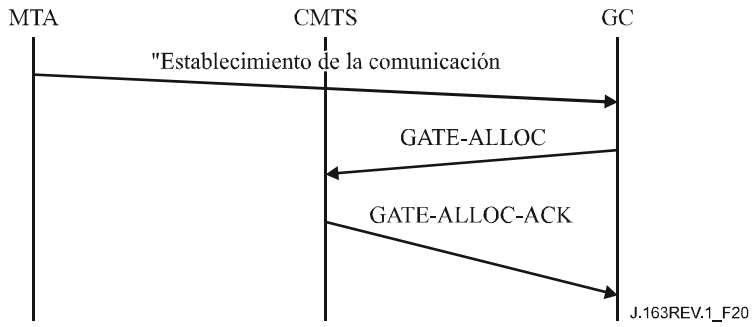
El controlador de puerta envía al CMTS un mensaje GATE-ALLOC cuando el MTA de origen envía el mensaje "establecimiento de la comunicación" ("Call_Set-up") [por ejemplo, el mensaje "Invite(stage 1)" si se utiliza DCS]. Véase la figura 19.

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 8.4.8). 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 20) 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 20/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

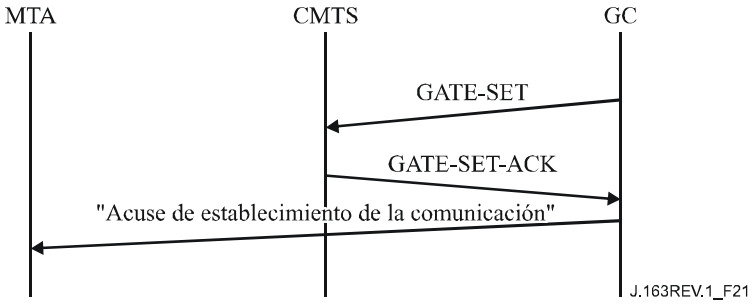
6 = Falta un objeto necesario

7 = Objeto no válido

127 = Otros, error no especificado

8.4.4 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 21 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 21/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 8.4.3).

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 no válido

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 objeto RSVP ID de puerta o mediante 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 la bandera compromiso automático está validada, el CMTS TIENE QUE tomar las medidas adecuadas en la capa MAC J.112 para comprometer inmediatamente los recursos. 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. 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.

8.4.5 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 no válido

127 = Otros, error no especificado

8.4.6 Procedimientos para comprometer una puerta

Cuando el MTA realiza una operación Commit (procedimiento de 6.7 en el caso de un MTA de tipo RSVP, o 7.2.1 para un MTA integrado), el CMTS TIENE QUE enviar un mensaje Apertura de puerta (Gate-Open).

8.4.7 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 de 6.5.3 en el caso de un MTA de tipo RSVP, o 7.3.3 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.

8.4.8 Procedimientos para la supresión de una puerta

En un flujo de llamada normal, el CMTS suprime una puerta cuando recibe un mensaje RSVP-PATH-TEAR o la petición de liberar el flujo J.112 a través de la interfaz de capa MAC J.112 (enviada por un MTA integrado que no soporta RSVP). El CMTS también suprime una puerta cuando recibe un mensaje GATE-CLOSE de un CMTS distante (modelo DCS) o de un CMS (modelo NCS).

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 no válido

127 = Otros, error no especificado

8.4.9 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.

8.4.10 Situaciones de fallo

Si un CMTS detecta la pérdida de conexión TCP con el GC, por ejemplo en caso de fallo catastrófico del GC, TIENE QUE mantener todas las puertas establecidas. 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.

8.5 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 6.2.1 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.

8.6 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.

8.6.1 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 22.

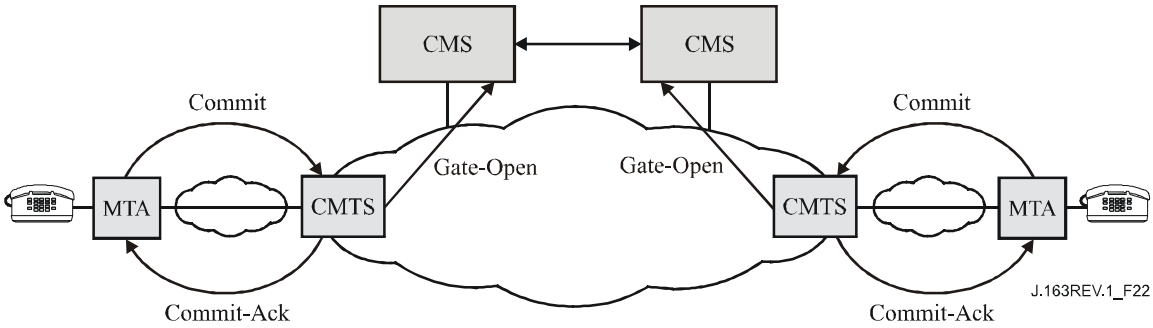


Figura 22/J.163 – Conexión de llamada

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".

8.6.2 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 23.

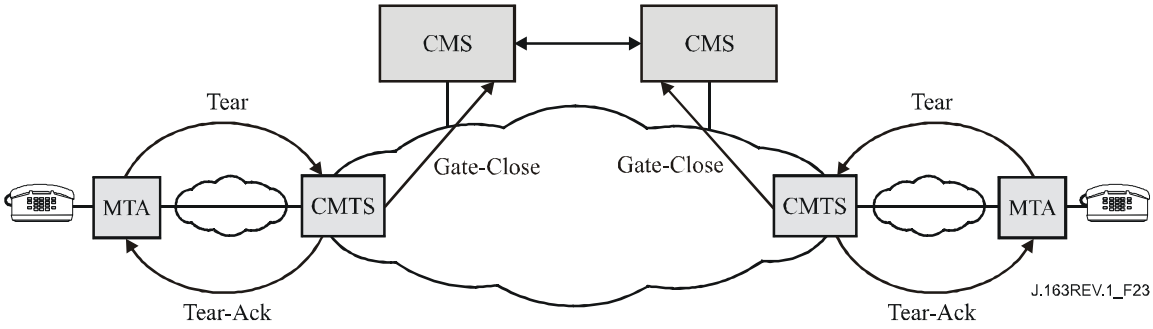


Figura 23/J.163 – Terminación de llamada

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 señalización 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 se implementa en el MTA o en el CMTS para tratar reservas RSVP. Controla el tiempo total que puede transcurrir antes de que el proceso de retransmisión RSVP termine sin haber recibido un acuse de recibo, cuando hay una pérdida en la red. Es suficientemente corto para que la recuperación sea rápida en caso de mensajes perdidos y no alargar significativamente el retardo

posterior a la marcación, pero también suficientemente largo para permitir que el CMTS acuse recibo de la petición y todos lo encaminadores intermedios de la red del cliente.

Este temporizador arranca cuando el MTA o el CMTS envía un mensaje RSVP que requiera un acuse de recibo (como el RSVP-PATH). Se pone a cero nuevamente cuando el emisor de ese mensaje recibe una respuesta. En el caso de un mensaje RSVP-PATH, la respuesta PUEDE ser RSVP-RESV, RSVP-PATH-ERROR, RSVP-MESSAGE-ACK o RSVP-MESSAGE-NACK.

Al expirar el temporizador termina el procedimiento de retransmisión RSVP.

El valor RECOMENDADO de este temporizador es 4 segundos (4 000 ms).

Temporizador T4

Este temporizador se implementa en el MTA para tratar los mensajes COMMIT. Controla la retransmisión de mensajes COMMIT posiblemente perdidos en la red. Es suficientemente corto para que la recuperación sea rápida en caso de pérdida de mensajes Commit y no alargar significativamente el retardo después de descolgar, pero también suficientemente largo para permitir el procesamiento de la petición COMMIT en el CMTS.

Este temporizador arranca cuando el MTA envía un mensaje COMMIT.

Se pone a cero nuevamente cuando el MTA recibe un mensaje COMMIT-ACK o COMMIT-ERR que se reconoce como respuesta al mensaje COMMIT.

Al expirar este temporizador el MTA vuelve a enviar el mensaje COMMIT.

El valor RECOMENDADO de este temporizador es 500 ms.

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 se implementa en el MTA o en el CMTS para tratar las reservas RSVP. Controla el retardo inicial utilizado por el procedimiento de retransmisión RSVP.

El valor RECOMENDADO de este temporizador es 500 ms.

Temporizador T7

El CMTS TIENE QUE adoptar el valor de este temporizador para los parámetros de QoS Plazo de estado Admitido para el flujo de servicio. 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 EMTA pueda renovar este temporizador, el CMTS TIENE QUE comunicar al EMTA 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 adoptar el valor de este temporizador para los parámetros de QoS Plazo de estado Activo para el flujo de servicio. 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 EMTA pueda renovar este temporizador, el CMTS TIENE QUE comunicar al EMTA 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.

Apéndice I

Ningún texto.

Apéndice II

Ejemplo de intercambio de mensajes del protocolo para una llamada DCS básica entre elementos de la de red para MTA autónomos

En este apéndice se presenta una descripción informal, de carácter informativo, de las relaciones entre el protocolo de señalización distribuida de la llamada (DCS) y los métodos de QoS dinámica que pueden invocarse en distintos puntos del flujo de la llamada. La descripción no pretende ser completa. Aunque este ejemplo pretende ser lo más preciso posible, la especificación de señalización de llamada DCS es la especificación de referencia de los flujos de señalización de llamada.

Cuando el GC_O recibe un mensaje INVITE del MTA_O de origen, envía una petición GATE-ALLOC al $CMTS_O$ que está más cerca del MTA_O de origen para que se asigne un identificador de puerta (GateID) de 32 bits exclusivo en dicho $CMTS_O$. Este identificador se comunica al $CMTS_T$ distante en el mensaje INVITE que reenvía el GC_O. Además, el $CMTS_O$ de origen comunica el número de conexiones activas (puertas) que utiliza el MTA_O para que el GC_O o el DP puedan informar del nivel de actividad actual del abonado.

El GC_T de terminación conoce todos los códecs posibles que pueden ser utilizados para la llamada (propuestos por el MTA_O) y con ello puede calcular una "capacidad máxima autorizada" y generar una instrucción GATE-SET dirigida al $CMTS_T$. También es posible que el GC_T sólo genere una instrucción GATE-ALLOC, espere los resultados de los procedimientos de negociación de códec realizados por el MTA_T, calcule una "capacidad máxima de autorización" más precisa después de haber recibido el 200-OK del MTA_T, y entonces envíe la instrucción GATE-SET. Esta opción se muestra en los siguientes diagramas de flujo de llamada. En cualquier caso, el ID de puerta se asigna y se entrega al MTA_T en el mensaje INVITE, y el MTA_T espera el mensaje de señalización ACK (acuse de recibo) para determinar los valores definitivos del códec de la negociación.

En el mensaje 200-OK del GC_T al GC_O se incluye el ID de puerta del extremo de terminación. Se comunica al $CMTS_O$ en el correspondiente intercambio de GATE-SET junto con la "capacidad máxima autorizada" de parámetros de especificación de flujo.

El MTA_O que ha recibido el mensaje de retorno 200-OK conoce la dirección del MTA_T de destino y los parámetros asociados a la llamada (los códecs utilizados) y los traduce a parámetros de especificación de flujo (Flowspec) en ambos sentidos. El MTA_O de origen envía un ACK para el 200-OK y hace una reserva de recursos. Al recibir el ACK, el MTA_T de terminación dispone de toda la información necesaria y realiza una reserva de recursos.

La reserva implica enviar un mensaje RSVP-PATH con parámetros de especificación de flujo para ambos sentidos. El CMTS realiza el control de admisión después de comparar los parámetros con la capacidad máxima autorizada y con la disponibilidad de recursos; si el resultado es positivo, confirma la reserva mediante un mensaje RSVP-RESV. Mientras tanto, el CMTS y el CM realizan el intercambio de mensajes MAC J.112 para la asignación de recursos de capa 2. Los recursos necesarios para la llamada quedan entonces disponibles para ser comprometidos. No obstante, todavía hay que hacer otra fase del protocolo de señalización de llamada y esperar a que los usuarios de ambos extremos descuelguen el "teléfono" para establecer la comunicación.

El segundo mensaje 200-OK desde el MTA_T al MTA_O de origen es una indicación de que los dos usuarios (en este caso sencillo de llamada básica entre dos partes) están listos para comunicar. El MTA_T de terminación envía un mensaje COMMIT inmediatamente después de enviar el 200-OK. Cuando el MTA_O de origen recibe el 200-OK, acusa recibo de este mensaje y genera un mensaje COMMIT. El mensaje COMMIT se transmite desde cada MTA a su CMTS local y provoca un intercambio de mensajes MAC J.112 para comprometer los recursos para el flujo. Cuando los CMTS acusan recibo de COMMIT, los dos extremos pueden comenzar la comunicación con una QoS mejorada. Cuando cualquiera de los dos CMTS recibe el mensaje COMMIT, arranca el temporizador T2 que espera la recepción del mensaje apertura de puerta (Gate-Open) desde el CMTS distante con su ID de puerta.

También se indican los mensajes de coordinación de puertas entre los dos CMTS que se informan entre sí que la puerta ha sido abierta y que se ha intercambiado la descripción (especificación de flujo) del flujo esperado procedente del otro extremo. La recepción del mensaje apertura de puerta supone la suspensión del temporizador situado en los CMTS.

Al terminar la llamada los MTA envían un mensaje RSVP-PATH-TEAR para cancelar las reservas. En ese momento también los CMTS envían un mensaje de coordinación Cierre de puerta (Gate-Close) al CMTS distante.

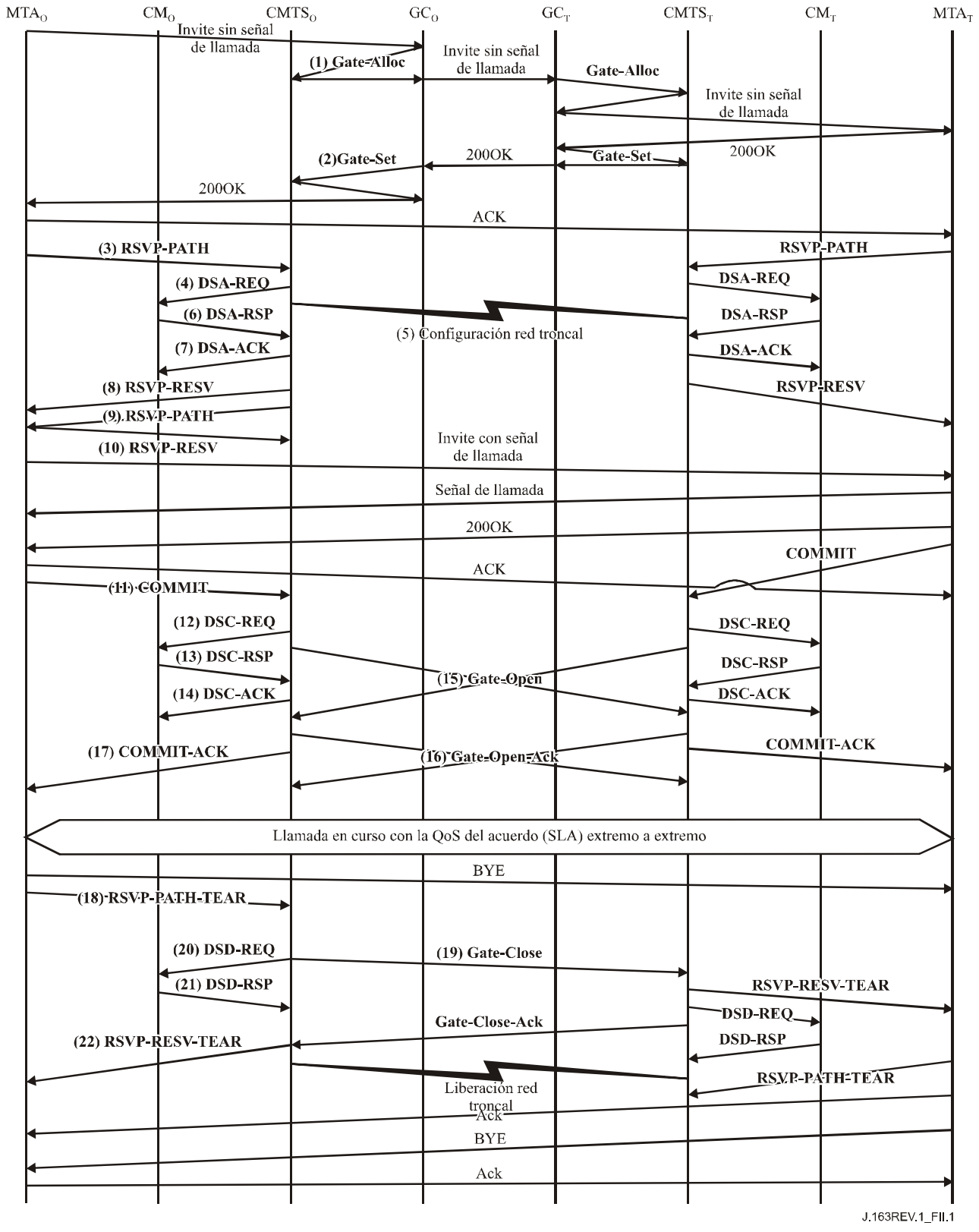


Figura II.1/J.163 – Flujo de llamada básica con señalización DCS

1) Cuando el GCo recibe la información de señalización del MTAo, verifica el consumo actual de recursos del MTAo consultando al CMTSo.

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos que utiliza este punto extremo.
Total de actividad		4	Número máximo de conexiones permitidas por cliente.

El CMTSo verifica la utilización actual de recursos del MTAo, y responde indicando el número de conexiones activas.

GATE-ALLOC-ACK (acuse de asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos que utiliza este punto extremo
ID de puerta		37125	Identificador de puerta asignada.
Total de actividad		3	Número total de conexiones establecidas por este cliente.
Puerto para la coordinación de puertas		4104	Puerto UDP en el que el CMTS espera los mensajes de coordinación de puerta.

2) Después de otros intercambios de señalización, el GCo autoriza la admisión de la nueva conexión en el CMTSo.

GATE-SET (establecimiento de puerta)

ID de transacción		3177	Identificador de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección CMTS	CMTSt	Información necesaria para la coordinación de puertas.
	Puerto CMTS	2052	
	ID de puerta distante	1273	
	Clave de seguridad	<key>	
Información de generación de evento	Dirección RKS	RKS	Dirección del servidor de mantenimiento de registros (RKS).
	Puerto RKS	3288	Puerto en el servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se pasan al RKS cuando se comprometen recursos.

GATE-SET (establecimiento de puerta)

Información de conexión de medios	Número llamado	212-555-2222	Campos necesarios para generar un mensaje respuesta de llamada.
	Número de encaminamiento	212-555-2222	
	Número facturado	212-555-1111	
	Número de encaminamiento del punto de interconexión	212-555-2222	
Especificación de puerta	Sentido	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	MTAo	
	Dirección de destino	MTAt	
	Puerto de fuente	0	
	Puerto de destino	7000	
	DSCP	6	Valor que indica el tipo de paquete en sentido ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

GATE-SET (establecimiento de puerta)

Especificación de puerta	Sentido	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	MTAt	
	Dirección de destino	MTAo	
	Puerto de fuente	0	
	Puerto de destino	7120	
	DSCP	9	Valor que indica el tipo de paquete en sentido descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

El CMTSo responde a la instrucción establecimiento de puerta con un acuse de recibo.

GATE-SET-ACK (acuse de establecimiento de puerta)

ID de transacción		3177	
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Total de actividad		4	Número total de conexiones establecidas por este cliente.

3) Cuando el MTAo recibe información de señalización de llamada, envía un mensaje RSVP-PATH que va dirigido al MTAt pero tiene validado el bit Aviso a encaminadores (Router-Alert) en la cabecera IP. Los encaminadores intermedios de la red LAN propia interceptan, procesan y reenvían este mensaje como un mensaje RSVP-PATH normal.

RSVP-PATH (trayecto RSVP)

Objeto Sesión	Protocolo	UDP	Parámetros que identifican la sesión RSVP, concuerdan con la autorización previamente enviada por el controlador de puerta y se utilizan en los clasificadores de QoS.
	Dirección destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Tspec de emisor	r	12000	Parámetros de tráfico negociados solicitados para esta llamada. El CMTS calcula los parámetros efectivos de QoS en sentido ascendente utilizando estos parámetros Tspec y Rspec. Es un objeto RSVP normalizado que será interpretado por todos los encaminadores intermedios en el trayecto entre el MTA y el CMTS.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
Rspec hacia adelante	R	12000	
	S	0	
Sesión hacia atrás	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al CMTS información suficiente para calcular los parámetros de tráfico descendente y generar un mensaje RSVP-PATH para el flujo descendente.
	Dirección destino	MTAo	
	Puerto de destino	7120	
Plantilla de emisor hacia atrás	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Tspec de emisor hacia atrás	r	12000	Parámetros de tráfico negociados solicitados para esta llamada. El CMTS calcula los parámetros efectivos de QoS en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un objeto RSVP nuevo que no será considerado por los encaminadores intermedios.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	0	
	VAD	Desact.	
Rspec hacia atrás	R	12000	
	S	0	
ID de puerta		37125	

4) El CMTS utiliza el mensaje RSVP-PATH y calcula los parámetros de QoS para el enlace J.112. El CMTS envía el mensaje DSA-REQ siguiente al CM, que se utiliza para establecer los parámetros en sentido ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 120 (Tspec) más 18 (tara Ethernet) menos 40 (valor de supresión de cabecera) más 13 (tara J.112). Para la supresión de cabecera, cuya longitud se ha especificado en RSVP-PATH (40), se trata de los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se lee en el paquete RSVP.

DSA-REQ

ID de transacción		1
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado admitido	200
	Program. flujo de servicio	UGS (6)
	Política de petición/transmis.	0x00000017
	Intervalo de autoriz. nominal	10 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño de autorización sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquetes ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquetes	3001
	Prioridad del clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección IP fuente	MTAo
	Puerto IP fuente	7120
	Dirección IP destino	MTAt
	Puerto IP destino	7000
	Protocolo IP	UDP (17)
Clasificación de paquetes descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquetes	3002
	Prioridad del clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección IP fuente	MTAt
	Dirección IP destino	MTAo
	Puerto IP destino	7120
	Protocolo IP	UDP (17)

DSA-REQ

Supresión de cabecera de cabida útil	Identif. del clasificador	3001
	Identif. flujo de servicio	1001
	Indice supresión de cabecera	1
	Campo supresión cabecera	<42bytes>
	Máscara supresión cabecera	<42bits>
	Tamaño supresión cabecera	42
	Verificac. supresión cabecera	Verificar (0)
HMAC		

5) Simultáneamente con el mensaje N.° 4, el CMTS inicia las reservas en la red trocal necesarias para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del ámbito de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación que sea necesaria para indicar que la reserva se ha realizado con éxito.

6) El CM verifica los recursos que debe asignar (por ejemplo, espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado del clasificador, ancho de banda de la red local) e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSA-RSP con resultado positivo.

DSA-RSP

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

7) Cuando recibe el mensaje DSA-RSP el CMTS acusa recibo con un mensaje DSA-ACK.

DSA-ACK

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

8) Cuando se completa la reserva J.112 y se ha realizado con éxito la reserva en la red troncal, el CMTS responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. El mensaje incluye el identificador de recurso que el CMTS asigna a esta conexión. La dirección fuente del mensaje RSVP-RESV es MTAt y la dirección de destino MTAo. Todos los encaminadores intermedios lo interceptarán, procesarán y reenviarán como un mensaje RSVP-RESV normalizado.

RSVP-RESV (reserva RSVP)

Objeto Sesión	Protocolo	UDP	Campos que identifican el flujo IP para el que se establece la reserva.
	Dirección destino	MTAt	
	Puerto de destino	7000	
Especificación de flujo	r	12000	Campos que identifican los recursos reservados para este flujo.
	b	120	
	p	12000	
	m	120	
	M	120	

RSVP-RESV (reserva RSVP)

	R	12000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

9) Si la dirección del tramo anterior es diferente de la dirección de fuente, el CMTS debe generar un mensaje RSVP-PATH a fin de reservar recursos en sentido descendente en todos los encaminadores intermedios. Esta condición sólo se cumple si el MTA no es inmediatamente adyacente al CM.

En este ejemplo, supóngase que hay un encaminador intermedio entre el MTAo y su CM, pero no entre el MTAt y su CM.

El CMTS construye un mensaje RSVP-PATH utilizando la información de trayecto hacia atrás que ha recibido en el mensaje RSVP-PATH, y lo envía al MTA de origen. El mensaje incluye el objeto ID de recurso.

RSVP-PATH (trayecto RSVP)

Objeto Sesión	Protocolo	UDP	El objeto Sesión y la plantilla de emisor se reproducen como si el mensaje RSVP procediese del extremo lejano.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Especificación de tráfico del emisor	r	12000	Sender-Tspec se toma de la especificación del emisor hacia atrás (Reverse-Sender-Tspec) incluida en el mensaje RSVP-PATH del MTAo. Identifica los recursos que serán necesarios en sentido descendente (del MTAt al MTAo).
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
Especificación de recurso hacia adelante	R	12000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

10) En respuesta al mensaje RSVP-PATH (9), el MTAo envía al MTAt un mensaje RSVP-RESV (reserva de RSVP). En este mensaje se valida el bit de aviso a encaminadores, de forma que todos los encaminadores intermedios lo interceptan, procesan y reenvían hasta alcanzar el CMTS.

RSVP-RESV (reserva RSVP)

Objeto Sesión	Protocolo	UDP	El objeto sesión y la plantilla de emisor se copian del mensaje RSVP-PATH recibido.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Especificación de filtro	Dirección de fuente	MTAt	
	Puerto de fuente	7000	

RSVP-RESV (reserva RSVP)

Especificación de flujo	r	12000	Estos valores también se copian del mensaje RSVP-PATH y especifican la cantidad de recursos reservados para el flujo.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
	R	12000	
	S	0	
ID de recurso		1	ID de recurso copiado de RSVP-PATH.

11) En respuesta a los mensajes de señalización que indican que se ha completado el establecimiento de la comunicación (el otro extremo ha descolgado), el MTAo envía al CMTS el mensaje COMMIT. Este mensaje se envía a un puerto UDP del CMTS determinado mediante señalización de llamada.

El objeto Sesión y la plantilla de emisor proporcionan al CMTS información suficiente para identificar la "puerta" y los recursos reservados que ahora se comprometen.

COMMIT (compromiso)

Objeto Sesión	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino deben concordar con los valores correspondientes al ID de puerta.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	

12) El CMTS determina cuáles son los recursos reservados que se han de activar y envía al CM un mensaje DSC-REQ para activar el flujo.

DSC-REQ

ID de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planificac. flujo servicio	UGS (6)
	Política de petición/transm	0x00000017
	Intervalo de autoriz. nominal	10 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000

DSC-REQ

Clasificación paquetes ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquetes	3001
	Acción reemplazo clasific.	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Activo (1)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MTAt
	Puerto destino IP	7000
	Protocolo IP (IPProtocol)	UDP (17)
Clasificación paquetes descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquetes	3002
	Acción reemplazo clasific.	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Activo (1)
	Dirección fuente IP	MTAt
	Puerto fuente IP	7000
	Dirección destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
HMAC		

13) El CM envía un mensaje DSC-RSP para indicar que la operación se ha realizado satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

14) El CMTS envía un mensaje DSC-ACK para indicar que ha recibido y tratado satisfactoriamente el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

15) El CMTS envía el mensaje de coordinación de puertas al CMTS distante para notificarle que se han comprometido los recursos en este extremo.

GATE-OPEN

ID de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
Identif. de puerta		1273	Gate-ID en el CMTS distante.

GATE-OPEN

Especificación de tráfico	r	12000	Parámetros de tráfico comprometidos y utilizados ahora en el sentido MTAo a MTAt.
	b	120	
	p	12000	
	m	120	
	M	120	
Especificación de tráfico hacia atrás	r	12000	Parámetros de tráfico previsibles y utilizados en el sentido MTAt a MTAo.
	b	120	
	p	12000	
	m	120	
	M	120	
HMAC			Suma de control de seguridad para este mensaje.

16) El CMTS distante responde a GATE-OPEN con el siguiente mensaje:

GATE-OPEN-ACK

ID de transacción		72	Identificador para concordancia de este mensaje y su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

17) El CMTS acusa recibo del mensaje COMMIT:

COMMIT-ACK (acuse de compromiso)

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino pueden facilitar la correlación del acuse de recibo con el mensaje COMMIT.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	

18) Al finalizar la llamada el MTA envía al CMTS el mensaje RSVP-PATH-TEAR. El MTA envía un mensaje RSVP-PATH-TEAR diferente para cada reserva RSVP.

RSVP-PATH-TEAR (Deshacer trayecto RSVP)

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino identifican el flujo RSVP.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	

19) Al recibir el mensaje RSVP-PATH-TEAR el CMTS envía el mensaje de coordinación de puertas al CMTS correspondiente adscrito al MTAt.

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para concordancia de este mensaje y su respuesta.
ID de puerta		1273	Identificador de la puerta en el CMTS distante.
HMAC			Suma de control de seguridad para este mensaje.

El CMTS distante responde con el siguiente mensaje:

GATE-CLOSE-ACK (acuse de cierre de puerta)

ID de transacción		73	Identificador para concordancia de este mensaje y su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

20) Al recibir el mensaje RSVP-PATH-TEAR el CMTS envía un mensaje DSD-REQ al CM indicando el identificador del flujo de servicio que debe eliminarse.

DSD-REQ

ID de transacción		3
ID del flujo de servicio		1001
HMAC		

DSD-REQ

ID de transacción		4
ID del flujo de servicio		2001
HMAC		

21) El CM suprime el identificador de flujo de servicio y envía la respuesta al CMTS.

DSD-RSP

ID de transacción		3
ID del flujo de servicio		1001
Código de confirmación		Positivo (0)
HMAC		

DSD-RSP

ID de transacción		4
ID del flujo de servicio		2001
Código de confirmación		Positivo (0)
HMAC		

22) El CMTS envía el mensaje RSVP-RESV-TEAR al MTA.

RSVP-RESV-TEAR

Objeto Sesión	Protocolo	UDP	Parámetros que identifican el flujo IP que finaliza.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	

Apéndice III

Ejemplo de intercambio de mensajes del protocolo para una llamada NCS básica entre elementos de la red para MTA autónomos

En este apéndice se hace una descripción de carácter informativo de la posible relación entre el protocolo de señalización de llamada (Rec. UIT-T J.162) y los métodos de QoS dinámica que pueden invocarse en distintos momentos del flujo de la llamada.

Cuando el MTA_O iniciador completa la marcación (el mapa de dígitos corresponde a un número telefónico completo), los dígitos se envían al CMS_O mediante un mensaje notificación. En la etapa inicial de una nueva llamada, el CMS_O indica al MTA_O que debe crear una nueva conexión inactiva. El MTA_O asigna un puerto para recepción del tren de medios y responde con un mensaje ACK que incluye la descripción de sesión que enumera todos los trenes de medios que el MTA_O está dispuesto a recibir. El CMS_O intercambia un mensaje GATE-ALLOC con el $CMTS_O$ para asignar un identificador de puerta (GateID) y pasa esta información al CMS_T de terminación junto con el perfil SDP del origen.

El CMS_T de terminación establece la puerta en el $CMTS_T$ de terminación (mediante una instrucción GATE-SET), que admite todos los flujos de medios que son aceptables para la parte iniciadora dentro de los límites de una "capacidad máxima autorizada" y permite que el puerto de destino sea libremente elegido en el MTA_T. El $CMTS_T$ también asigna un GateID y lo comunica al CMS_T. El CMS_T comunica el GateID local al MTA_T de terminación en una instrucción Creación de conexión junto con el perfil SDP propuesto. En su respuesta, el MTA_T indica el conjunto de trenes de medios que considera aceptables y el puerto asignado para la recepción de dichos trenes.

Llegado a este punto el MTA_T conoce el códec de emisión, el códec de recepción, la dirección y el puerto de destino para los paquetes vocales que envía, así como el puerto local para la recepción de paquetes vocales. Entonces puede iniciar la secuencia de reserva enviando al $CMTS_T$ un mensaje RSVP-PATH.

Cuando el CMS_O recibe el perfil SDP del MTA_T tiene información suficiente para establecer la puerta en el $CMTS_O$ y puede realizar la operación GATE-SET, incluyendo el ID de puerta distante y la dirección del $CMTS_T$. El CMS_O envía entonces al MTA_O una instrucción Modificación de conexión, informándole de la dirección de destino, el puerto y el códec que se debe utilizar. Entonces el MTA_O tiene información suficiente para reservar los recursos y al final envía al CMS_O un acuse de recibo positivo. Ahora el CMS_T indica al MTA_T que debe avisar al usuario que tiene una llamada entrante. El MTA_T verifica en primer lugar que la reserva de recursos que inició anteriormente se ha realizado satisfactoriamente y si es así envía la señal de llamada al teléfono.

Cuando la parte llamada responde, el MTA_T envía un mensaje de notificación al CMS_T para informar que la otra parte ha descolgado. Entonces el CMS_T envía una instrucción Modificación de conexión al MTA_T para validar el modo de conexión Emisión + Recepción; el MTA_T realiza el intercambio COMMIT con el $CMTS_T$ y envía el acuse de recibo. El CMS_O también envía una instrucción Modificación de conexión al MTA_O para validar el modo de conexión Emisión + Recepción, y esto a su vez hace que el MTA_O también realice el intercambio COMMIT con el $CMTS_O$. La comunicación queda entonces establecida.

Cualquiera de las partes puede iniciar una terminación de llamada enviando un mensaje notificación a su CMS para indicar que ha colgado. Este caso se representa en el diagrama para el MTA_O. El CMS_O responde a la notificación de colgado enviando una instrucción Supresión de conexión que inicia la secuencia RSVP-PATH-TEAR (deshacer trayecto RSVP) para liberar los recursos. Se informa al MTA_T que se ha colgado mediante señalización de llamada (una instrucción Supresión de conexión que no se muestra en el diagrama) o mediante el mensaje de DQoS RSVP-RESV-TEAR (deshacer reserva RSVP). Al colgar posteriormente el MTA_T produce el mismo mensaje notificación, tal como hizo anteriormente el MTA_O, y termina la secuencia. Véase la figura III.1.

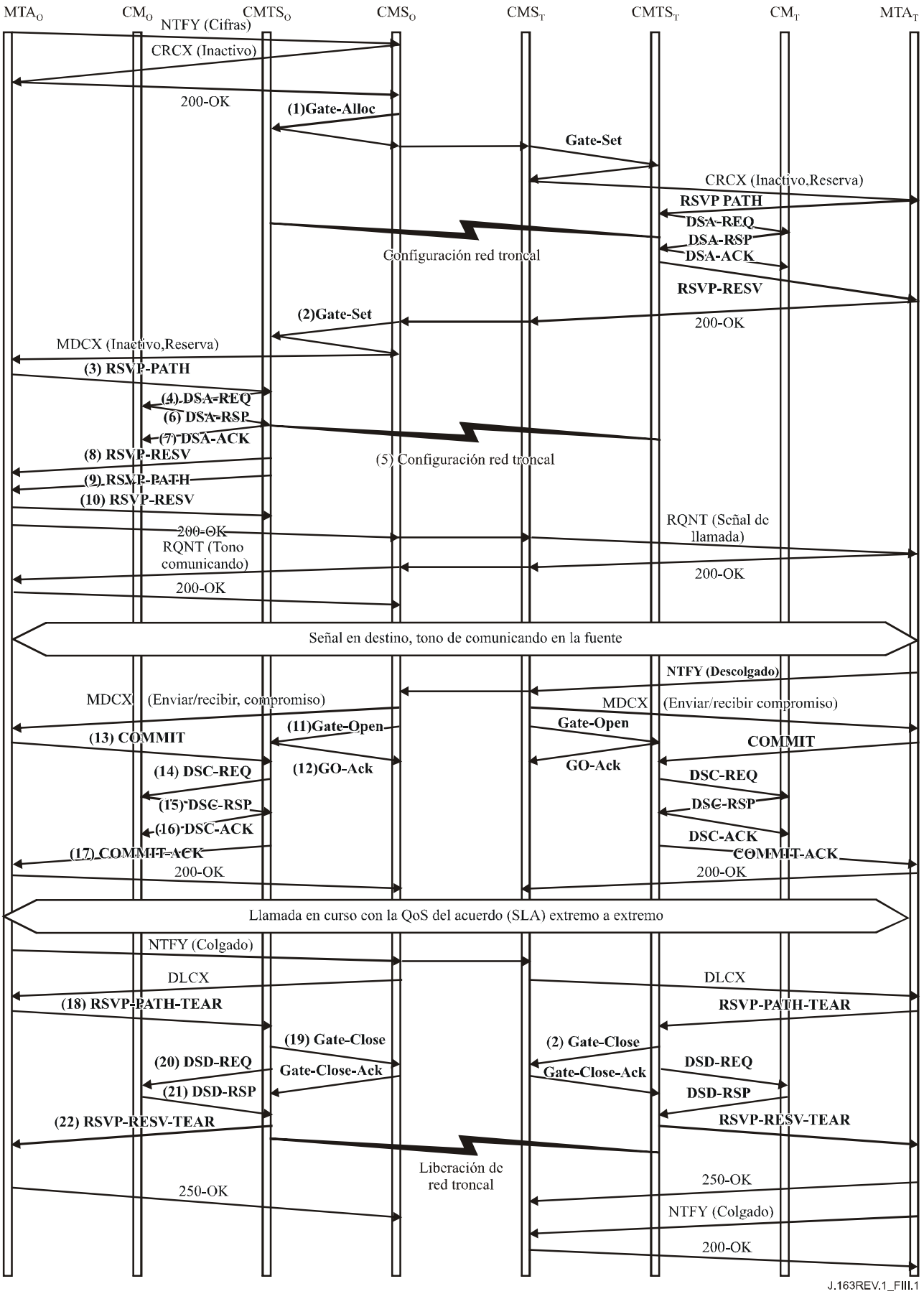


Figura III.1/J.163 – Flujo de llamada básica – NCS

1) Al recibir información de señalización del MTAo el CMSo verifica el consumo actual de recursos del MTAo consultando al CMTSo.

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos que utiliza este punto extremo.
Total de actividad		12	Número máximo de conexiones permitidas por cliente.

El CMTSo verifica la utilización actual de recursos por parte del MTAo y responde indicando el número de conexiones activas.

GATE-ALLOC-ACK (acuse de asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos que utiliza este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Total de actividad		3	Número máximo de conexiones establecidas por este cliente.

2) Tras un intercambio adicional de señalización, el CMSo autoriza que el CMTSo admita la nueva conexión.

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección	CMSo	Información necesaria para realizar la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas. Indica que el CMTS no debería enviar un mensaje apertura de puerta cuando recibe un mensaje COMMIT del MTA, sino esperar a recibir un mensaje apertura de puerta del CMSo.
	Puerto	2052	
	ID de puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	No enviar apertura de puerta	
Información de generación de eventos	Dirección RKS	RKS	Dirección del servidor de mantenimiento de registros (RKS).
	Puerto RKS	3288	Puerto en el servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Sentido	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utilizan en los clasificadores de QoS.
	Dirección de fuente	MTAo	
	Dirección de destino	MTAt	
	Puerto de fuente	0	
	Puerto de destino	7000	
	DSCP	6	Valor que indica el tipo de paquete en sentido ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
Especificación de puerta	Sentido	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	MTAt	
	Dirección de destino	MTAo	
	Puerto de fuente	0	
	Puerto de destino	7120	
	DSCP	9	Valor que indica el tipo de paquete en sentido descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

El CMTSo responde a la instrucción establecimiento de puerta con un acuse de recibo.

GATE-SET-ACK (acuse de establecimiento de puerta)

ID de transacción		3177	
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Total de actividad		3	Número total de conexiones establecidas por este cliente.

3) Al recibir una instrucción Modificación de conexión el MTAo envía un mensaje RSVP-PATH que va dirigido al MTAt pero tiene validado el bit Aviso a encaminadores en la cabecera IP. Los encaminadores intermedios en la red LAN propia interceptan, procesan y retransmiten este mensaje como un mensaje RSVP-PATH normal.

RSVP-PATH (trayecto RSVP)

Objeto Sesión	Protocolo	UDP	Parámetros que identifican la sesión RSVP, concuerdan con la autorización enviada previamente por el controlador de puerta y se utilizan en los clasificadores de QoS.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Tspec de emisor	r	12000	Parámetros de tráfico negociados que se solicitan efectivamente para esta llamada. El CMTS calcula los parámetros de QoS efectivos en sentido ascendente utilizando estos parámetros Tspec y Rspec. Es un objeto RSVP normalizado que será interpretado por todos los encaminadores intermedios en el trayecto entre el MTA y el CMTS.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec hacia adelante	R	12000	
	S	0	
Sesión hacia atrás	Protocolo	UDP	Objetos RSVP nuevos que proporcionan al CMTS información suficiente para calcular los parámetros de tráfico descendente y generar un mensaje RSVP-PATH para el flujo descendente.
	Dirección de destino	MTAo	
	Puerto de destino	7 120	
Plantilla de emisor hacia atrás	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Tspec de emisor hacia atrás	r	12000	Parámetros de tráfico negociados que se solicitan efectivamente para esta llamada. El CMTS calcula los parámetros de QoS efectivos en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que no será considerado por los encaminadores intermedios.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión de cabecera	0	
	VAD	Desact.	

RSVP-PATH (trayecto RSVP)

Rspec hacia atrás	R	12000	
	S	0	
ID de puerta		37125	

4) El CMTS utiliza el mensaje RSVP-PATH y calcula los parámetros de QoS para el enlace J.112. El CMTS envía al CM el siguiente mensaje DSA-REQ que se utiliza para establecer los parámetros de los flujos ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 120 (Tspec) más 18 (tara Ethernet) menos 40 (valor de supresión de cabecera) más 13 (tara J.112). Para la supresión de cabecera, cuya longitud se ha especificado en RSVP-PATH (40), se trata de los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se lee en el paquete RSVP.

DSA-REQ

ID de transacción		1
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Admitido	200
	Program. flujo de servicio	UGS (6)
	Política de petición/transmis.	0x00000017
	Intervalo de autoriz. nominal	10 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquetes ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquetes	3001
	Prioridad del clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección IP fuente	MTAo
	Puerto IP fuente	7120
	Dirección IP destino	MTAt
	Puerto IP destino	7000
	Protocolo IP	UDP (17)
Clasificación de paquetes descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquetes	3002
	Prioridad del clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección IP fuente	MTAt
	Puerto IP fuente	7000
	Dirección IP destino	MTAo

DSA-REQ

Supresión de paquetes descendente	Puerto IP destino	7120
	Protocolo IP	UDP (17)
Supresión de cabecera de cabida útil	Identif. del clasificador	3001
	Identif. flujo de servicio	1001
	Índice supresión de cabecera	1
	Campo supresión cabecera	<42 bytes>
	Máscara supresión cabecera	<42 bits>
	Tamaño supresión cabecera	42
	Verificac. supresión cabecera	Verificar (0)
HMAC		

5) Simultáneamente con el mensaje N.° 4 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio solicitada. El contenido de este mensaje es función de los algoritmos específicos que se utilicen en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación que sea necesaria para indicar que la reserva se ha realizado satisfactoriamente.

6) El CM verifica los recursos que debe asignar (por ejemplo, espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado clasificador, ancho de banda en red local) e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSA-RSP con resultado positivo.

DSA-RSP

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

7) Cuando recibe el mensaje DSA-RSP, el CMTS acusa recibo con un mensaje DSA-ACK.

DSA-ACK

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

8) Cuando se completa la reserva J.112 y se ha realizado con éxito la reserva en la red troncal, el CMTS responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. El mensaje incluye el identificador de recurso que el CMTS asigna a esta conexión. La dirección fuente del mensaje RSVP-RESV es MTAt y la dirección de destino MTAo. Todos los encaminadores intermedios lo interceptarán, procesarán y reenviarán como un mensaje RSVP-RESV normalizado.

RSVP-RESV (reserva RSVP)

Objeto Sesión	Protocolo	UDP	Campos que identifican el flujo IP para el que se establece la reserva.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Especificación de filtro	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Especificación de flujo	r	12000	Campos que identifican los recursos reservados para este flujo.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

9) Si la dirección del tramo anterior es diferente de la dirección de fuente, el CMTS debe generar un mensaje RSVP-PATH a fin de reservar recursos en sentido descendente en todos los encaminadores intermedios. Esta condición sólo se cumple si el MTA no es inmediatamente adyacente al CM.

En este ejemplo, supóngase que hay un encaminador intermedio entre el MTAo y su CM, pero no entre el MTAt y su CM.

El CMTS construye un mensaje RSVP-PATH utilizando la información de trayecto hacia atrás que ha recibido en el mensaje RSVP-PATH, y lo envía al MTA iniciador. El mensaje incluye el objeto ID de recurso.

RSVP-PATH (trayecto RSVP)

Objeto Sesión	Protocolo	UDP	El objeto Sesión y la plantilla de emisor se reproducen como si el mensaje RSVP procediese del extremo lejano.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Especificación de tráfico del emisor	r	12000	Sender-Tspec se toma de la especificación del emisor hacia atrás (Reverse-Sender-Tspec) incluida en el mensaje RSVP-PATH del MTAo. Identifica los recursos que serán necesarios en sentido descendente (del MTAt al MTAo).
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
Especificación de recursos hacia adelante	R	12000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

10) En respuesta al mensaje RSVP-PATH (9), el MTAo envía al MTAt un mensaje RSVP-RESV (reserva de RSVP). En este mensaje se valida el bit de aviso a encaminadores, de forma que todos los encaminadores intermedios lo interceptan, procesan y reenvían hasta alcanzar el CMTS.

RSVP-RESV (reserva RSVP)

Objeto Sesión	Protocolo	UDP	El objeto Sesión y la plantilla de emisor se copian del mensaje RSVP-PATH recibido.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Especificación de flujo	r	12000	Estos valores también se copian del mensaje RSVP-PATH y especifican la cantidad de recursos reservados para el flujo.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
	R	12000	
	S	0	
ID de recurso		1	ID de recurso copiado de RSVP-PATH.

11) El CMS envía al CMTS el mensaje de coordinación de puertas para informar que los recursos se deberían comprometer. Si el CMTS no recibe un mensaje COMMIT del MTA en el plazo del temporizador T2, anulará la conexión.

GATE-OPEN

ID de transacción		8096	Identificador para concordancia de este mensaje y la respuesta.
ID de puerta		37125	Gate-ID en el CMTS distante.
HMAC			Suma de control de seguridad para este mensaje.

12) El CMTS responde al mensaje GATE-OPEN:

GATE-OPEN-ACK

ID de transacción		8096	Identificador para concordancia de este mensaje y la respuesta.
HMAC			Suma de control de seguridad para este mensaje.

13) En respuesta a la instrucción Modificar conexión, que indica que se ha completado el establecimiento de la comunicación (el otro extremo ha descolgado), el MTAo envía al CMTS el mensaje COMMIT. Este mensaje se envía a un puerto UDP del CMTS determinado por el objeto Entidad para compromiso del mensaje RSVP-RESV. El objeto Sesión y la plantilla de emisor proporcionan al CMTS información suficiente para identificar la "puerta" y los recursos reservados que ahora se comprometen.

COMMIT (compromiso)

Objeto Sesión	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino deben concordar con los valores correspondientes al ID de puerta.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	

14) El CMTS determina cuáles son los recursos reservados que se han de activar y envia al CM un mensaje DSC-REQ para activar el flujo.

DSC-REQ

ID de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planificac. flujo servicio	UGS (6)
	Política de petición/transm	0x00000017
	Intervalo de autoriz. nominal	10 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	111

DSC-REQ

Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico)	5
	Veloc. máxima soportada	12000
Clasificación paquetes ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquetes	3001
	Acción reemplazo clasific.	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Activo (1)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MTAt
	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificación paquetes descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquetes	3002
	Acción reemplazo clasific.	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Activo (1)
	Dirección fuente IP	MTAt
	Puerto fuente IP	7000
	Dirección destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
HMAC		

15) El CM envía un mensaje DSC-RSP para indicar que la operación se ha realizado satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

16) El CMTS envía un mensaje DSC-ACK para indicar que ha recibido y tratado satisfactoriamente el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

17) El CMTS acusa recibo del mensaje COMMIT:

COMMIT-ACK (acuse de compromiso)

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino pueden facilitar la correlación del acuse de recibo con el mensaje COMMIT.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	

18) Al finalizar la llamada y en respuesta a una instrucción Suprimir conexión, el MTA envía al CMTS el mensaje RSVP-PATH-TEAR. El MTA envía un mensaje RSVP-PATH-TEAR diferente para cada reserva RSVP.

RSVP-PATH-TEAR (Deshacer trayecto RSVP)

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino identifican el flujo RSVP.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	

19) Al recibir el mensaje RSVP-PATH-TEAR el CMTS envía el mensaje de coordinación de puertas a la dirección indicada antes por la instrucción GATE-SET (el agente de llamada en el caso de NCS)

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para concordancia de este mensaje y su respuesta.
ID de puerta		8095	Identificador de la puerta en el CMTS distante.
HMAC			Suma de control de seguridad para este mensaje.

El CMS responde con el siguiente mensaje:

GATE-CLOSE-ACK (acuse de cierre de puerta)

ID de transacción		73	Identificador para concordancia de este mensaje y su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

20) Al recibir el mensaje RSVP-PATH-TEAR el CMTS envía un mensaje DSD-REQ al CM indicando el identificador del flujo de servicio que debe eliminarse.

DSD-REQ

ID de transacción		3
ID del flujo de servicio		1001
HMAC		

DSD-REQ

ID de transacción		4
ID del flujo de servicio		2001
HMAC		

21) El CM suprime el identificador de flujo de servicio y envía la respuesta al CMTS.

DSD-RSP

ID de transacción		3
ID del flujo de servicio		1001
Código de confirmación		Positivo (0)
HMAC		

DSD-RSP

ID de transacción		4
ID del flujo de servicio		2001
Código de confirmación		Positivo (0)
HMAC		

22) El CMTS envía el mensaje RSVP-RESV-TEAR al MTA.

RSVP-RESV-TEAR

Objeto Sesión	Protocolo	UDP	Parámetros que identifican el flujo IP que finaliza.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	

Apéndice IV

Ejemplo de intercambio de mensajes de protocolo para el cambio de códec durante la llamada

Los MTA realizan el cambio de códec transmitiendo un nuevo mensaje RSVP-PATH después del intercambio de señalización de llamada entre ellos que permite determinar el nuevo códec a utilizar. La nueva especificación de flujo para la llamada, que se describe en el mensaje RSVP-PATH, ha de estar dentro de los límites de la capacidad máxima autorizada especificada en el mensaje establecimiento de puerta que anteriormente han intercambiado los GC y los CMTS para esta puerta. El RSVP-PATH incluye el mismo ID de puerta que se había utilizado previamente para esta llamada. En el mensaje INVITE (invitación) inicial para establecer la comunicación se han debido incluir los códecs, en el SDP, para crear una capacidad máxima autorizada suficiente que permita hacer el cambio de módem.

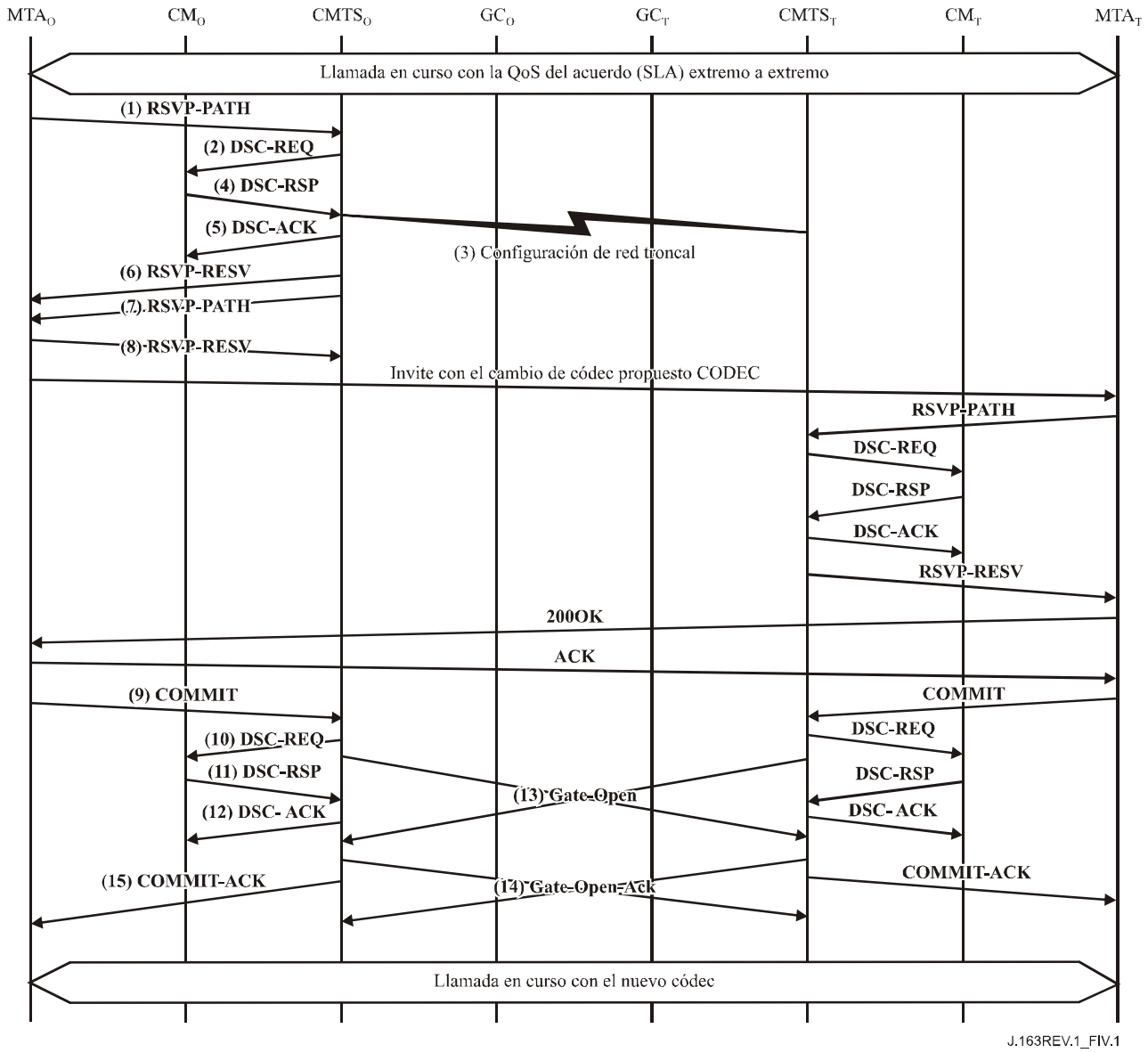


Figura IV.1/J.163 – Señalización de QoS para el cambio de códec

1) Se supone que el MTAo y el MTAt tienen una llamada activa G.728 (paquetes de 20 ms, cada uno con 80 bytes) cuando el MTAo decide, por cualquier motivo, que es necesario cambiar al CÓDEC G.711 (paquetes de 10 ms, cada uno de 120 bytes). Después de un intercambio inicial de señalización que determina que el MTAt puede aceptar el nuevo CÓDEC, el MTAo envía un mensaje RSVP-PATH que va dirigido al MTAt pero tiene validado el bit de aviso a encaminadores en la cabecera IP. Los encaminadores intermedios en la LAN propia interceptan, procesan y reencaminan este mensaje como un mensaje RSVP-PATH normal, del que sólo pueden interpretar el conjunto de parámetros de tráfico especificado en Sender-Tspec y que constituyen el mínimo valor superior.

RSVP-PATH (trayecto RSVP)

Objeto Sesión	Protocolo	UDP	Parámetros que identifican la sesión RSVP, concuerdan con la autorización previamente enviada por el controlador de puerta y también se utilizan en los clasificadores de QoS.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Especificación de tráfico del emisor	r	12000	Estos parámetros constituyen el mínimo valor superior de todos los parámetros de tráfico para los dos flujos posibles. Es un objeto RSVP normalizado que será interpretado por todos los encaminadores intermedios en el trayecto entre el MTA y el CMTS.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
Especificación de recursos hacia adelante	R	12000	
	S	0	
Sesión hacia atrás	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al CMTS información suficiente para calcular los parámetros de tráfico descendente y generar un mensaje RSVP-PATH para el flujo descendente.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Plantilla de emisor hacia atrás	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
Especificación de tráfico del emisor hacia atrás	r	12000	Parámetros de tráfico negociados para el nuevo CÓDEC solicitado para esta llamada. El CMTS calcula los parámetros de QoS efectivos en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que no será considerado por los encaminadores intermedios.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	0	
	VAD	Desact.	
Especificación de recursos hacia atrás	R	12000	
	S	0	
ResourceID		472	Identificador de recurso asignado para esta llamada.
Gate-ID		37125	Identificador de la puerta que autoriza esta petición.

2) El CMTS utiliza el mensaje RSVP-PATH y calcula los nuevos parámetros de QoS para el enlace J.112. Dado que el tren G.728 corresponde a una asignación para G.711, no es necesario otro flujo de servicio y los flujos de servicio existentes se modifican para incrementar la anchura de banda admitida. El CMTS envía al CM el siguiente mensaje DSC-REQ que se utiliza para establecer los parámetros en sentido ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 120 (Tspec) más 18 (tara Ethernet) menos 40 (valor de supresión de cabecera) más 13 (tara J.112). Para la supresión de cabecera, cuya longitud se ha especificado en RSVP-PATH (40), se trata de

los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se lee en el paquete RSVP.

DSC-REQ (petición DSC)

ID de transacción		1
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificación flujo de servicio	UGS (6)
	Política de petición/transmis.	0x00000017
	Intervalo de autoriz. nominal	10 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño de autorización sin petición	111
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Activo (4)
	Plazo estado Activo	10
	Planificación flujo de servicio	UGS (6)
	Intervalo de autoriz. nominal	20 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño de autorización sin petición	71
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Velocidad máxima sostenida	12000
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Activo (4)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Velocidad máxima sostenida	4000
HMAC		

3) Simultáneamente con el mensaje N.° 2 el CMTS inicia las reservas de la red troncal necesarias para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del ámbito de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación que sea necesaria para indicar que la reserva se ha hecho satisfactoriamente.

4) El CM verifica los recursos adicionales que debe asignar (por ejemplo, anchura de banda de red local). Si la operación se realiza satisfactoriamente devuelve el mensaje DSC-RSP (respuesta DSC) con resultado positivo.

DSC-RSP (respuesta DSC)

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

5) Cuando el CMTS recibe el DSC-RSP acusa recibo con un mensaje DSA-ACK (acuse de recibo DSA).

DSC-ACK (acuse de recibo DSA)

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

6) Con la reserva J.112 y después de realizar satisfactoriamente la reserva en la red troncal, el CMTS responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. Este mensaje incluye el mínimo valor superior de las dos Tspec de emisor, de forma que los encaminadores intermedios asignen recursos suficientes para cualquiera de los dos flujos. La dirección fuente del mensaje RSVP-RESV es MTAt y la dirección de destino MTAo. Todos los encaminadores intermedios lo interceptarán, procesarán y reenviarán como un mensaje RSVP-RESV normalizado.

RSVP-RESV (reserva RSVP)

Objeto Sesión	Protocolo	UDP	Campos que identifican el flujo IP para el que se establece la reserva.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Especificación de filtro	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Especificación de flujo	r	12000	Campos que identifican los recursos reservados para este flujo. Constituyen el mínimo valor superior de las dos Tspec incluidas en RSVP-PATH.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
ID de recurso		1	ID de recurso previamente creado para esta reserva.

7) Si la dirección del tramo anterior es diferente de la dirección de fuente, el CMTS debe generar un mensaje RSVP-PATH a fin de reservar recursos en sentido descendente en todos los encaminadores intermedios. Esta condición sólo se cumple si el MTA no es inmediatamente adyacente al CM.

El CMTS construye un mensaje RSVP-PATH utilizando la información de trayecto hacia atrás que ha recibido en el mensaje RSVP-PATH, y lo envía al MTA iniciador. El mensaje incluye el objeto ID de recurso.

RSVP-PATH (trayecto RSVP)

Objeto Sesión	Protocolo	UDP	El objeto Sesión y la plantilla de emisor se reproducen como si el mensaje RSVP procediese del extremo lejano.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Plantilla de emisor	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
Especificación de tráfico del emisor	r	12000	Tspec de emisor reproduce los valores de Tspec de emisor hacia atrás comunicados en el mensaje RSVP-PATH procedente del MTAo. Identifica los recursos que serán necesarios en sentido descendente (del MTAt al MTAo). Esta Tspec es el mínimo valor superior de las dos Tspec enviadas al CMTS y hace que todos los encaminadores intermedios asignen recursos suficientes para cualquiera de los flujos.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
Rspec hacia adelante	R	12000	
	S	0	
ID de recurso		1	ID de recurso previamente creado para esta reserva.

8) En respuesta al RSVP-PATH (7) el MTAo envía al MTAt un mensaje RSVP-RESV. En este mensaje se valida el bit de aviso a encaminadores, de forma que todos los encaminadores intermedios lo interceptan, procesan y reenvían hasta alcanzar el CMTS.

RSVP-RESV (reserva RSVP)

Objeto Sesión	Protocolo	UDP	El objeto Sesión y la plantilla de emisor se copian del mensaje RSVP-PATH recibido.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Especificación de filtro	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
Especificación de flujo	r	12000	Los valores de estos parámetros también se copian del mensaje RSVP-PATH y especifican la cantidad de recursos reservados para el flujo.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
	R	12000	
	S	0	
ID de recurso		1	ID de recurso copiado del RSVP-PATH.

9) En respuesta a los mensajes de señalización extremo a extremo que indican que los recursos fueron reservados satisfactoriamente en ambos extremos, el MTAo envía al CMTS el mensaje COMMIT. Este mensaje se envía a un puerto UDP del CMTS que se determina mediante señalización de llamada.

El objeto Sesión y la plantilla de emisor proporcionan al CMTS información necesaria para verificar el identificador de la puerta e identificar los recursos reservados que han sido comprometidos.

COMMIT (compromiso)

Objeto Sesión	Protocolo	UDP	Los valores de la cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino deben concordar con los valores del ID de puerta.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	

10) El CMTS determina cuáles son los recursos reservados que se han de activar y envia al CM un mensaje DSC-REQ para activar el flujo.

DSC-REQ

ID de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planificación flujo servic	UGS (6)
	Política de petición/transm.	0x00000017
	Intervalo de autoriz. nominal	10 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
HMAC		

11) El CM envía un mensaje DSC-RSP para indicar que la operación se ha realizado satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

12) El CMTS envía un mensaje DSC-ACK para indicar que ha recibido y tratado satisfactoriamente el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

13) El CMTS envía el mensaje de coordinación de puertas al CMTS distante para informarle que en este extremo se han comprometido los recursos.

GATE-OPEN (apertura de puerta)

ID de transacción		74	Identificador para la concordancia de este mensaje y su respuesta.
ID de puerta		1273	ID de puerta en el CMTS distante.
Tspec	r	12000	Parámetros de tráfico comprometidos que están siendo utilizados en el sentido de MTAo a MTAt.
	b	120	
	p	12000	
	m	120	
	M	120	
Tspec hacia atrás	r	12000	Parámetros de tráfico previsibles que están siendo utilizados en el sentido del MTAt al MTAo.
	b	120	
	p	12000	
	m	120	
	M	120	
HMAC			Suma de control de seguridad para este mensaje.

14) El CMTS distante responde al mensaje GATE-OPEN con:

GATE-OPEN-ACK (acuse de apertura de puerta)

ID de transacción		74	Identificador para la concordancia de este mensaje y su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

15) El CMTS acusa recibo del mensaje COMMIT con:

COMMIT-ACK (acuse de recibo de compromiso)

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino pueden ayudar a establecer la concordancia entre el acuse de recibo y el mensaje COMMIT.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	

Apéndice V

Ejemplo de intercambio de mensajes de protocolo para la retención de llamada

Para retener una llamada en un MTA se envía a éste un mensaje INVITE con los parámetros SDP puestos a cero, lo que hace que el MTA envíe un mensaje COMMIT cuya especificación de flujo es 0. También se incluye un ID de recurso, que permite al CMTS retener los recursos admitidos, pero no comprometer ningún recurso para este flujo. El proceso consiste en un intercambio de mensajes MAC al nivel de MAC J.112.

V.1 Ejemplo de flujo de llamada

Véase la figura V.1.

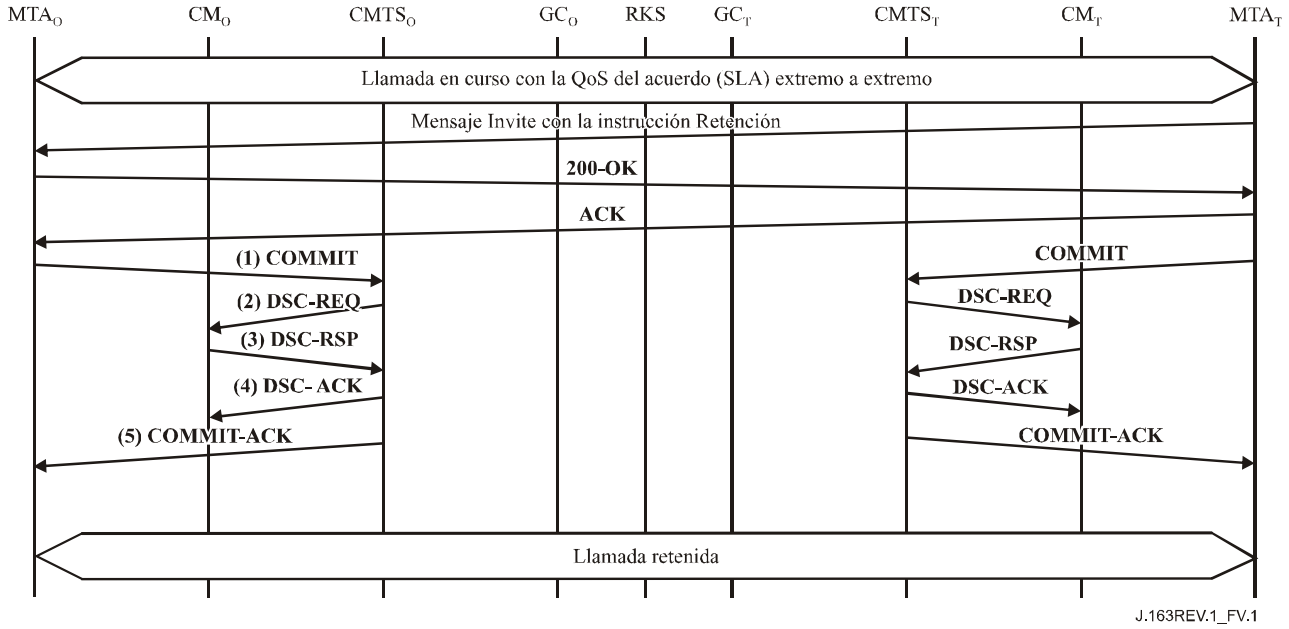


Figura V.1/J.163 – Señalización de QoS para retención de llamada

1) Para retener la llamada en curso el MTA envía un mensaje Commit especificando ancho de banda cero. El MTA no puede modificar el identificador de la sesión activa en un mensaje COMMIT para retención de la llamada.

COMMIT (compromiso)

Objeto Sesión	Protocolo	UDP	El objeto Sesión y la plantilla de emisor verifican la identidad de la puerta.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Plantilla de emisor	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
ID de puerta		37125	

COMMIT (compromiso)

Especificación de flujo	r	0	La especificación de flujo es un objeto opcional de un mensaje COMMIT. Puede indicar que la cantidad de recursos para esta activación es diferente de la reserva. En este caso, es una activación en sentido ascendente nula.
	b	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	
Especificación de flujo hacia atrás	r	0	La especificación de flujo es un objeto opcional de un mensaje COMMIT. Puede indicar que la cantidad de recursos para esta activación es diferente de la reserva. En este caso, es una activación en sentido descendente nula.
	b	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	

2) El CMTS envía al CM un mensaje DSC-REQ para desactivar el flujo de servicio y los clasificadores.

DSC-REQ

ID de transacción		1
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Política de petición/transmis.	0x00000017
	Intervalo de autoriz. nominal	10 ms
	Fluctuac. de autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño de autorización sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquetes ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquetes	3001
	Prioridad del clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección IP fuente	MTAo
	Puerto IP fuente	7120
	Dirección IP destino	MTAt

DSC-REQ

Clasificación de paquetes ascendente	Puerto IP destino	7000
	Protocolo IP	UDP (17)
Clasificación de paquetes descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquet	3002
	Prioridad del clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección IP fuente	MTAt
	Puerto IP fuente	7000
	Dirección IP destino	MTAo
	Puerto IP destino	7124
	Protocolo IP	UDP (17)
HMAC		

3) El CM envía un mensaje DSC-RSP para indicar que la operación se realizó satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

4) El CMTS envía un mensaje DSC-ACK para indicar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

5) El CMTS envía un mensaje COMMIT-ACK.

COMMIT-ACK (acuse de recibo de compromiso)

Objeto Sesión	Protocolo	UDP	El objeto Sesión y la plantilla de emisor verifican la identidad de la puerta.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Plantilla de emisor	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
ID de puerta		37125	

Apéndice VI

Ejemplo de intercambio de mensajes del protocolo para llamada en espera

VI.1 Ejemplo de flujo de llamada

Véase la figura VI.1.

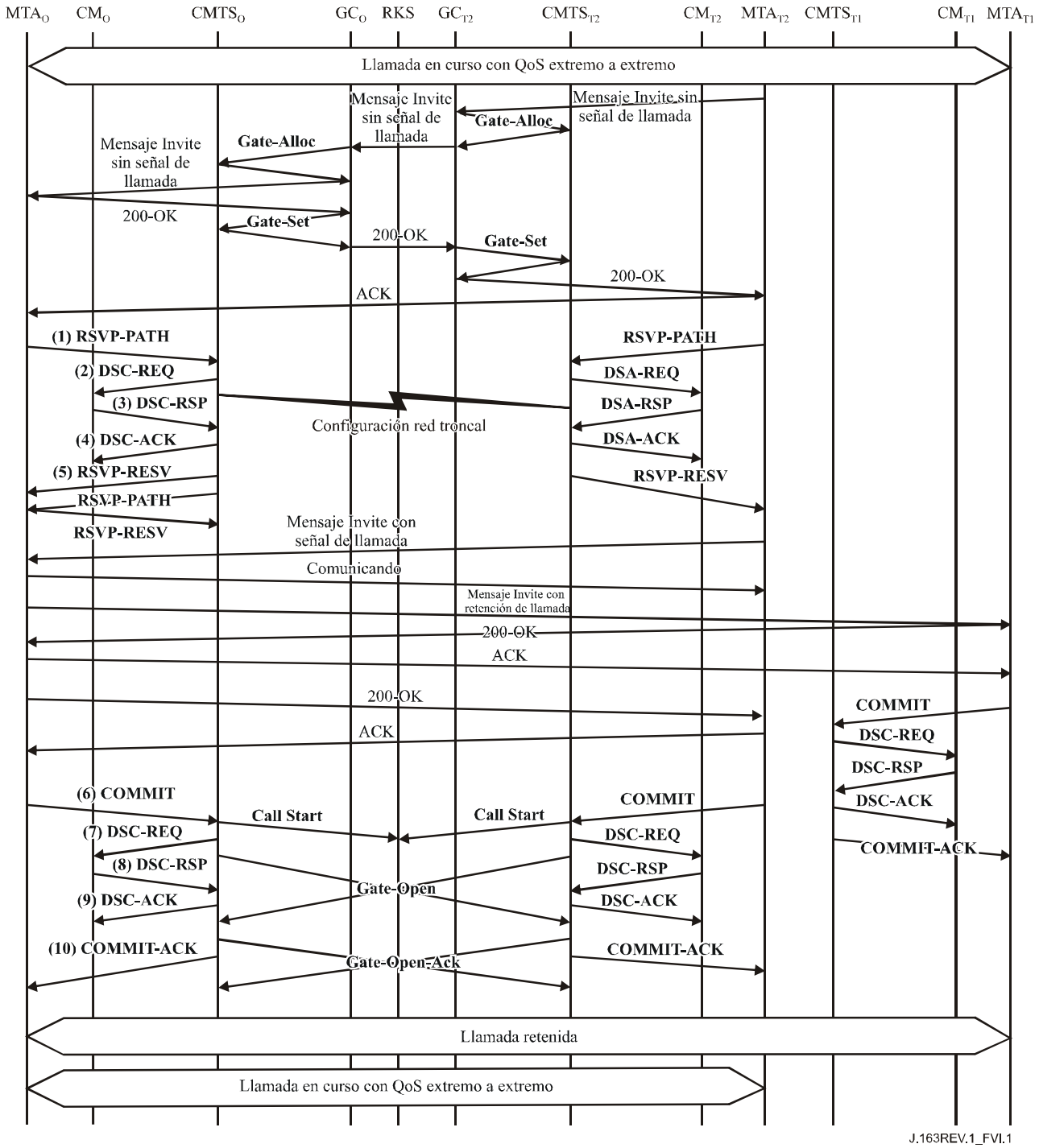


Figura VI.1/J.163 – Señalización de QoS para llamada en espera

1) El MTAo está conectado al MTAt1 y recibe una llamada entrante del MTAt2. En este ejemplo se supone que la llamada procedente del MTAt1 ha utilizado el puerto UDP 7120 y el ID de recurso asignado 472. Al recibir la información de señalización de llamada el MTAo envía un mensaje RSVP-PATH que está dirigido al MTAt2 pero tiene validado el bit de aviso a encaminadores en la cabecera IP. Los encaminadores intermedios en la LAN propia interceptan, procesan y reenvían este mensaje como un mensaje RSVP-PATH normal, asumiendo que se trata de un flujo diferente y asignándole recursos.

RSVP-PATH

Objeto Sesión	Protocolo	UDP	Parámetros del clasificador que concuerdan con la autorización enviada previamente por el controlador de puerta.
	Dirección de destino	MTAt2	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7122	
Especificación de tráfico del emisor	r	12000	Parámetros de tráfico negociados y efectivamente solicitados para esta llamada. El CMTS calcula los parámetros de QoS efectivos en sentido ascendente utilizando estos parámetros Tspec y Rspec. Es un objeto RSVP normalizado que será interpretado por todos los encaminadores intermedios en el trayecto entre el MTA y el CMTS.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec hacia adelante	R	12000	
	S	0	
Sesión hacia atrás	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al CMTS información suficiente para calcular los parámetros de tráfico descendente y generar un mensaje RSVP-PATH para el flujo descendente.
	Dirección de destino	MTAo	
	Puerto de destino	7122	
Plantilla de emisor hacia atrás	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Especificación de tráfico del emisor hacia atrás	r	12000	Parámetros de tráfico negociados y efectivamente solicitados para esta llamada. El CMTS calcula los parámetros de QoS efectivos en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que no será considerado por los encaminadores intermedios.
	b	120	
	p	12000	
	m	120	
	M	120	
	Supresión de cabecera	0	
	VAD	Desact.	
Rspec hacia atrás	R	12000	
	S	0	
ID de recurso		472	ID de recurso asignado para la llamada existente.
ID de puerta		37126	ID de puerta para esta nueva llamada que toma los recursos de la anterior.

2) El CMTS utiliza el mensaje RSVP-PATH y calcula los parámetros de QoS para el enlace J.112. En este ejemplo se supone que la llamada anterior también era G.711, lo que significa los mismos requisitos de ancho de banda. Por consiguiente, el flujo de servicio existente puede ser utilizado por ambos trenes de paquetes. El CMTS envía al CM el siguiente mensaje DSC-REQ que establece los nuevos clasificadores. La supresión de la cabecera, que según el mensaje RSVP-PATH supone una longitud de 40 bytes, resulta de los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se lee en el paquete RSVP.

DSC-REQ (petición DSC)

ID de transacción		1
Clasificación de paquete ascendente	Identificador flujo de servicio	1001
	Identif. clasificador de paquete	3003
	Acción modificación clasificador	Añadir (0)
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7122
	Dirección destino IP	MTAt2
	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Identificador flujo de servicio	2001
	Identif. clasificador de paquete	3004
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	MTAt2
	Dirección destino IP	MTAo
	Puerto destino IP	7122
	Protocolo IP	UDP (17)
Supresión de cabecera de cabida útil	Identificador del clasificador	3003
	Identif. flujo de servicio	1001
	Índice supresión de cabecera	1
	Campo supresión de cabecera	<42bytes>
	Máscara supresión de cabecera	<42bits>
	Tamaño supresión de cabecera	42
	Verificar supresión de cabecera	Verificar (0)
HMAC		

3) El CM verifica los recursos que debe asignar (por ejemplo, espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado clasificador, ancho de banda en red local) e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSC-RSP con resultado positivo.

DSC-RSP (respuesta DSC)

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

4) El CMTS que ha recibido el mensaje DSC-RSP acusa recibo mediante un mensaje DSC-ACK.

DSC-ACK (acuse de recibo DSC)

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

5) Una vez que se ha completado la reserva J.112 y se ha realizado satisfactoriamente la reserva en la red troncal, el CMTS responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV que incluye el ID de recurso asignado por el CMTS a esta conexión. La dirección fuente del mensaje RSVP-RESV es MTAt y la dirección de destino MTAo. Todos los encaminadores intermedios lo interceptarán, procesarán y reenviarán como un mensaje RSVP-RESV normalizado.

RSVP-RESV (reserva RSVP)

Objeto Sesión	Protocolo	UDP	Campos que identifican el flujo IP para el que se establece la reserva.
	Dirección destino	MTAt2	
	Puerto de destino	7000	
Especificación de filtro	Dirección de fuente	MTAo	
	Puerto de fuente	7122	
Especificación de flujo	r	12000	Campos que identifican los recursos reservados para este flujo.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
ID de recurso		472	ID de recurso para esta reserva.

6) En respuesta a una acción de conmutación entre llamadas (accionamiento del correspondiente interruptor del aparato telefónico) y habiendo terminado la señalización con las partes anteriores y las nuevas, el MTAo envía al CMTS el mensaje COMMIT. Este mensaje se dirige a un puerto UDP del CMTS determinado mediante señalización de llamada.

COMMIT (compromiso)

Objeto Sesión	Protocolo	UDP	Los valores de protocolo, dirección de destino, dirección de fuente y puerto de destino deben concordar con los valores del ID de puerta.
	Dirección destino	MTAt2	
	Puerto de destino	7000	
Plantilla de emisor	Dirección fuente	MTAo	
	Puerto de fuente	7122	
ID de puerta		37126	

7) El objeto Sesión y la plantilla del emisor proporcionan al CMTS información suficiente para identificar la "puerta" y los recursos reservados que se comprometen. Dado que en este mensaje no se incluyen Tspec, todos los recursos reservados quedarán activados. Todos los demás flujos que tienen asignado el mismo ID de recurso son desactivados.

8) El CMTS decide las reservas que se activan y envía al CM un mensaje DSC-REQ para activar el flujo.

DSC-REQ (petición DSC)

ID de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planific. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuac. autoriz. tolerada)	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12 000
Clasificador en sentido ascendente	Identif. flujo de servicio	1001
	Ident. clasif. de paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Inactivo (0)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MTAt
	Puerto destino IP	7000
	Protocolo IP	UDP (17)

DSC-REQ (petición DSC)

Clasificador en sentido descendente	Identif. flujo de servicio	2001
	Ident. clasif. de paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Inactivo (0)
	Dirección fuente IP	MTAt
	Puerto fuente IP	7000
	Dirección destino IP	MTAo
	Puerto destino IP	7120
	Protocolo IP	UDP (17)
Clasificación de paquetes en sentido ascendente	Identif. flujo de servicio	1001
	Ident. clasif. de paquete	3003
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Activo (1)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7122
	Dirección destino IP	MTAt2
	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificación de paquetes en sentido descendente	Identif. flujo de servicio	2001
	Ident. clasif. de paquete	3004
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Activo (1)
	Dirección fuente IP	MTAt2
	Puerto fuente IP	7000
	Dirección destino IP	MTAo
	Puerto destino IP	7122
	Protocolo IP	UDP (17)
HMAC		

9) El CM envía un mensaje DSC-RSP para indicar que la operación se ha realizado satisfactoriamente.

DSC-RSP (respuesta DSC)

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

10) El CMTS envía un mensaje DSC-ACK (acuse de recibo DSC) para indicar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-ACK (acuse de recibo DSC)

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

11) El CMTS acusa recibo del mensaje COMMIT con:

COMMIT-ACK (acuse de recibo de compromiso)

Objeto Sesión	Protocolo	UDP	Los valores de la cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino concuerdan con el ID de puerta.
	Dirección de destino	MTAt2	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7122	
ID de puerta		37126	

Apéndice VII

Ejemplo de intercambio de mensajes del protocolo de llamadas DCS básicas entre elementos de la red de un MTA integrado

Véase la figura VII.1.

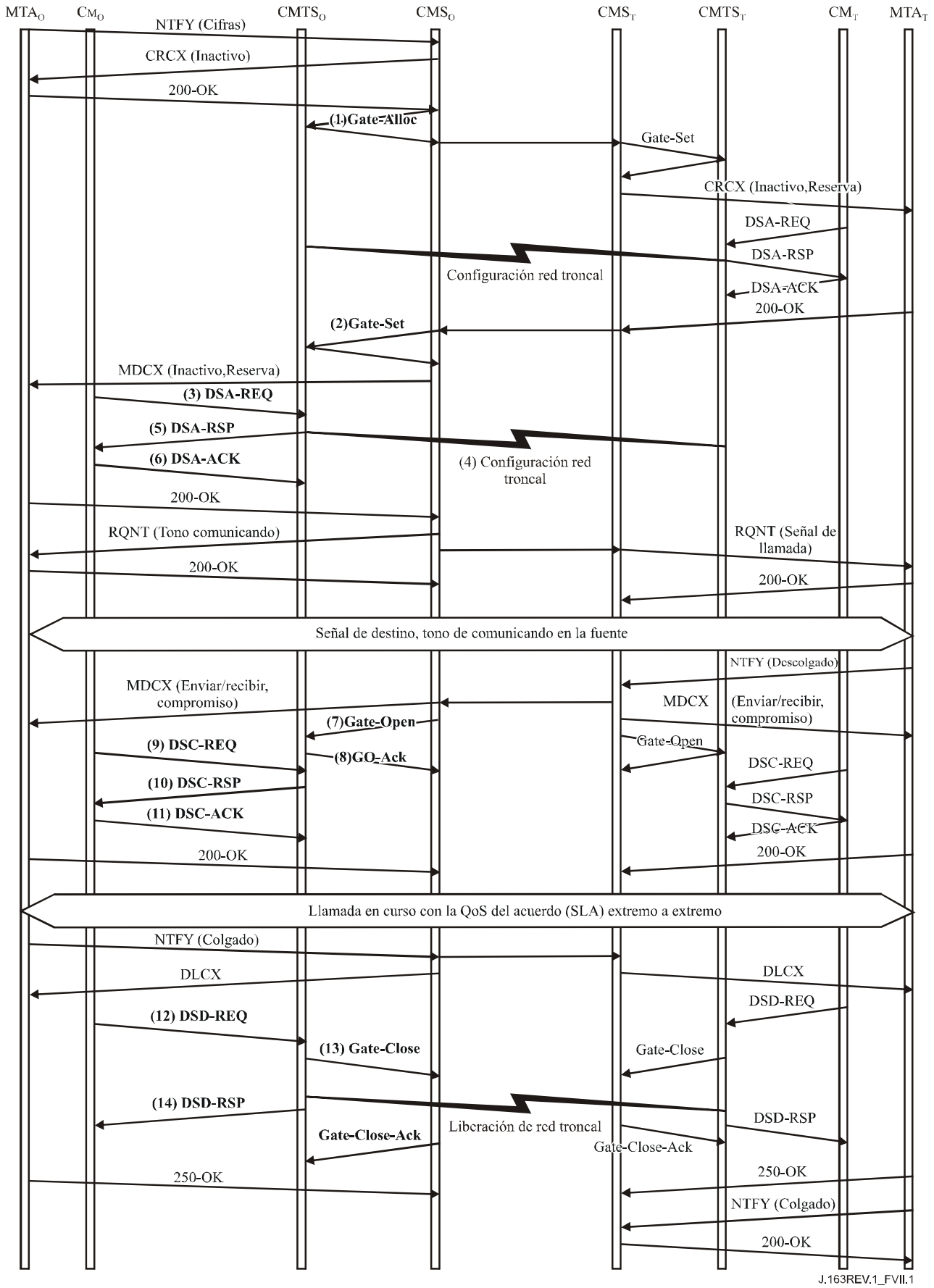


Figura VII.1/J.163 – Flujo de llamada básica – MTA integrado

1) Cuando el CMSo recibe información de señalización del MTAo verifica el consumo actual de recursos del MTAo consultando al CMTSo.

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
Total de actividad		4	Número máximo de conexiones permitidas por cliente.

El CMTSo verifica la utilización actual de recursos por parte del MTAo, y responde indicando el número de conexiones activas.

GATE-ALLOC-ACK (acuse de asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Total de actividad		3	Número total de conexiones establecidas por este cliente.

2) Tras un intercambio adicional de señalización el CMSo autoriza la admisión de la nueva conexión en el CMTSo.

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección CMTS	CMTSo	Información necesaria para la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas.
	Puerto CMTS	2052	
	ID de puerta distante	8095	
	Clave de seguridad	<key>	
Información de generación de eventos	Dirección RKS	RKS	Dirección del servidor de mantenimiento de registros (RKS).
	Puerto RKS	3288	Puerto del servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Sentido	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	MTAo	
	Dirección de destino	MTAt	
	Puerto de fuente	0	
	Puerto de destino	7000	
	DSCP	6	Valor del tipo de paquete en sentido ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
Especificación de puerta	Sentido	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	MTAt	
	Dirección de destino	MTAo	
	Puerto de fuente	0	
	Puerto de destino	7120	
	DSCP	9	Valor del tipo de paquete en sentido descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

El CMTSo responde a la instrucción establecimiento de puerta (Gate-Setup) con un acuse de recibo.

GATE-SET-ACK (acuse de establecimiento de puerta)

ID de transacción		3177	
Abonado		MTAo	Petición del total de recursos que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada
Total de actividad		4	Número total de conexiones establecidas por este cliente.

3) Cuando el MTAo recibe información de señalización de llamada calcula los parámetros de QoS para el enlace J.112. Utiliza la interfaz con el CM, descrita en el anexo E al anexo B/J.112, para enviar el siguiente mensaje DSA-REQ al CMTS, que establece los parámetros en los sentidos ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 120 (de SDP) más 18 (tara Ethernet) menos 40 (valor de supresión de cabecera) más 13 (tara J.112). El valor de supresión de cabecera son los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se incluye en el mensaje DSA-REQ.

DSA-REQ

Identificador de transacción		1
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planific. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Ref. flujo de servicio	2
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador paquete	1
	Prioridad clasificador	150
	Estado activación clasific.	Inactivo (0)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MGt
	Puerto destino IP	7000
	Protocolo IP	UDP (17)

DSA-REQ

Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador paquete	2
	Prioridad clasificador	150
	Estado activación clasific.	Inactivo (0)
	Dirección fuente IP	MGt
	Dirección destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
Supresión cabecera de cabida útil	Referencia clasificador	1
	Ref. flujo de servicio	1
	Índice supresión de cabecera	1
	Campo supresión cabecera	<42bytes>
	Máscara supresión cabecera	<42bits>
	Tamaño supresión cabecera	42
	Verificar supresión cabecera	Verificar (0)
Bloque de autorización		37125
HMAC		

4) Simultáneamente con el mensaje N.° 5 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación necesaria para informar que la reserva se ha realizado satisfactoriamente.

5) El CMTS comprueba la autorización buscando una puerta con un Gate-ID igual al valor de AuthBlock y los recursos que es necesario asignar (espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado de clasificador, etc.) e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSA-RSP con el indicador positivo.

DSA-RSP

Identificador de transacción		1
Código de confirmación		Positivo (0)
Flujo de servicio ascendente	Referencia flujo de servicio	1
	Identific. flujo de servicio	1001
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	111

DSA-RSP

Flujo de servicio descendente	Ref. flujo de servicio	2
	Identific. flujo de servicio	2001
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador paquete	1
	Identif. clasificador paquete	3001
	Prioridad clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Direcc. fuente IP	MTAo
	Puerto fuente IP	7120
	Direcc. destino IP	MGt
	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador paquete	2
	Identif. clasificador paquete	3002
	Prioridad clasificador	150
	Estado activac. clasificador	Activo (1)
	Direcc. fuente IP	MGt
	Direcc. destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
HMAC		

6) Al recibir el mensaje DSA-RSP el CM envía un acuse de recibo DSA-ACK.

DSA-ACK

ID de transacción		1
Código de confirmación		Positivo (0)
HMAC		

7) El CMS envía al CMTS el mensaje de apertura de puerta, para señalar que deberían comprometerse los recursos. El CMTS debería revocar la autorización de puerta en caso de no recibir rápidamente un mensaje DSC-REQ de MTAo.

GATE-OPEN

ID de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
Gate ID		37125	Identificador de puerta en el CMTS
HMAC			Suma de control de seguridad para este mensaje

8) El CMTS responde a GATE-OPEN con el siguiente mensaje:

GATE-OPEN-ACK

ID de transacción		72	Identificador para concordancia de este mensaje y la respuesta
HMAC			Suma de control de seguridad para este mensaje

9) Respondiendo a los mensajes de señalización que indican que se ha completado el establecimiento de llamada (el otro extremo ha descolgado), el MTAo utiliza la interfaz especificada en el anexo E al documento anexo B/J.112 para activar los recursos admitidos. Envía una instrucción DSC-REQ al CMTS.

DSC-REQ

Identificador de transacción		2
Flujo de servicio ascendente	Identificador flujo de servicio	1001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Identificador flujo de servicio	2001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Identificador flujo de servicio	1001
	Identif. clasificador paquete	3001
	Acción modific. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasificador	Activo (1)
	Direcc. fuente IP	MTAo
	Puerto fuente IP	7120
	Direcc. destino IP	MGt
	Puerto destino IP	7000
	Protocolo IP	UDP (17)

DSC-REQ

Clasificación de paquete descendente	Identificador flujo de servicio	2001
	Identif. clasificador paquete	3002
	Acción modific. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasificador	Activo (1)
	Direcc. fuente IP	MGt
	Puerto fuente IP	7000
	Direcc. destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
HMAC		

10) El CMTS envía un mensaje DSC-RSP para confirmar la realización de la operación.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

11) El CM envía el mensaje DSC-ACK para indicar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

12) Al finalizar la llamada el MTA utiliza la interfaz especificada en el anexo E al anexo B/J.112 para suprimir los flujos de servicio, enviando un DSD-REQ al CMTS.

DSD-REQ

ID de transacción		3
ID del flujo de servicio		1001
HMAC		

DSD-REQ

ID de transacción		4
ID del flujo de servicio		2001
HMAC		

13) Al recibir el mensaje DSD-REQ el CMTS envía el mensaje de coordinación de puertas al CMS (identificado en el mensaje Gate-Set).

GATE-CLOSE

ID de transacción		73	Identificador para concordancia de este mensaje y la respuesta
Gate-ID		8095	Identificador de puerta en el CMS.
HMAC			Suma de control de seguridad para este mensaje

Respuesta del CMTS distante:

GATE-CLOSE-ACK

ID de transacción		73	Identificador para concordancia de este mensaje y la respuesta.
HMAC			Suma de control de seguridad para este mensaje.

14) El CMTS suprime los identificadores del flujo de servicio y envía la respuesta al CM.

DSD-RSP

ID de transacción		3
ID del flujo de servicio		1001
Código de confirmación		Positivo (0)
HMAC		

DSD-RSP

ID de transacción		4
ID del flujo de servicio		2001
Código de confirmación		Positivo (0)
HMAC		

Apéndice VIII

Ejemplo de intercambios de mensajes del protocolo para una llamada NCS básica con un MTA integrado

Véase la figura VIII.1.

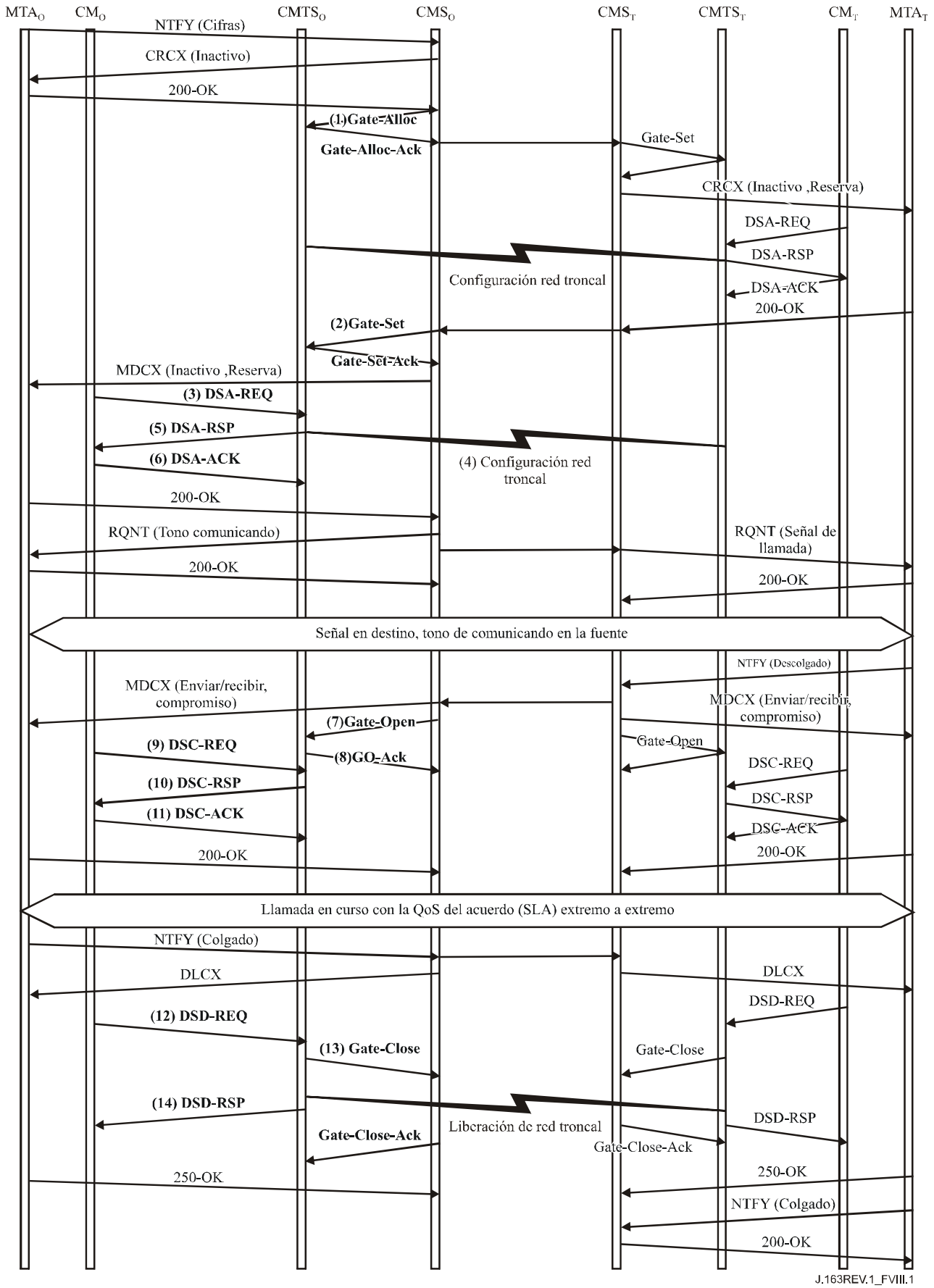


Figura VIII.1/J.163 – Llamada NCS entre elementos de red con MTA integrado

1) Al recibir la información de señalización del MTAo el CMSo verifica el consumo actual de recursos del MTAo consultando al CMTSo.

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos utilizados por este cliente.
Total actividad		12	Número máximo de puertas permitidas por cliente.

El CMTSo verifica la utilización actual de recursos por parte del MTAo y responde indicando el número de conexiones activas.

GATE-ALLOC-ACK (acuse de asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición del total de recursos utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Total de actividad		3	Número total de conexiones establecidas por este cliente.
Puerto para coordinación de puertas		7890	Puerto UDP en el que el CMTSo espera los mensajes de coordinación para esta puerta.

2) Tras un intercambio de señalización adicional, el CMSo autoriza la admisión de la nueva conexión en el CMTSo.

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición del total de recursos utilizados por este cliente.
Gate-ID		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección CMTS	CMSo	Información necesaria para realizar la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas.
	Puerto CMTS	2052	
	ID puerta distante	8095	
	Clave de seguridad	<key> (16 octetos)	
	Bandera	No enviar apertura de puerta	
	Algoritmo de autenticación	100 (MD5MAC)	

GATE-SET (establecimiento de puerta)

Información de generación de eventos	RKS-Addr-1	RKS-1	Dirección del servidor de mantenimiento de registros (RKS) primario.
	RKS-Port-1	3288	Puerto del servidor de mantenimiento de registros primario.
	Banderas	0	No formar lotes.
	RKS-Addr-2	RKS-2	Dirección del servidor de mantenimiento de registros (RKS) secundario.
	RKS-Port-2	3288	Puerto del servidor de mantenimiento de registros secundario.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.
Especificación de puerta	Sentido	1 (asc)	
	Protocolo	17 (UDP)	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Banderas	0	
	Clase de sesión	1 (prioridad normal)	
	Dirección de fuente	MTAo	
	Dirección de destino	MTAt	
	Puerto de fuente	0	
	Puerto de destino	7000	
	DS	5	Valor de punto de código DiffServ para paquetes en sentido ascendente.
	T1	300	Tiempo máximo entre la reserva y el compromiso.
	T2	2	Tiempo máximo para realizar la coordinación de puertas.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12000	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	800	

GATE-SET (establecimiento de puerta)

Especificación de puerta (Gate-Spec)	Sentido	0 (desc)	
	Bandera	0	
	Protocolo	17 (UDP)	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Clase de sesión		
	Dirección de fuente	MTAt	
	Dirección de destino	MTAo	
	Puerto de fuente	0	
	Puerto de destino	7120	
	DS	5	Valor tipo de paquete en sentido descendente.
	T1	300	Tiempo máximo entre la reserva y el compromiso.
	T2	2	Tiempo máximo para realizar la coordinación de puertas.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12000	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

El CMTSo responde a la instrucción establecimiento de puerta con un acuse de recibo.

GATE-SET-ACK (acuse de establecimiento de puerta)

ID de transacción		3177	
Abonado		MTAo	
ID de puerta		37125	Identificador de puerta asignada.
Total actividad		4	Número total de conexiones establecidas por este cliente.
Puerto para la coordinación de puertas		7890	Puerto UDP en el que el CMTSo espera los mensajes de coordinación para esta puerta. Es necesario para la segunda puerta (creada mediante Gate-Set). Las dos puertas tienen el mismo identificador.

3) Al recibir información de señalización de la llamada el MTAo calcula los parámetros de QoS para el enlace J.112. Utiliza la interfaz con el CM, descrita en el anexo E al anexo B/J.112, para enviar el siguiente mensaje DSA-REQ al CMTS, que establece los parámetros en los sentidos ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 120 (de SDP) más 18 (tara Ethernet) más 14 (tara DOCSIS).

DSA-REQ

Identificador de transacción		1
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Tipo parámetros QoS	Admitido (2)
	Planificac. flujo de servicio	UGS (6)
	Política de petición/transmis.	0x0000017F
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	800 µs
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	152
Flujo de servicio descendente	Ref. flujo de servicio	2
	Tipo parámetros QoS	Admitido (2)
	Velocidad mínima reservada	110400
	Tamaño mín. previsto de paquete a la velocidad reservada	138
Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador paquete	1
	Prioridad del clasificador	128
	Estado activac. clasificador	Inactivo (0)
	Direcc. fuente IP	MTAo
	Puerto fuente IP inicial	7120
	Puerto fuente IP final	7120
	Direcc. destino IP	MTAt
	Puerto destino IP inicial	7000
	Puerto destino IP final	7000
	Protocolo IP	UDP (17)

DSA-REQ

Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador paquete	2
	Prioridad del clasificador	128
	Estado activac. clasificador	Inactivo (0)
	Direcc. fuente IP	MTAt
	Direcc. destino IP	MTAo
	Puerto destino IP inicial	7120
	Puerto destino IP final	7120
	Protocolo IP	UDP (17)
Bloque de autorización		37125
HMAC		

4) Simultáneamente con el mensaje N.° 5 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación necesaria para indicar que la reserva se ha realizado satisfactoriamente.

5) El CMTS comprueba la autorización buscando una puerta con un Gate-ID igual al valor de AuthBlock y los recursos que es necesario asignar (espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado de clasificador, etc.) e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSA-RSP con el indicador positivo.

DSA-RSP

Identificador de transacción		1
Código de confirmación		Positivo (0)
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Identif. flujo de servicio	1001
	Identif. servicio	801
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificación flujo de servicio	UGS (6)
	Política petición/transmis.	0x0000017F
	Intervalo autorización nominal	10 ms
	Fluctuación autoriz. tolerada	800 µs
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	152
Flujo de servicio descendente	Ref. flujo de servicio	2
	Identif. flujo de servicio	2001
	Tipo parámetros QoS	Admitido (2)
	Veloc. mínima reservada	110400
	Tamaño mín. previsto de paquete a la velocidad reservada	138

DSA-RSP

Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Identif. flujo de servicio	1001
	Ref. clasificador de paquete	1
	Identif. clasificador paquete	3001
	Prioridad clasificador	128
	Estado activac. clasificador	Inactivo (0)
	Direcc. fuente IP	MTAo
	Puerto fuente IP inicial	7120
	Puerto fuente IP final	7120
	Direcc. destino IP	MTAt
	Puerto destino IP inicial	7000
	Puerto destino IP final	7000
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Ref. flujo de servicio	2
	Identif. flujo de servicio	2001
	Ref. clasificador paquete	2
	Identif. clasificador paquete	3002
	Prioridad clasificador	128
	Estado activac. clasificador	Inactivo (0)
	Direcc. fuente IP	MTAt
	Direcc. destino IP	MTAo
	Puerto destino IP inicial	7120
	Puerto destino IP final	7120
	Protocolo IP	UDP (17)
Bloque de autorización	Identificador de puerta	37125
	Identificador de recurso	71209
HMAC		

6) Al recibir el mensaje DSA-RSP el CM acusa recibo con un mensaje DSA-ACK.

DSA-ACK

Identificador de transacción		1
ConfirmationCode		Positivo (0)
HMAC		

7) El CMS envía un mensaje de apertura de puerta al CMTS para señalar que se deberían comprometer los recursos. El CMTS debería revocar la autorización de puerta en caso de no recibir rápidamente un mensaje DSC-REQ de MTAo.

GATE-OPEN

Identificador de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
Identif. puerta		37125	Gate-ID en el CMTS.

8) El CMTS responde al mensaje GATE-OPEN:

GATE-OPEN-ACK

Identificador de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
Identif. puerta		37125	GATE-ID en el CMTS.

9) En respuesta a los mensajes de señalización que indican que se ha completado el establecimiento de la comunicación (el otro lado ha descolgado), el MTAo utiliza la interfaz para activar los recursos admitidos, enviando una instrucción DSC-REQ al CMTS.

DSC-REQ

Identificador de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros QoS	Admitido + Activo (6)
	Planificac. flujo de servicio	UGS (6)
	Política petición/transmis.	0x0000017F
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	800 µs
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	152
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros QoS	Admitido + Activo (6)
	Veloc. mínima reservada	110400
	Tamaño mín. de paquete previsto a la veloc. reservada	138
Clasificación de paquete ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad clasificador	128
	Estado activac. clasificador	Activo (1)
	Direcc. fuente IP	MTAo
	Puerto fuente IP inicial	7120
	Puerto fuente IP final	7120
	Direcc. destino IP	MTAt
	Puerto destino IP inicial	7000
	Puerto destino IP final	7000
	Protocolo IP	UDP (17)

DSC-REQ

Clasificación de paquete descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad clasificador	128
	Estado activac. clasificador	Activo (1)
	Direcc. fuente IP	MTAt
	Direcc. destino IP	MTAo
	Puerto destino IP inicial	7120
	Puerto destino IP final	7120
	Protocolo IP	UDP (17)
Bloque de autorización	Identificador de puerta	37125
HMAC		

10) El CMTS envía un mensaje DSC-RSP para indicar que la operación se realizó satisfactoriamente.

DSC-RSP

Identificador de transacción		2
Código de confirmación		Positivo (0)
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Identificador servicio	801
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Admitido	200s
	Plazo estado Activo	10s
	Planificac. flujo de servicio	UGS (6)
	Política petición/transmis.	0x0000017F
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	800 μs
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	152
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros QoS	Admitido + Activo (6)
	Veloc. mínima reservada	110400
	Tamaño mín. de paquete a la veloc. reservada	138
Clasificación de paquete ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad clasificador	128
	Estado activac. clasificador	Activo (1)
	Direcc. fuente IP	MTAo
	Puerto fuente IP inicial	7120
	Puerto fuente IP final	7120
	Direcc. destino IP	MTAt

DSC-RSP

Clasificación de paquete ascendente	Puerto destino IP inicial	7000
	Puerto destino IP final	7000
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad clasificador	128
	Estado activac. clasificador	Activo (1)
	Direcc. fuente IP	MTAt
	Direcc. destino IP	MTAo
	Puerto destino IP inicial	7120
	Puerto destino IP final	7120
	Protocolo IP	UDP (17)
HMAC		

11) El CM envía un mensaje DSC-ACK para confirmar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-ACK

Identificador de transacción		2
Código de confirmación		Positivo (0)
HMAC		

12) Al finalizar la llamada el MTA utiliza la interfaz especificada en el anexo E al anexo B/J.112 para suprimir los flujos de servicio, enviando un mensaje DSD-REQ al CMTS.

DSD-REQ

Identificador de transacción		3
ServiceFlowID		1001
ServiceFlowID		2001
HMAC		

13) Al recibir el mensaje DSD-REQ el CMTS envía el mensaje de coordinación de puertas al CMS (identificado en Gate-Set).

GATE-CLOSE

ID de transacción		73	Identificador para concordancia de este mensaje y la respuesta.
Gate-ID		8095	Identificador de puerta en el CMS.

Respuesta del CMS:

GATE-CLOSE-ACK

ID de transacción		73	Identificador para concordancia de este mensaje y la respuesta.
GateID		8095	Identificador de puerta en el CMS

14) El CMTS suprime los identificadores de flujos de servicio y envía la respuesta al CM.

DSD-RSP

Identificador de transacción		3
Código de confirmación		Positivo (0)
HMAC		

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 J.112, 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 el mecanismo RSVP o la interfaz del anexo E al anexo B/J.112 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 J.112, 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 no coopera para la facturación

Puede imaginarse fácilmente qué ocurriría si en el establecimiento de la sesión existiera un mensaje así del MTA: "La parte llamada ha respondido, facturar a partir de ahora", o un mensaje así en el momento de colgar: "Fin de la sesión, suspender ahora la facturación". No obstante, existen formas más sutiles que un usuario puede utilizar y que tendrían el mismo efecto que la manipulación de dichos mensajes en caso de que existieran.

Para prestar un servicio de comunicaciones vocales con una calidad comercial utilizando IPCablecom es esencial asegurar que hay capacidad de red antes de iniciar la señalización con el CPE del receptor. Esta función se realiza mediante mensajes RESERVE (reserva). Si el mensaje RESERVE provocara la asignación efectiva de la anchura de banda (es decir, una combinación de los mecanismos RESERVE y COMMIT), el MTA no tendría motivo alguno para enviar un mensaje COMMIT. El MTA comenzaría a transmitir inmediatamente paquetes vocales y el destino comenzaría a transmitir paquetes vocales tan pronto como respondiese el teléfono. Puede decirse que el mensaje COMMIT es el mensaje de inicio de facturación antes mencionado. Por lo tanto, es esencial que RESERVE no produzca una asignación efectiva de anchura de banda, sino la verificación de todas las asignaciones actuales y las reservas pendientes para garantizar que la anchura de banda estará disponible cuando se produzca el mensaje COMMIT.

IX.4 Escenario N.º 4: 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.5 Escenario N.º 5: 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 envía un mensaje COMMIT y que el otro no lo hace. Por ejemplo, supóngase que el cliente terminación envía un mensaje COMMIT, pero no el mensaje de señalización adecuado, de forma que el origen no envía ningún mensaje COMMIT. En este caso sólo se abre una puerta y tanto los usuarios como la red quedan con media conexión. Como el iniciador no envió un mensaje COMMIT, 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.6 Escenario N.º 6: 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.7 Escenario N.º 7: 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.8 Escenario N.º 8: 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.

La coordinación entre puertas, utilizada anteriormente para la protección contra las medias conexiones, protege también contra este tipo de fraude. El mensaje GATE-OPEN informa de la anchura de banda asignada como resultado del mensaje COMMIT, y el mensaje COMMIT-ACK enviado al iniciador indica exactamente la anchura de banda que será facturada por la sesión. Si el iniciador detecta alguna circunstancia anómala, puede dar por terminada la sesión inmediatamente.

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. Puede encontrarse una definición de COPS en el documento Internet Draft-RAP-COPS-07.

El servicio común de política abierta (COPS, *common open policy service*) es un protocolo cliente/servidor definido en el grupo de trabajo del IETF sobre política de admisión del RSVP (RAP) 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.

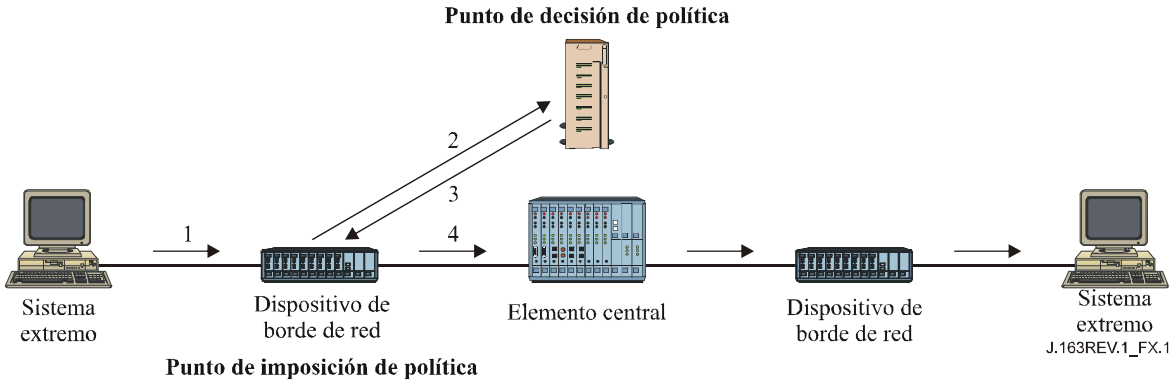


Figura X.1/J.163 – Protocolo COPS

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.

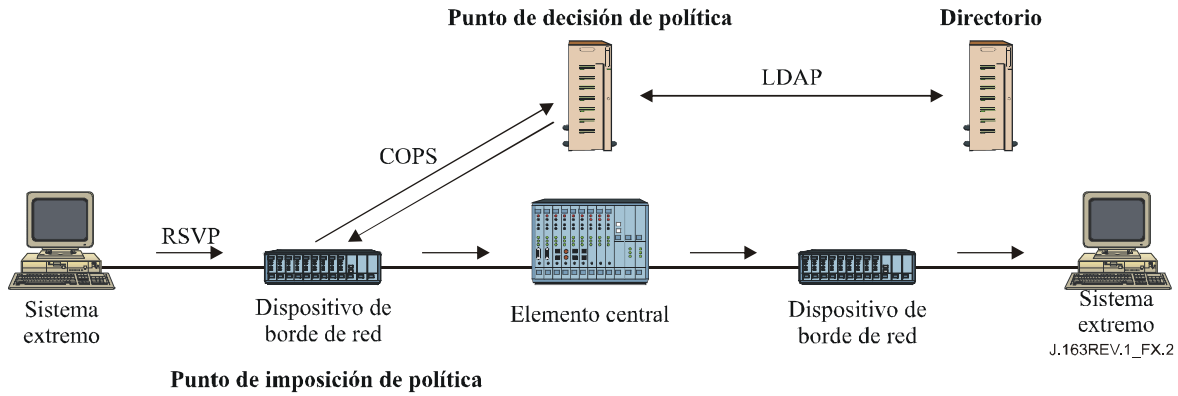


Figura X.2/J.163 – Modelo con COPS y LDAP

Apéndice XI

Protocolo de reserva de recursos (RSVP)

XI.1 Procedimientos y principios del RSVP

Este apéndice es una breve descripción de los procedimientos y principios del protocolo de reserva de recursos (RSVP). El protocolo RSVP se encuentra actualmente definido en IETF RFC 2205. Véase la figura XI.1.

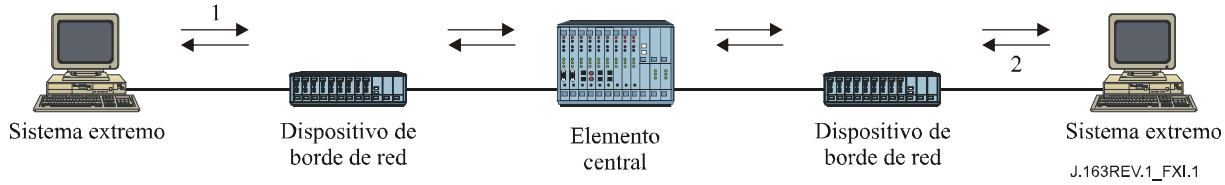


Figura XI.1/J.163 – RSVP

El IETF creó el protocolo de reserva de recursos RSVP para soportar flujos de información a través de Internet. Estas son algunas de las principales características del RSVP:

- se reservan recursos tramo a tramo para soportar flujos de información extremo a extremo;
- cada encaminador que participa en la conexión mantienen información de estado;
- los encaminadores que no participan tratan los mensajes RSVP como paquetes normales;
- estado de reserva temporal que debe renovarse periódicamente o caduca automáticamente;
- mecanismo de peticiones: un mensaje PATH inicial establece un estado en el encaminador. El receptor envía un mensaje RESV para reservar efectivamente los recursos.

En RSVP, la fuente inicia una sesión enviando un mensaje PATH (1). Éste se encamina a través de la red en función de su dirección de destino (puede ser multidifusión) y crea un estado de flujo en cada encaminador RSVP por el que pasa. El mensaje PATH se encamina utilizando los mismos procedimientos que los restantes paquetes IP con esa dirección de destino, duplicando la ruta que siguen los paquetes de datos. Conforme progresa el mensaje se registra la dirección del último encaminador RSVP pasado, que se añade a la información de estado que se incorpora en el siguiente encaminador.

En el extremo de recepción, el receptor se incorpora a la sesión enviando un mensaje RESV (2) que identifica uno o varios flujos que el receptor desea recibir de entre los flujos soportados en esta sesión. El mensaje RESV repite en sentido contrario la secuencia que ha seguido el mensaje PATH, utilizando los registros del último encaminador RSVP y haciendo que queden reservados los recursos en cada tramo. Si en el mismo encaminador se reciben múltiples mensajes RESV, éstos pueden fusionarse en un único mensaje RESV con una petición combinada de reserva de recursos.

El proceso requiere que se establezca un estado en numerosos nodos internos, así como una reserva de recursos en dichos nodos. Se establece un trayecto fijo para el flujo de información, con la garantía de que hay recursos asignados en todos los puntos del trayecto que soportan el protocolo RSVP.

XI.2 Especificación de flujo RSVP

Una petición elemental de reserva RSVP consta de una "especificación de flujo" (flowspec) y de una "especificación de filtro" (filter-Spec) que constituyen el "descriptor de flujo". La especificación de flujo determina la QoS deseada. La especificación de filtro, junto con la especificación de sesión, define el conjunto de paquetes de datos – el "flujo" – que se han de tratar con la QoS definida por la especificación de flujo. La especificación de flujo se utiliza para fijar parámetros del planificador de paquetes del nodo o cualquier otro mecanismo de la capa de enlace, mientras que la especificación de filtro se utiliza para fijar los parámetros del clasificador de paquetes. Los paquetes de datos que están destinados a una sesión en particular, pero que no concuerdan con ninguna de las especificaciones de filtro de dicha sesión, se tratan como tráfico que se encamina en condiciones de mejor esfuerzo.

La especificación de flujo de una petición de reserva incluye, en general, una clase de servicio y dos conjuntos de parámetros numéricos:

1) una "especificación de reserva" (Rspec) que define la QoS deseada, y

2) una "especificación de tráfico" (Tspec) que describe el flujo de datos.

Es importante señalar que los formatos y contenidos de Tspec y Rspec vienen determinados por los modelos de servicios integrados (IntServ) descritos en IETF RFC 2210 que se han definido en el grupo de trabajo de servicios integrados (intserv) del IETF y son, en general, opacos al propio RSVP. El RSVP define el mecanismo de señalización y no el modelo de tráfico.

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).

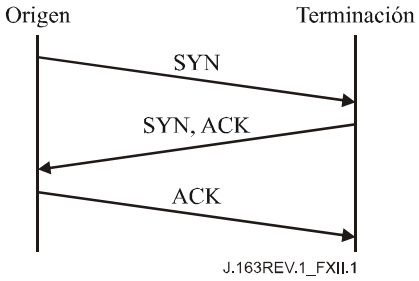


Figura XII.1/J.163 – Establecimiento de una conexión TCP

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 postmarcación. 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 postmarcación es un motivo suficiente para no crear una conexión durante el periodo de retardo postmarcación. 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 2^9 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.

---

[9] 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.

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).

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.

Apéndice XIII

Modificación de parámetro incompatible para una llamada NCS básica con un MTA integrado

Véase la figura XIII.1.

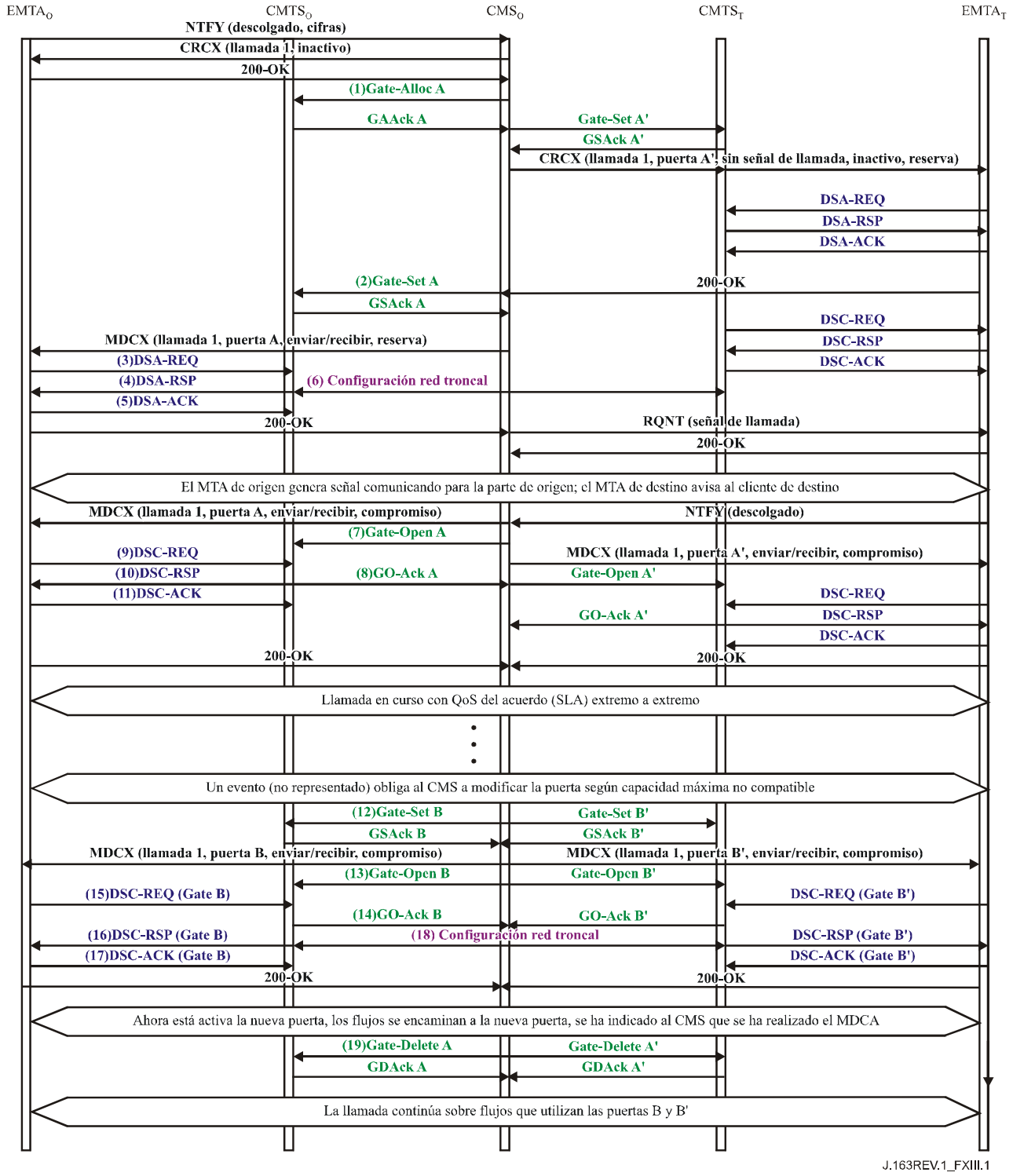


Figura XIII.1/J.163 – Llamada NCS entre elementos de red con MTA integrado

1) Al recibir la información de señalización del EMTAo el CMSo verifica el consumo actual de recursos del EMTAo consultando al CMTSo.

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Total actividad		32	Número máximo de conexiones permitidas por cliente, previsiblemente superior al número que será realmente necesario.

El CMTSo verifica la utilización actual de recursos por parte del EMTAo y responde indicando el número de conexiones activas.

GATE-ALLOC-ACK (acuse de asignación de puerta)

ID de transacción		3176	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
ID de puerta		37125	Identificador de la puerta asignada A.
Total actividad		1	Número total de conexiones establecidas por este cliente.

2) Tras un intercambio de señalización adicional, el CMSo autoriza la admisión de la nueva conexión en el CMTSo.

GATE-SET (establecimiento de puerta)

ID de transacción		3193	ID de transacción único para este intercambio de mensajes.
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Gate-ID		37125	Identificador de la puerta asignada A.
Información de puerta distante	Dirección CMTS	CMSo	Información necesaria para realizar la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas.
	Puerto CMTS	2052	
	ID de puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	No enviar apertura de puerta	
Información de generación de eventos	RKS-Addr	RKS	Dirección del servidor de mantenimiento de registros (RKS).
	RKS-Port	3288	Puerto del servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Sentido	Asc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAo	
	Dirección de destino	EMTAt	
	Puerto de fuente	7820	
	Puerto de destino	8422	
	DSCP	6	Valor de tipo de paquete en sentido ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
Especificación de puerta	Sentido	Desc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAt	
	Dirección de destino	EMTAo	
	Puerto de fuente	8420	
	Puerto de destino	7822	
	DSCP	9	Valor tipo de paquete en sentido descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

El CMTSo responde a la instrucción establecimiento de puerta con un acuse de recibo.

GATE-SET-ACK (acuse de establecimiento de puerta)

ID de transacción		3193	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
ID de puerta		37125	Identificador de la puerta asignada A.
Total actividad		1	Número total de conexiones establecidas por este cliente.

3) Al recibir información de señalización de la llamada el EMTAo calcula los parámetros de QoS para el enlace J.112. Envía el siguiente mensaje DSA-REQ al CMTS, que establece los parámetros en los sentidos ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 80 bytes de cabida útil de voz, más 12 bytes de cabecera RTP, más 2 bytes de etiqueta PHS, más 2 bytes de suma de control de cabecera, más 5 bytes de información J.112 BPI+, más 4 bytes de cabecera MAC J.112, más 4 bytes de CRC. La supresión de cabecera significa los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se puede leer en DSA-REQ.

DSA-REQ

Identificador de transacción		1
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	109
Flujo de servicio descendente	Ref. flujo de servicio	2
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador de paquete	1
	Prioridad de clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820
	Dirección destino IP	EMTAt
	Puerto destino IP	8422
	Protocolo IP	UDP (17)

DSA-REQ

Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador de paquete	2
	Prioridad de clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección fuente IP	EMTAt
	Puerto fuente IP	8420
	Dirección destino IP	EMTAo
	Puerto destino IP	7822
	Protocolo IP	UDP (17)
Supresión de cabecera de cabida útil	Referencia del clasificador	1
	Ref. flujo de servicio	1
	Índice supresión de cabecera	1
	Campo supresión cabecera	<42bytes>
	Máscara supresión cabecera	<42bits>
	Tamaño supresión cabecera	42
	Verificar supresión cabecera	Verificar (0)
Bloque de autorización		37125
HMAC		

4) El CMTS comprueba la autorización buscando una puerta con un gate-ID igual al valor de AuthBlock y los recursos que es necesario asignar (espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado de clasificador, etc.) e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSA-RSP con el indicador positivo.

DSA-RSP

Identificador de transacción		1
Código de confirmación		Positivo (0)
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Identificador flujo de servicio	1001
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificación flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	109
Flujo de servicio descendente	Ref. flujo de servicio	2
	Identificador flujo de servicio	2001
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000

DSA-RSP

Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador de paquete	1
	Identif. clasificador de paquete	3001
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820
	Dirección destino IP	EMTAt
	Puerto destino IP	8422
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador de paquete	2
	Identif. clasificador de paquete	3002
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	EMTAt
	Dirección destino IP	EMTAo
	Puerto fuente IP	8420
	Puerto destino IP	7822
	Protocolo IP	UDP (17)
HMAC		

5) Al recibir el mensaje DSA-RSP el CM acusa recibo con un mensaje DSA-ACK.

DSA-ACK

Identificador de transacción		1
Código de confirmación		Positivo (0)
HMAC		

6) Simultáneamente con el mensaje N.° 4 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación necesaria para indicar que la reserva se ha realizado satisfactoriamente.

7) El CMS envía un mensaje de apertura de puerta al CMTS para señalar que se deberían comprometer los recursos. El CMTS debería revocar la autorización de puerta en caso de no recibir rápidamente un mensaje DSC-REQ del EMTAo.

GATE-OPEN

Identificador de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
Gate ID		37125	Identificador de puerta en el CMTS.
HMAC			Suma de control de seguridad para este mensaje.

8) El CMTS responde al mensaje GATE-OPEN:

GATE-OPEN-ACK

Identificador de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
HMAC			Suma de control de seguridad para este mensaje.

9) En respuesta a los mensajes de señalización que indican que se ha completado el establecimiento de la comunicación (el otro lado ha descolgado), el EMTAo utiliza la interfaz descrita en el anexo E al anexo B/J.112 para activar los recursos admitidos, enviando DSC-REQ al CMTS.

DSC-REQ

Identificador de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	109
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820
	Dirección destino IP	EMTAt
	Puerto destino IP	8422
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAt
	Dirección destino IP	EMTAo
	Puerto fuente IP	8420

DSC-REQ

Clasificación de paquete descendente	Puerto destino IP	7822
	Protocolo IP	UDP (17)
Bloque de autorización		37125
HMAC		

10) El CMTS envía un mensaje DSC-RSP para indicar que la operación se realizó satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

11) El CM envía un mensaje DSC-ACK para indicar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

12) Por algún motivo no representado aquí (en este ejemplo es la modificación del número del puerto y el códec: 729E con paquetes de 30 ms), el CMSo modifica los parámetros de recursos de la llamada, siendo incompatible con los parámetros de recursos de la puerta A (37125). Previo intercambio de otros mensajes de señalización, el CMSo autoriza al CMTSo para admitir la nueva conexión.

GATE-SET

ID de transacción		95	Identificador que es exclusivo de este intercambio de mensajes.
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Total actividad		32	
Información de puerta distante	Dirección CMTS	CMSo	Información necesaria para realizar la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas.
	Puerto CMTS	2052	
	Gate-ID distante	8095	
	Clave de seguridad	<key>	
	Bandera	No enviar apertura de puerta	
Información de generación de eventos	Dirección RKS	RKS	Dirección del servidor de mantenimiento de registros.
	Puerto RKS	3288	Puerto del servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.

GATE-SET

Especificación de puerta	Sentido	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAo	
	Dirección de destino	EMTAt	
	Puerto de fuente	7820	
	Puerto de destino	8632	
	DSCP	6	Valor de tipo de paquete en sentido ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	2833	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	b	85	
	p	2833	
	m	85	
	M	85	
	R	2833	
	S	0	
Especificación de puerta	Sentido	Desc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAt	
	Dirección de destino	EMTAo	
	Puerto de fuente	8630	
	Puerto de destino	7822	
	DSCP	9	Tipo de paquete descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	2833	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	b	85	
	p	2833	
	m	85	
	M	85	
	R	2833	
	S	0	

CMTSo envía un acuse de recibo del mensaje de establecimiento de puerta (Gate Setup).

GATE-SET-ACK

ID de transacción		95	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Gate-ID		38205	Identificador de la nueva puerta B asignada.
Total actividad		32	

13) El CMS envía el mensaje de apertura de puerta al CMTS para señalar que se deberían comprometer los recursos. El CMTS debería revocar la autorización de puerta en caso de no recibir rápidamente un mensaje DSC-REQ del EMTAo.

GATE-OPEN

Identificador de transacción		143	Identificador para concordancia de este mensaje y la respuesta.
Gate ID		38205	Identificador de puerta B en el CMTS.
HMAC			Suma de control de seguridad para este mensaje

14) El CMTS responde al mensaje GATE-OPEN:

GATE-OPEN-ACK

Identificador de transacción		143	Identificador para concordancia de este mensaje y la respuesta.
HMAC			Suma de control de seguridad para este mensaje

15) Habiendo recibido los mensajes de señalización, el EMTAo calcula los parámetros de QoS para el enlace J.112 y envía el siguiente mensaje DSC-REQ al CMTS, que se utiliza para establecer los parámetros en los sentidos ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 30 bytes de cabida útil de voz, más 12 bytes de cabecera RTP, más 2 bytes de etiqueta PHS, más 2 bytes de suma de control de cabecera, más 5 bytes de información J.112 BPI+, más 4 bytes de cabecera MAC J.112, más 4 bytes de CRC. La supresión de cabecera significa los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se puede leer en DSC-REQ.

DSC-REQ

Identificador de transacción		2004
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	30 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	59

DSC-REQ

Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	2833
Clasificación de paquete ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820
	Dirección destino IP	EMTAt
	Puerto destino IP	8632
Clasificación de paquete descendente	Protocolo IP	UDP (17)
	Identif. flujo de servicio	2001
	Identif. clasificador paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAt
	Dirección destino IP	EMTAo
	Puerto fuente IP	8630
	Puerto destino IP	7822
	Protocolo IP	UDP (17)
Bloque de autorización		38205
HMAC		

16) Al recibir el mensaje DSC-REQ del EMTA, el CMTS envía un mensaje DSC-RSP al EMTA.

DSC-RSP

ID de transacción		2004
Código de confirmación		Positivo (0)
HMAC		

17) Al recibir el mensaje DSC-RSP del CMTS, el EMTA envía un mensaje DSC-ACK al CMTS.

DSC-RSP

ID de transacción		2004
Código de confirmación		Positivo (0)
HMAC		

18) Simultáneamente con el mensaje N.° 6 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación necesaria para indicar que la reserva se ha realizado satisfactoriamente.

19) Al recibir el 200 OK del MTA, que indica que se ha transferido satisfactoriamente la llamada a la nueva puerta B, el CMSo emite un mensaje de supresión (Gate Delete) de la puerta A que ya no se utiliza.

GATE-DELETE

ID de transacción	143	Identificador para concordancia de este mensaje y la respuesta.
Gate ID	37125	Identificador de la puerta en el CMTS.

CMTSo envía un acuse de recibo de la instrucción de supresión de puerta:

GATE-DELETE-ACK

ID de transacción		95	
Gate ID		37125	Identificador de la puerta A.

Apéndice XIV

Modificación de parámetro incompatible para una llamada NCS básica con un MTA integrado

El siguiente ejemplo (figura XIV.1) ilustra el tratamiento de una llamada en espera con señalización NCS y mensajes DQoS RSVP iniciados por el CM. En este flujo de llamada se supone que ya hay una llamada en curso entre el MTAo y el MTA_{T1} con la puerta GateID N.° 1 (37125) y el flujo de servicio N.° 1. La segunda conexión para MTA_{T2} abre una nueva puerta (38205) y un nuevo flujo de servicio, y utiliza el identificador de recurso (472) que se ha notificado de la llamada inicial para indicar al CMTS que debe compartir el ancho de banda entre estos dos flujos de servicio.

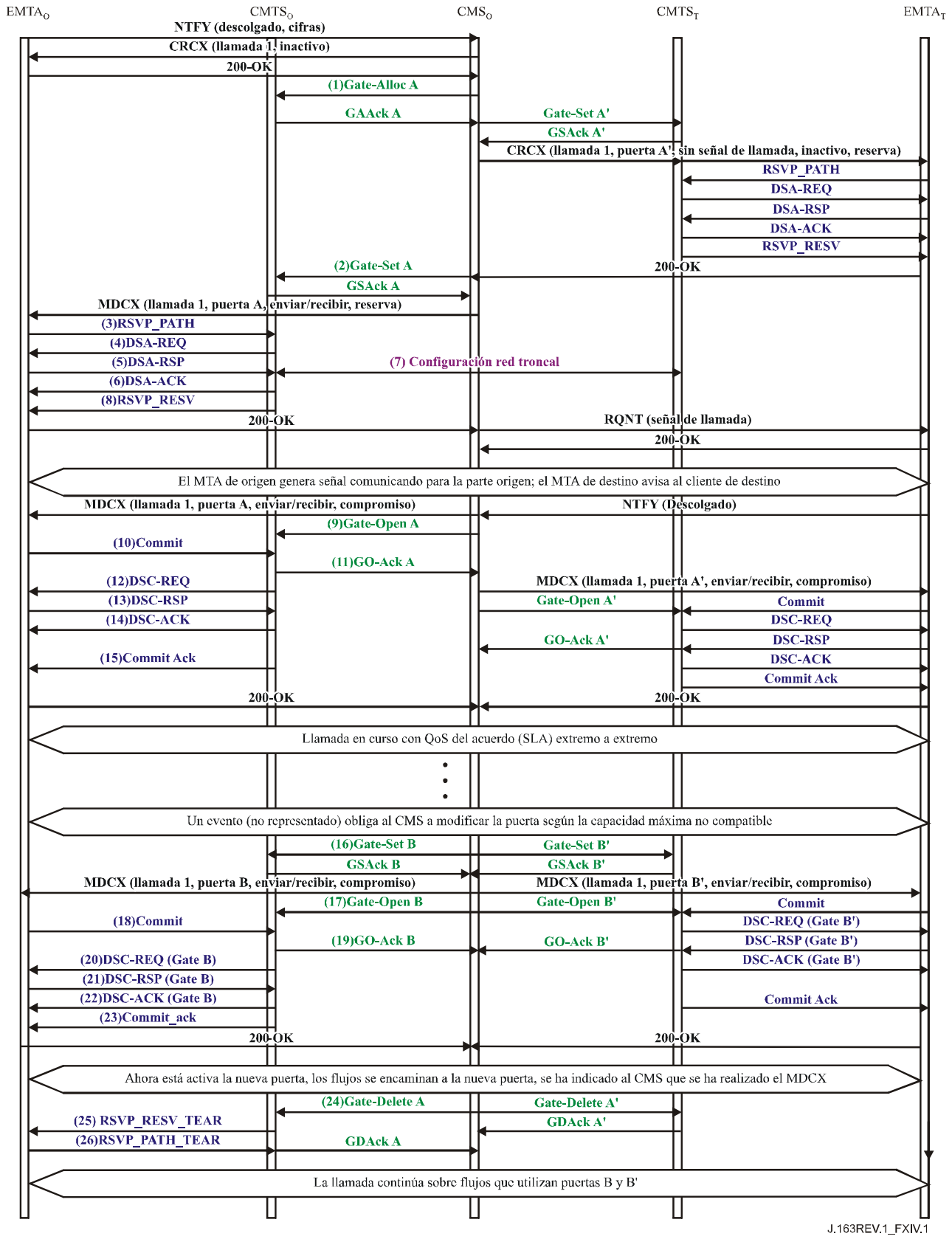


Figura XIV.1/J.163 – Llamada NCS entre elementos de red con MTA integrado

1) Al recibir la información de señalización del EMTAo el CMSo verifica el consumo actual de recursos del EMTAo consultando al CMTSo.

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Total actividad		32	Número máximo de conexiones permitidas por cliente, previsiblemente superior al número que será realmente necesario.

El CMTSo verifica la utilización actual de recursos por parte del EMTAo y responde indicando el número de conexiones activas.

GATE-ALLOC-ACK (acuse de asignación de puerta)

ID de transacción		3176	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Gate-ID		37125	Identificador de la puerta asignada A.
Total actividad		1	Número total de conexiones establecidas por este cliente.

2) Tras un intercambio de señalización adicional, el CMSo autoriza la admisión de la nueva conexión en el CMTSo.

GATE-SET (establecimiento de puerta)

ID de transacción		3193	ID de transacción único para este intercambio de mensajes.
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Gate-ID		37125	Identificador de la puerta asignada A.
Información de puerta distante	Dirección CMTS	CMSo	Información necesaria para realizar la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas.
	Puerto CMTS	2052	
	ID puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	No enviar apertura de puerta	
Información de generación de eventos	RKS-Addr	RKS	Dirección del servidor de mantenimiento de registros (RKS).
	RKS-Port	3288	Puerto del servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Sentido	Asc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAo	
	Dirección de destino	EMTAt	
	Puerto de fuente	7820	
	Puerto de destino	8422	
	DSCP	6	Valor de tipo de paquete en sentido ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	rb	12000	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	br	12000	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
Especificación de puerta	Sentido	Desc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAt	
	Dirección de destino	EMTAo	
	Puerto de fuente	8420	
	Puerto de destino	7822	
	DSCP	9	Valor tipo de paquete en sentido descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	rb	12000	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	br	12000	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

El CMTSo responde a la instrucción establecimiento de puerta con un acuse de recibo.

GATE-SET-ACK (acuse de establecimiento de puerta)

ID de transacción		3193	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
ID de puerta		37125	Identificador de la puerta asignada A.
Total de actividad		1	Número total de conexiones establecidas por este cliente.

3) Al recibir información de señalización de la llamada el EMTAo calcula los parámetros de QoS para el enlace DOCSIS 1.1 y envía un mensaje RSVP al MTA de terminación.

RSVP-PATH

Objeto Sesión	Protocolo	UDP	Parámetros que identifican la sesión RSVP, concuerdan con la autorización previamente enviada por el controlador de puerta y también se utilizan en los clasificadores de QoS.
	Dirección de destino	EMTAt	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	EMTAo	
	Puerto de fuente	8422	
Especificación de tráfico del emisor	b	120	Estos parámetros constituyen el mínimo valor superior de todos los parámetros de tráfico para los dos flujos posibles. Es un objeto RSVP normalizado que será interpretado por todos los encaminadores intermedios en el trayecto entre el MTA y el CMTS.
	r	12000	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	40	
	VAD	Desact.	
Gate-ID		37125	Identifica la puerta que autoriza esta petición.
Espec. de recursos hacia adelante	R	12000	Esta Rspec corresponde a la Tspec del emisor inmediatamente anterior.
	S	0	
Sesión hacia atrás	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al CMTS información suficiente para calcular los parámetros de tráfico descendente y generar un mensaje RSVP-PATH para el flujo descendente.
	Dirección de destino	EMTAo	
	Puerto de destino	7822	
Plantilla emisor hacia atrás	Direcc. de fuente	EMTAt	
	Puerto de fuente	8420	
Especificación de tráfico del emisor hacia atrás	b	120	Parámetros de tráfico negociados para el nuevo CÓDEC solicitado para esta llamada. El CMTS calcula los parámetros de QoS efectivos en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que no será considerado por los encaminadores intermedios.
	r	12000	
	p	12000	
	m	120	
	M	120	
	Supresión cabecera	0	
	VAD	Desact.	
Rspec hacia atrás	R	12000	
	S	0	

4) Habiendo recibido el mensaje RSVP, el CMTS comprueba la autorización buscando una puerta con el mismo identificador de Gate-ID, comprueba los recursos que tendrá que asignar (por ejemplo, espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado de clasificador) y calcula los parámetros de QoS para el enlace DOCSIS 1.1. Entonces envía el siguiente mensaje DSA-REQ al EMTAo utilizando la interfaz del anexo E al anexo B/J.112 a RFI DOCSIS con el módem de cable. Este mensaje se utiliza para establecer los parámetros en sentido ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 80 bytes de cabida útil de voz, más 12 bytes de cabecera RTP, más 2 bytes de etiqueta PHS, más 2 bytes de suma de control de cabecera, más 5 bytes de información DOCSIS BPI+, más 4 bytes de cabecera MAC DOCSIS, más 4 bytes de CRC. La supresión de cabecera significa los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se puede leer en DSA-REQ.

DSA-REQ

Identificador de transacción		1
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	109
Flujo de servicio descendente	Ref. flujo de servicio	2
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador de paquete	1
	Prioridad de clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820
	Dirección destino IP	EMTAt
	Puerto destino IP	8422
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador de paquete	2
	Prioridad de clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección fuente IP	EMTAt
	Puerto fuente IP	8420
	Dirección destino IP	EMTAo

DSA-REQ

Clasificación de paquete descendente	Puerto destino IP	7822
	Protocolo IP	UDP (17)
Supresión de cabecera de cabida útil	Referencia del clasificador	1
	Ref. flujo de servicio	1
	Índice supresión de cabecera	1
	Campo supresión cabecera	<42bytes>
	Máscara supresión cabecera	<42bits>
	Tamaño supresión cabecera	42
	Verificar supresión cabecera	Verificar (0)
Bloque de autorización		37125
HMAC		

5) El EMTAo comprueba la admisión e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSA-RSP con el indicador positivo.

DSA-RSP

Identificador de transacción		1
Código de confirmación		Positivo (0)
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Identificador flujo de servicio	1001
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	109
Flujo de servicio descendente	Ref. flujo de servicio	2
	Identificador flujo de servicio	2001
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador de paquete	1
	Identif. clasificador de paquete	3001
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820

DSA-RSP

Clasificación de paquete ascendente	Dirección destino IP	EMTAt
	Puerto destino IP	8422
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador de paquete	2
	Identif. clasificador de paquete	3002
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	EMTAt
	Dirección destino IP	EMTAo
	Puerto fuente IP	8420
	Puerto destino IP	7822
	Protocolo IP	UDP (17)
HMAC		

6) Al recibir el mensaje DSA-RSP el CMTS acusa recibo con un mensaje DSA-ACK.

DSA-ACK

Identificador de transacción		1
Código de confirmación		Positivo (0)
HMAC		

7) Simultáneamente con el mensaje N.° 5 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación necesaria para indicar que la reserva se ha realizado satisfactoriamente.

8) El CMTS devuelve un mensaje RSVP_RESV al EMTAo para confirmar que se ha reservado satisfactoriamente.

RSVP-RESV

Objeto Sesión	Protocolo	UDP	Estos campos identifican el flujo IP para el que se hace la reserva.
	Dirección destino	EMTAt	
	Puerto de destino	7820	
Filter-Spec	Dirección de fuente	EMTAo	
	Puerto de fuente	8422	
Flowspec	br	12000	Estos campos identifican los recursos que se reservan para este flujo.
	rb	12000	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	
ResourceID		472	ID de recurso para esta reserva.

9) El CMS envía un mensaje de apertura de puerta al CMTS para señalar que se deberían comprometer los recursos. El CMTS debería revocar la autorización de puerta en caso de no recibir rápidamente un mensaje DSC-REQ Commit del EMTAo.

GATE-OPEN

Identificador de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
Gate ID		37125	Identificador de puerta en el CMTS.
HMAC			Suma de control de seguridad para este mensaje.

10) En respuesta a los mensajes de señalización que indican que la otra parte ha contestado a la llamada, el EMTAo utiliza el mensaje de compromiso de la interfaz descrita en el anexo E al anexo B/J.112 para activar los recursos admitidos, enviando una instrucción DOCSIS 1.1 DSC-REQ al CMTS.

COMMIT

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino tienen que coincidir con los valores del identificador de puerta.
	Dirección de destino	EMTAt	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	EMTAo	
	Puerto de fuente	8422	
Gate-ID		37125	

11) El CMTS responde al mensaje GATE-OPEN:

GATE-OPEN-ACK

Identificador de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
HMAC			Suma de control de seguridad para este mensaje.

12) Para responder a los mensajes de señalización que indican que se ha contestado a la llamada, el CMTSo utiliza la interfaz del anexo E al anexo B/J.112 para activar los recursos admitidos. Con este fin transmite una instrucción DOCSIS 1.1 DSC-REQ al EMTAo.

DSC-REQ

Identificador de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	109

DSC-REQ

Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Identif. flujo de servicio	1001
	Identif. clasificador paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820
	Dirección destino IP	EMTAt
	Puerto destino IP	8422
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Identif. flujo de servicio	2001
	Identif. clasificador paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAt
	Dirección destino IP	EMTAo
	Puerto fuente IP	8420
	Puerto destino IP	7822
	Protocolo IP	UDP (17)
Bloque de autorización		37125
HMAC		

13) El EMTAo envía un mensaje DSC-RSP para indicar que la operación se ha realizado satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

14) El CMTS envía un mensaje DSC-ACK para indicar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

15) El CMTS acusa recibo del mensaje COMMIT:

COMMIT-ACK

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino concuerdan con los valores de Gate ID.
	Dirección destino	MTAt2	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	8422	
Gate-ID		37125	

16) Por algún motivo no representado aquí (en este ejemplo es la modificación del número del puerto y el códec: 729E con paquetes de 30 ms), el CMSo modifica los parámetros de recursos de la llamada, siendo incompatible con los parámetros de recursos de la puerta A (37125). Previo intercambio de otros mensajes de señalización, el CMSo autoriza al CMTSo para admitir la nueva conexión.

GATE-SET

ID de transacción		95	Identificador que es exclusivo de este intercambio de mensajes.
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Total actividad		32	
Información de la puerta distante	Dirección CMTS	CMSo	Información necesaria para realizar la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas.
	Puerto CMTS	2052	
	Gate-ID distante	8095	
	Clave de seguridad	<key>	
	Bandera	No enviar apertura de puerta	
Información de generación de eventos	Dirección RKS	RKS	Dirección del servidor de mantenimiento de registros.
	Puerto RKS	3288	Puerto en el servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.
Especificación de puerta	Sentido	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAo	
	Dirección destino	EMTAt	
	Puerto de fuente	7820	
	Puerto de destino	8632	
	DSCP	6	Valor de tipo de paquete ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	rb	852833	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	br	283385	
	p	2833	
	m	85	

GATE-SET

Especificación de puerta	M	85	
	R	2833	
	S	0	
	Sentido	Desc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	EMTAt	
	Dirección destino	EMTAo	
	Puerto de fuente	8630	
	Puerto de destino	7822	
	DSCP	9	Tipo de paquete descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	rb	283385	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	br	283385	
	p	2833	
	m	85	
	M	85	
	R	2833	
	S	0	

El CMTSo envía un acuse de recibo del mensaje de establecimiento de puerta (*Gate Setup*).

GATE-SET-ACK

ID de transacción		95	
Abonado		EMTAo	Petición del total de recursos utilizados por este cliente.
Gate-ID		38205	Identificador de la nueva puerta B asignada.
Total actividad		32	

17) El CMS envía el mensaje de apertura de puerta al CMTS para señalar que se deberían comprometer los recursos. El CMTS debería revocar la autorización de puerta en caso de no recibir rápidamente un mensaje DSC-REQ del EMTAo.

GATE-OPEN

ID de transacción		143	Identificador para concordancia de este mensaje y la respuesta.
Gate-ID		38205	Identificador de puerta B en el CMTS.
HMAC			Suma de control de seguridad para este mensaje.

18) Habiendo recibido los mensajes de señalización, el EMTAo calcula los parámetros de QoS para el enlace DOCSIS 1.1 y envía los mensaje RSVP para reservar el ancho de banda. Al recibir una instrucción del CMSo para modificar los recursos con un nuevo compromiso, envía el mensaje Commit para comprometer los recursos.

COMMIT

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino tienen que coincidir con los valores del identificador de puerta.
	Dirección de destino	EMTAt	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	EMTAo	
	Puerto de fuente	8632	
Gate-ID		37126	

RSVP-PATH

Objeto Sesión	Protocolo	UDP	Parámetros que identifican la sesión RSVP, concuerdan con la autorización previamente enviada por el controlador de puerta y también se utilizan en los clasificadores de QoS.
	Dirección de destino	EMTAt	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	EMTAo	
	Puerto de fuente	8632	
Especificación de tráfico del emisor	r	2833	Estos parámetros constituyen el mínimo valor superior de todos los parámetros de tráfico para los dos flujos posibles. Es un objeto RSVP normalizado que será interpretado por todos los encaminadores intermedios en el trayecto entre el MTA y el CMTS.
	b	85	
	p	2833	
	m	85	
	M	85	
	Supresión cabecera	40	
	VAD	Desact.	
Gate-ID		37126	Identifica la puerta que autoriza esta petición.
ID de recurso		472	Identificador de recurso atribuido al enlace RSVP anterior.
Espec. de recursos hacia adelante	R	12000	Esta Rspec corresponde a la Tspec del emisor inmediatamente anterior.
	S	0	
Sesión hacia atrás	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al CMTS información suficiente para calcular los parámetros de tráfico descendente y generar un mensaje RSVP-PATH para el flujo descendente.
	Direcc. de destino	EMTAo	
	Puerto de destino	7822	
Plantilla de emisor hacia atrás	Direcc. de fuente	EMTAt	
	Puerto de fuente	8420	
Especificación de tráfico del emisor hacia atrás	r	2833	Parámetros de tráfico negociados para el nuevo CÓDEC solicitado para esta llamada. El CMTS calcula los parámetros de QoS efectivos en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que no será considerado por los encaminadores intermedios.
	b	85	
	p	2833	
	m	85	
	M	85	
	Supresión cabecera	0	
	VAD	Desact.	
Rspec hacia atrás	R	2833	
	S	0	

19) El CMTS responde al mensaje GATE-OPEN:

GATE-OPEN-ACK

ID de transacción		143	Identificador para concordancia de este mensaje y la respuesta.
HMAC			Suma de control de seguridad para este mensaje.

20) Habiendo recibido la información de señalización para la llamada, el CMTSo calcula los parámetros de QoS para el enlace DOCSIS 1.1. Utiliza la interfaz del anexo E al anexo B/J.112 a RFI DOCSIS con el módem de cable para enviar el siguiente mensaje DSC-REQ al EMTAo. Este mensaje se utiliza para establecer los parámetros en sentido ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 30 bytes de cabida útil de voz, más 12 bytes de cabecera RTP, más 2 bytes de etiqueta PHS, más 2 bytes de suma de control de cabecera, más 5 bytes de información DOCSIS BPI, más 4 bytes de cabecera MAC DOCSIS, más 4 bytes de CRC. La supresión de cabecera significa los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se puede leer en DSC-REQ.

DSC-REQ

Identificador de transacción		2004
Flujo de servicio ascendente	Ref. flujo de servicio	1001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	30 ms
	Fluctuación autoriz. tolerada	2 ms
	Autoriz. por intervalo	1
	Tamaño autoriz. sin petición	59
Flujo de servicio descendente	Ref. flujo de servicio	2001
	Tipo parámetros QoS	Admitido + Activo (6)
	Plazo estado Admitido	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	2833
Clasificador en sentido ascendente	Identif. flujo de servicio	1001
	Identif. clasif. de paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad de clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAo
	Puerto fuente IP	7820
	Dirección destino IP	EMTAt
	Puerto destino IP	8632
	Protocolo IP	UDP (17)

DSC-REQ

Clasificador en sentido descendente	Identif. flujo de servicio	2001
	Identif. clasif. de paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad de clasificador	150
	Estado activac. clasificador	Activo (1)
	Dirección fuente IP	EMTAt
	Dirección destino IP	EMTAo
	Puerto fuente IP	8630
	Puerto destino IP	7822
	Protocolo IP	UDP (17)
Bloque de autorización		38205
HMAC		

21) Al recibir el mensaje DSC-REQ del CMTS, el EMTAo envía un mensaje DSC-RSP al CMTS.

DSC-RSP

ID de transacción		2004
Código de confirmación		Positivo (0)
HMAC		

22) Al recibir el mensaje DSC-RSP del EMTAo, el CMTSo acusa recibo al EMTAo con un mensaje DSC-ACK.

DSC-ACK

ID de transacción		2004
Código de confirmación		Positivo (0)
HMAC		

23) Simultáneamente con el mensaje N.° 21 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación necesaria para indicar que la reserva se ha realizado satisfactoriamente.

24) El CMTS acusa recibo de commit con.

COMMIT-ACK

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino tienen que coincidir con los valores del identificador de puerta.
	Dirección de destino	MTAt2	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	84632	
Gate-ID		37126	

25) Al recibir el 200 OK del MTA, que indica que se ha transferido satisfactoriamente la llamada a la nueva puerta B, el CMSo emite un mensaje de supresión (Gate Delete) de la puerta A que ya no se utiliza.

GATE-DELETE

ID de transacción	143	Identificador para concordancia de este mensaje y la respuesta.
Gate ID	37125	Identificador de la puerta en el CMTS.

El CMTSo envía un acuse de recibo de la instrucción de supresión de puerta.

GATE-DELETE-ACK

ID de transacción		95	Suma de control de seguridad para este mensaje.
Gate-ID		37125	

26) Al recibir el mensaje Gate_Delete el CMTS suprime el enlace RSVP que utiliza la puerta 37125.

RSVP-RESV-TEAR

Objeto Sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino identifican el flujo RSVP.
	Dirección de destino	EMTAt	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	8422	

27) Al recibir el mensaje RSVP-RESV-TEAR el EMTAo envía un mensaje RSV-PATH-TEAR al CMTSo.

RSVP-PATH-TEAR

Objeto Sesión	Protocolo	UDP	Estos parámetros identifican el flujo IP que se suprime.
	Dirección de destino	MTAt	
	Puerto de destino	7820	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	8422	

Apéndice XV

Ejemplo de intercambio de mensajes de protocolo para llamada en espera con NCS

El siguiente ejemplo (figura XV.1) ilustra el tratamiento de una llamada en espera, utilizando la señalización NCS y mensajes DSx iniciados por el CM. En el siguiente flujo se supone que hay una llamada en curso entre el MTAo y el MTA_{T1} que utiliza el identificador de puerta GateId #1 (37125) y los flujos de servicio ServiceFlows #1 (1001/2001). La segunda conexión para MTA_{T2} abre una nueva puerta (37130) y un nuevo flujo (1002/2002), y utiliza el identificador de recurso ResourceId (3333) que se ha comunicado de la llamada inicial para indicar al CMTS que debe compartir el ancho de banda subyacente entre estos dos flujos de servicio.

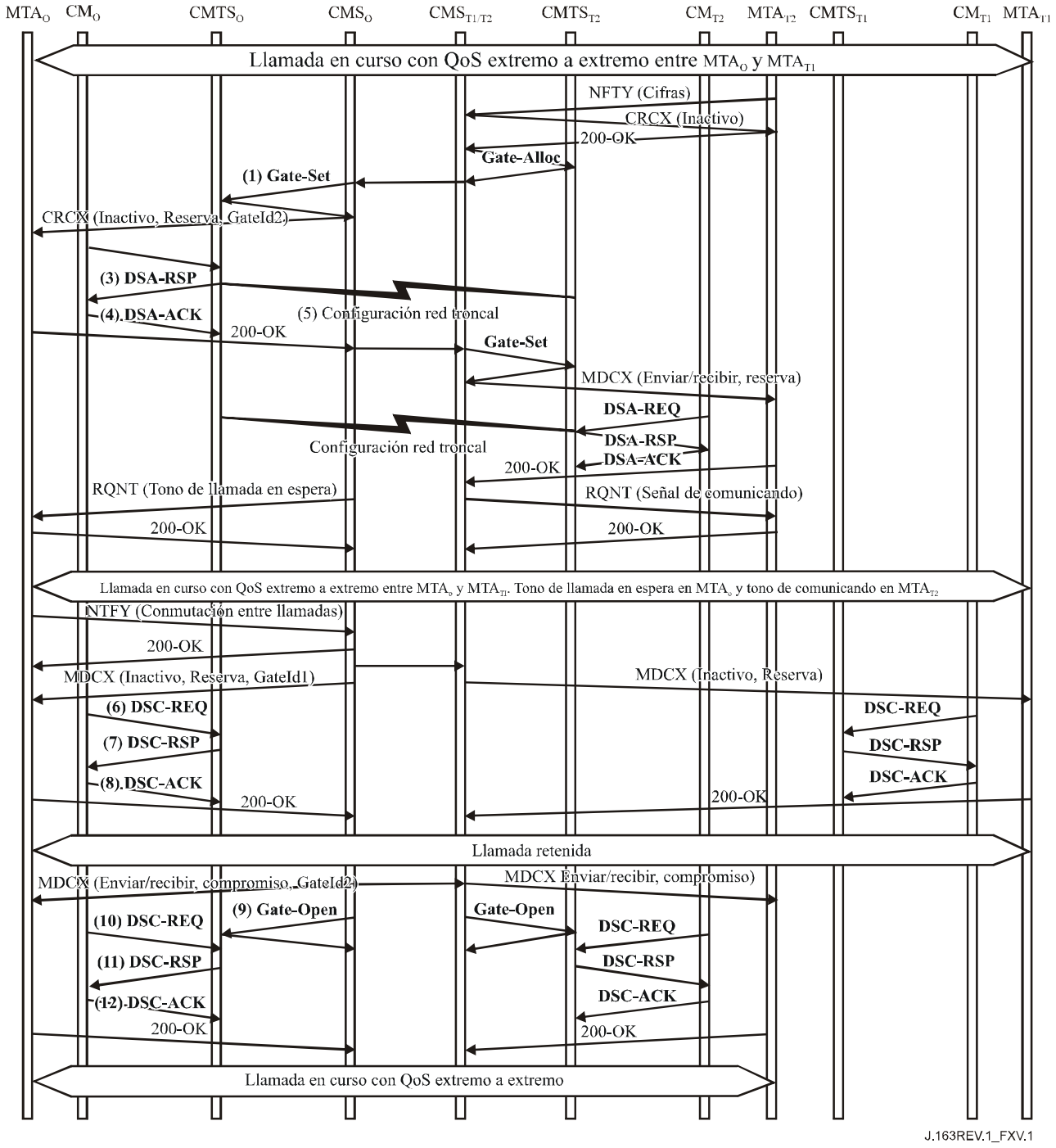


Figura XV.1/J.163 – Llamada en espera con NCS

1) Al recibir la información de señalización del $CMS_{T1/T2}$ el CMSo autoriza la admisión de la nueva conexión en el CMTSo.

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición del total de recursos utilizados por este cliente.
Información de puerta distante	Dirección CMTS	CMSo	Información necesaria para realizar la coordinación de puertas. Obsérvese que el CMS se ha designado como entidad encargada del intercambio de mensajes de coordinación de puertas.
	Puerto CMTS	2052	
	ID puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	No enviar apertura de puerta	
Información de generación de eventos	RKS-Addr	RKS	Dirección del servidor de mantenimiento de registros (RKS).
	RKS-Port	3288	Puerto del servidor de mantenimiento de registros.
	ID de correlación para facturación	<id>	Datos opacos que se comunican al RKS cuando se comprometen recursos.
Especificación de puerta	Sentido	Asc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	MTAo	
	Dirección de destino	MTAt2	
	Puerto de fuente	0	
	Puerto de destino	7000	
	DSCP	6	Valor de tipo de paquete en sentido ascendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

GATE-SET (establecimiento de puerta)

Especificación de puerta	Sentido	Desc.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de fuente	MTA_{T2}	
	Dirección de destino	MTAo	
	Puerto de fuente	0	
	Puerto de destino	7120	
	DSCP	9	Valor tipo de paquete en sentido descendente.
	T1	180000	Tiempo máximo entre la reserva y el compromiso.
	T2	2000	Tiempo máximo para realizar la coordinación de puertas.
	r	12000	Parámetros de la anchura de banda máxima que el EMTAo está autorizado a solicitar para esta conversación.
	b	120	
	p	12000	
	m	120	
	M	120	
	R	12000	
	S	0	

El CMTSo responde a la instrucción establecimiento de puerta con un acuse de recibo.

GATE-SET-ACK (acuse de establecimiento de puerta)

ID de transacción		3177	
Abonado		MTAo	Petición del total de recursos utilizados por este cliente.
ID de puerta		37130	Identificador de la puerta asignada.
Total de actividad		3	Número total de conexiones establecidas por este cliente.

2) Al recibir la instrucción CRCX del CMS, el MTAo calcula los parámetros de QoS para el enlace DOCSIS 1.1. Utiliza la interfaz del anexo E al anexo B/J.112 con el módem de cable para enviar el siguiente mensaje DSA-REQ al CMTS, que establece los parámetros en los sentidos ascendente y descendente. El tamaño de autorización sin petición en sentido ascendente es 120 (de SDP), más 18 (tara Ethernet), menos 40 (valor de supresión de cabecera), más 13 (cabecera DOCSIS). La supresión de cabecera significa los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se incluye en el mensaje DSA-REQ.

NOTA – Esta operación DSA identifica la puerta GateId2 (37130) y el identificador de recursos (ResourceId) de la llamada original comunicado por el CRCX (3333) en el bloque de autorización. Así se informa al CMTS que este flujo de servicio debería compartir los recursos DOCSIS subyacentes con el flujo de servicio de la llamada original.

DSA-REQ

Identificador de transacción		1
Flujo de servicio ascendente	Ref. flujo de servicio	1
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Ref. flujo de servicio	2
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Ref. flujo de servicio	1
	Ref. clasificador de paquete	1
	Prioridad de clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MGt2
	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Ref. flujo de servicio	2
	Ref. clasificador de paquete	2
	Prioridad de clasificador	150
	Estado activac. clasificador	Inactivo (0)
	Dirección fuente IP	MGt2
	Dirección destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
Supresión de cabecera de cabida útil	Referencia del clasificador	1
	Referencia flujo de servicio	1
	Índice supresión de cabecera	1
	Campo supresión cabecera	<42bytes>
	Máscara supresión cabecera	<42bits>
	Tamaño supresión cabecera	42
	Verificar supresión cabecera	Verificar (0)
Bloque de autorización	GateID	37130
	ResourceID	3333
HMAC		

3) El CMTS comprueba la autorización buscando una puerta cuyo identificador (Gate-ID) corresponda al valor de AuthBlock, comprueba los recursos que tendrá que asignar (por ejemplo, espacio estructurado de supresión de cabecera, identificadores de flujo de servicio, espacio estructurado de clasificador) e instala los clasificadores. Si la operación se realiza satisfactoriamente devuelve el mensaje DSA-RSP con el indicador positivo.

DSA-RSP

Identificador de transacción		1
Código de confirmación		Positivo (0)
Flujo de servicio ascendente	Referencia flujo de servicio	1
	Identificador flujo de servicio	1002
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuación autoriz. tolerada	2 ms
	Autorizaciones por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Referencia flujo de servicio	2
	Identificador flujo de servicio	2002
	Tipo parámetros QoS	Admitido (2)
	Plazo estado Admitido	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificación de paquete ascendente	Referencia flujo de servicio	1
	Ref. clasificador de paquete	1
	Identif. clasificador de paquete	3001
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MGt2
	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificación de paquete descendente	Referencia flujo de servicio	2
	Ref. clasificador de paquete	2
	Identif. clasificador de paquete	3002
	Prioridad del clasificador	150
	Estado activación clasificador	Inactivo (0)
	Dirección fuente IP	MGt2
	Dirección destino IP	MTAo
	Puerto destino IP	7124

DSA-RSP

Clasificación de paquete descendente	Protocolo IP	UDP (17)
Bloque de autorización	Identif. de recurso	3333
HMAC		

4) El CM acusa recibo del mensaje DSA-RSP enviando un mensaje DSA-ACK.

DSA-ACK

ID de transacción		2004
Código de confirmación		Positivo (0)
HMAC		

5) Simultáneamente con el mensaje N.° 3 el CMTS inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos utilizados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal envía al CMTS la notificación necesaria para indicar que la reserva se ha realizado satisfactoriamente.

6) Respondiendo a los mensajes de señalización que indican la intención del usuario de cambiar la parte llamante (el MTAo detecta una acción de conmutación de llamadas), el MTAo utiliza la interfaz del anexo E al anexo B/J.112 para desactivar los recursos admitidos en el flujo de servicio N.° 1. Lo hace enviando una instrucción DOCSIS 1.1 DSC-REQ al CMTS.

DSC-REQ (petición DSC)

ID de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Activo	200
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuac. autoriz. tolerada	2 ms
	Autorizac. por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2001
	Tipo parámetros de QoS	Admitido (2)
	Plazo estado Activo	200
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificador de paquetes en sentido ascendente	Identif. flujo de servicio	1001
	Identif. clasif. de paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Inactivo (0)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MGt1

DSC-REQ (petición DSC)

Clasificador de paquetes en sentido ascendente	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificador de paquetes en sentido descendente	Identif. flujo de servicio	2001
	Identif. clasif. de paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasific.	Inactivo (0)
	Dirección fuente IP	MGt1
	Dirección destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
Bloque de autorización	GateID	37125
HMAC		

7) El CMTS envía un mensaje DSC-RSP para indicar que la operación se ha realizado satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

8) El CM envía un mensaje DSC-ACK para indicar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-ACK

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

9) El CMS envía un mensaje de apertura de puerta al CMTS para informarle que se deberían comprometer los recursos para la puerta N.° 2. El CMTS debería revocar la autorización de puerta en caso de no recibir rápidamente un mensaje DSC-REQ del MTAo.

GATE-OPEN

ID de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
Gate ID		37130	Identificador de puerta en el CMTS.
HMAC			Suma de control de seguridad para este mensaje.

El CMTS responde a este mensaje GATE-OPEN:

GATE-OPEN-ACK

ID de transacción		72	Identificador para concordancia de este mensaje y la respuesta.
HMAC			Suma de control de seguridad para este mensaje.

10) Después de invalidar la conexión para el flujo de servicio N.° 1, el CMS envía un mensaje de señalización al MTA para activar los recursos de la conexión N.° 2. El MTAo utiliza la interfaz del anexo E al anexo B/J.112 para activar los recursos admitidos, enviando una instrucción DOCSIS 1.1 DSC-REQ al CMTS.

DSC-REQ (petición DSC)

ID de transacción		2
Flujo de servicio ascendente	Identif. flujo de servicio	1002
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Planificac. flujo de servicio	UGS (6)
	Intervalo autoriz. nominal	10 ms
	Fluctuac. autoriz. tolerada	2 ms
	Autorizac. por intervalo	1
	Tamaño autoriz. sin petición	111
Flujo de servicio descendente	Identif. flujo de servicio	2002
	Tipo parámetros de QoS	Admitido + Activo (6)
	Plazo estado Activo	10
	Prioridad del tráfico	5
	Veloc. máxima sostenida	12000
Clasificador de paquetes en sentido ascendente	Identif. flujo de servicio	1002
	Ident. clasif. de paquete	3001
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasif.	Activo (1)
	Dirección fuente IP	MTAo
	Puerto fuente IP	7120
	Dirección destino IP	MGt2
	Puerto destino IP	7000
	Protocolo IP	UDP (17)
Clasificador de paquetes en sentido descendente	Identif. flujo de servicio	2002
	Ident. clasif. de paquete	3002
	Acción modif. clasificador	Reemplazar (1)
	Prioridad del clasificador	150
	Estado activación clasific.	Activo (1)
	Dirección fuente IP	MGt2
	Dirección destino IP	MTAo
	Puerto destino IP	7124
	Protocolo IP	UDP (17)
Bloque de autorización	GateID	37130
HMAC		

11) El CMTS envía un mensaje DSC-RSP para indicar que la operación se ha realizado satisfactoriamente.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

12) El CM envía un mensaje DSC-ACK para indicar que ha recibido y aceptado el mensaje DSC-RSP.

DSC-RSP

ID de transacción		2
Código de confirmación		Positivo (0)
HMAC		

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
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	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
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 y comunicación entre sistemas abiertos
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, 2005