UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.163

(03/2001)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE J: TRANSMISIONES DE SEÑALES RADIOFÓNICAS, DE TELEVISIÓN 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

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE J

TRANSMISIONES DE SEÑALES RADIOFÓNICAS, DE TELEVISIÓN Y DE OTRAS SEÑALES MULTIMEDIOS

Recomendaciones generales	J.1–J.9
Especificaciones generales para transmisiones radiofónicas analógicas	J.10–J.19
Características de funcionamiento de los circuitos radiofónicos	J.20–J.29
Equipos y líneas utilizados para circuitos radiofónicos analógicos	J.30–J.39
Codificadores digitales para señales radiofónicas analógicas	J.40–J.49
Transmisión digital de señales radiofónicas	J.50–J.59
Circuitos para transmisiones de televisión analógica	J.60–J.69
Transmisiones de televisión analógica por líneas metálicas e interconexión con radioenlaces	J.70–J.79
Transmisión digital de señales de televisión	J.80–J.89
Servicios digitales auxiliares para transmisiones de televisión	J.90–J.99
Requisitos operacionales y métodos para transmisiones de televisión	J.100–J.109
Sistemas interactivos para distribución de televisión digital	J.110–J.129
Transporte de señales MPEG-2 por redes de transmisión de paquetes	J.130–J.139
Mediciones de la calidad de servicio	J.140–J.149
Distribución de televisión digital por redes locales de abonados	J.150–J.159
IPCablecom	**J.160–J.179**

Para más información, véase la Lista de Recomendaciones del UIT-T.

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 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 con UIT-T J.83 y J.112. Dichos operadores 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.

Orígenes

La Recomendación UIT-T J.163, preparada por la Comisión de Estudio 9 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 9 de marzo de 2001.

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.

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Página

Recomendación UIT-T J.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 que un dispositivo de cliente solicite una calidad de servicio específica de la red J.112. La utilización de esta Recomendación se ilustra mediante ejemplos muy amplios. El alcance de esta Recomendación es la definición de 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.

NOTA – La referencia a un documento en esta Recomendación no otroga al mismo, de por sí, la calificación de Recomendación.

Referencias normativas

- UIT-T J.83 (1997), *Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable.*
- UIT-T J.112 (1998), *Sistemas de transmisión para servicios interactivos de televisión por cable.*
- UIT-T J.112 Anexo A (2001), *Radiodifusión de vídeo digital: Canal de interacción para sistemas de distribución de televisión por cable.*
- UIT-T J.112 Anexo B (2001), *Especificaciones de la interfaz del servicio de transmisión de datos por cable: Especificación de interfaz de radiofrecuencia.*
- UIT-T J.160 (2001), *Marco arquitectural para la prestación de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable.*
- 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)*.

Referencias informativas

– UIT-T G.114 (2000), *Tiempo de transmisión en un sentido.*

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

– UIT-T G.726 (1999), *Modulación por impulsos codificados diferencial adaptativa (MICDA) a 40, 32, 24, 16 kbit/s.*

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

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

– UIT-T J.162 (2001), *Protocolo de señalización de llamada de red para la prestación de servicios dependientes del tiempo de pordes de televisión por cable que utilizan módems de cable.*

– UIT-T J.164 (2001), *Requisitos de los mensajes de eventos para soportar servicios en tiempo real sobre redes de televisión por cable utilizando módems de cable.*

– UIT-T J.170 (2001), *Especificación de la seguridad sobre redes de comunicaciones por cable IP (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), *Session Initiation Protocol (SIP).*

– 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.*

– Draft-bernet-dclass-01, *Use and Format of the DCLASS Object with RSVP Signalling,* octubre de 1999.

– Draft-ietf-rsvp-refresh-reduct-02, *RSVP Refresh Overhead Reduction Extensions,* Enero de 2000.

– Draft-davie-intserv-compress-02, *Integrated Services in the Presence of Compressible Flows,* Febrero de 2000.

– Draft-ietf-mpls-rsvp-lsp-tunnel-06, *RSVP-TE Extensions to RSVP for LSP Tunnels*, Mayo de 2000.

– Draft-ietf-rap-pr-02, *COPS usage for Policy Provisioning* (2000).

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

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.

3.2 nodo de acceso: Tal como se utiliza en esta Recomendación, un nodo de acceso es un dispositivo de terminación de capa dos en el que termina el extremo de red de una conexión J.112. Es función de la tecnología. En UIT-T J.112 anexo A, se denomina adaptador de red interactivo o INA (*interactive network adapter*), mientras que en el anexo B de la misma se denomina nodo de acceso (AN, *access node*).

3.3 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 UIT-T J.112.

3.4 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 modems de cable.

3.5 DEBE: El término DEBE o NO DEBE se utiliza en esta Recomendación como un convenio para denotar un aspecto absolutamente obligatorio de la misma.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas:

AN Nodo de acceso (*access node*)

CM Módem de cable (*cable modem*)

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*)

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 la carga útil (*payload header suppression*)

RTPC Red telefónica pública conmutada

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*)

TLV Valor de longitud de tiempo (*type-length-value*)

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

5 Visión de conjunto de carácter técnico

La calidad de servicio mejorada es necesaria para poder ofrecer aplicaciones multimedios interactivos. Los recursos disponibles pueden estar limitados en determinados segmentos de la red, por lo que se requiere la asignación de recursos en la misma. El alcance de esta Recomendación es definir la arquitectura de calidad de servicio para la porción de "acceso" de la red IPCablecom. La porción de acceso de la red se define como la parte de la red comprendida entre el adaptador de terminal multimedios (MTA, *multimedia terminal adapter*) y el nodo de acceso (AN, *access network*), 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, siendo responsabilidad de los protocolos que en ella se desarrollan atender dicha necesidad. 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 la red troncal quedan fuera del ámbito de esta Recomendación.

En una red J.112 los recursos se atribuyen a flujos individuales asociados a cada una de las sesiones de una aplicación, para cada abonado, sobre la base de una autorización y autenticación. Esta Recomendación define una sesión de calidad de servicio dinámica (DQoS), o simplemente una sesión, como un flujo de datos bidireccional entre dos clientes. Cuando una aplicación multimedios 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. Las aplicaciones pueden utilizar exclusivamente la mitad de un flujo de datos bidireccional, proporcionando servicios de solo transmisión o de solo recepción. Por ejemplo, en una aplicación de comunicación vocal típica, una comunicación simple entre dos partes se implementa mediante una única sesión, mientras que las comunicaciones complejas, multipartitas (por ejemplo, las "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 (UIT-T J.162) y la señalización de llamada distribuida (SIP, RFC 2543 del IETF). Esta especificación de QoS dinámica es el marco de QoS subyacente para ambos protocolos de señalización de llamada. La QoS se asigna a los 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. Se aprovecha la información disponible en los protocolos de señalización para realizar asignaciones de QoS en el segmento "local" (la red J.112 cercana a la parte original) y en el segmento "distante" (la red J.112 cercana a la parte terminal). Por lo tanto, esta Recomendación permite que distintos proveedores utilicen los mecanismos más apropiados para el segmento que están gestionando. La utilización de 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 utilizar el marco de IPCablecom para 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.

La especificación de QoS dinámica reconoce que los requisitos de un servicio de comunicaciones vocales comercialmente viable son análogos a los que se ofrecen mediante la red telefónica pública conmutada. Es importante garantizar que los recursos están disponibles antes de invitar a que las dos partes que participan en una sesión se comuniquen. Por lo tanto, los recursos se reservan antes de que se notifique al receptor de la comunicación que alguien está intentando iniciar una comunicación. Si los recursos disponibles para una sesión son insuficientes, ésta se bloquea.

Los protocolos que se desarrollan en esta Recomendación reconocen explícitamente la necesidad de asegurar que no existe riesgo potencial de fraude o de hurto del servicio por parte de puntos extremos que no deseen cooperar con la señalización de la llamada y con los protocolos de señalización de QoS con el objeto de evitar ser tasados por la utilización realizada. Esta Recomendación introduce el concepto de activación en dos fases para la reserva de recursos (reserva y compromiso). En ambas fases un proveedor sólo asigna recursos cuando éstos han sido solicitados (cuando el trayecto vocal está establecido) lo cual puede utilizarse con fines de facturación. Además, y debido a que la segunda fase de compromiso de recursos necesita una petición explícita del MTA, ello permite al proveedor evitar el fraude y el hurto del servicio.

5.1 Requisitos de la arquitectura de calidad de servicio IPCablecom

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

1) *Proporcionar a IPCablecom facilidades de cómputo de los recursos de QoS de cada sesión*

   Se considera que, desde la perspectiva de facturación, uno de los recursos que deberá tenerse en cuenta sea la utilización de facilidades de QoS en una red J.112. Por lo tanto, la información debe identificarse de tal forma que sea posible 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 (que, por ejemplo, funcionen sobre la base 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 pendiente de 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*

   Los distintos tipos de sesiones deben poder tener distintos tipos de características de QoS. Así, por ejemplo, las sesiones en el dominio de un determinado proveedor OPERADOR DE CABLE pueden tener una QoS diferente a las sesiones externas a dicho dominio (por ejemplo, sesiones internacionales que incluyan enlaces con la RTPC). Esta especificación de QoS dinámica puede permitir 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 del sector negocios durante ciertas horas del día en comparación con la ofrecida a clientes residenciales) 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 con precisión, pero que provoca que se deniegue el servicio a otros, y aquélla que no se factura con precisión pero que puede producir la sustracción o hurto del servicio. Las aplicaciones de abonado y las aplicaciones IPCablecom (ya sean integradas o basadas en PC) pueden abusar de forma inadvertida o intencionada de sus privilegios de QoS (por ejemplo, utilizar para aplicaciones de tipo FTP una QoS que el proveedor desea limitar a aplicaciones vocales). Aunque es previsible que la red J.112 imponga a un acceso de usuario una QoS determinada, 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 las direcciones ascendente y descendente de las redes J.112*

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

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

Debe ser posible establecer una política (definida en términos de marcar, descartar o retardar paquetes) aplicable a todos los aspectos de la QoS definidos para el servicio en el AN mediante los mecanismos de QoS de J.112. Además, se deben soportar varios modelos de concordancia de flujos – asociar una sesión IPCablecom a un flujo J.112 y asociar múltiples sesiones IPCablecom a un único flujo J.112.

7) *El AN impone la política*

En última instancia, es prerrogativa del AN controlar la política. La filosofía es que cualquier cliente puede hacer una petición de QoS, pero el AN (o una entidad que actúa tras el AN) 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 de 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) *Reclamar recursos de QoS para sesiones muertas/interrumpidas*

En el caso de sesiones que no estén activas y que no se hubiesen cerrado adecuadamente, es necesario volver a solicitar y atribuir los valiosos recursos de QoS. No deberían haber "pérdidas" de recursos en el enlace J.112. Por ejemplo, si un módulo de cliente IPCablecom sufre un malfuncionamiento en el transcurso de una sesión IPCablecom, todos los recursos de QoS J.112 utilizados en dicha sesión se liberan cuando transcurre un periodo de tiempo razonable.

10) *Realizar cambios en la política de QoS dinámica*

Es deseable poder cambiar 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, si no mejor, en lo que se refiere al tiempo de establecimiento y a la métrica del retardo de postselección.

12) *Gestionar múltiples sesiones concurrentes*

Es deseable poder 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), o características definidas por el usuario destinadas a modificar los niveles de QoS o para la detección de flujos de facsímil o de módem (que necesitan cambiar de un CÓDEC con compresión a G.711).

14) *Soportar múltiples modelos de control de QoS*

Es significativo señalar la importancia del inicio de señalización de QoS tanto desde el lado de usuario como desde el lado de red. Desde el lado del usuario, una aplicación puede iniciar inmediatamente su petición de QoS cuando considere que necesita una 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 IPCablemodem (y en otras aplicaciones). La presente Recomendación sólo incluye la señalización del lado de abonado.

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

Debe poder señalizarse la 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 especificado utilizando 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 multimedios (MTA)

El dispositivo de cliente de una red IPCablecom (es decir, el MTA) puede ser uno de los dispositivos siguientes. Estos dispositivos se ubican junto al usuario y están conectados a la red a través del canal J.112. Se presupone que todos los MTA implementan algún protocolo de señalización multimedios, tal como el J.162. Un MTA puede ser un dispositivo con un terminal telefónico a dos hilos en la configuración MTA-1, o puede añadir capacidades de entrada/salida de vídeo en la configuración MTA-2. Puede tener capacidades mínimas o bien, implementar esta funcionalidad en una computadora personal multimedios, 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 multimedios 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 multimedios sin incorporar una interfaz de capa MAC J.112. El MTA autónomo utiliza típicamente Ethernet, USB o IEEE1394 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

El módem de cable (CM, *cable modem*) es el elemento de la red IPCablecom, tal como se define en UIT-T J.112. El módem de cable es responsable de la clasificación, la política y el marcaje de los paquetes una vez que los protocolos de señalización han establecido los flujos de tráfico.

5.2.3 Nodo de acceso

El nodo de acceso (AN) es el elemento de la red IPCablecom que contiene funciones centralizadas responsables del procesamiento de los flujos de información. El AN actúa como punto de imposición de la política (PEP, *policy enforcement point*) en el marco del protocolo de asignación de recursos (RAP, *resource allocation protocol*) del IETF.

Un AN implementa una "puerta IPCablecom de QoS dinámica" (en adelante denominada simplemente "puerta") entre la red J.112 y una red troncal IP. La puerta se implementa utilizando las funciones de clasificación y filtrado de paquetes definida en UIT-T J.112.

El AN puede o no ser configurado como una entidad "frontera IS-DS". Una frontera IS-DS presenta una interfaz con una red que utiliza el modelo de control de QoS de servicios integrados (Intserv, *integrated services*) y algún otro modelo, por ejemplo, el de servicios diferenciados (DiffServ, *differentiated services*).

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 multimedios [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 término controlador de puerta (GC) se utiliza para hacer referencia a la porción de cualquier tipo de CMS que realice 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 nodo de acceso (AN). El GC actúa como un punto de decisión de la política (PDP) en el marco del 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 UIT-T J.112, en el RSVP del IETF y en la QoS garantizada de servicios integrados del IETF.

Específicamente, la arquitectura de QoS IPCablecom utiliza el protocolo definido en UIT-T J.112 para la red de televisión por cable. Estos mensajes soportan la instalación estática y dinámica de clasificadores de paquetes (es decir, especificaciones de filtro) y la planificación de flujos (es decir, 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 de forma similar a los objetos TSPEC y RSPEC definidos en el protocolo de reserva de recursos (RSVP, *resource reservation protocolo*) del IETF. Ello 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.

El módem de cable (CM), a través del cual el tráfico accede a la red J.112 con capacidad de QoS, es responsable de lo siguiente:

- Clasificar el tráfico IP en flujos J.112 sobre la base de especificaciones de filtro definidas.
- Realizar las funciones de conformación de tráfico y de aplicación de la política conforme a lo requerido por la especificación de flujo.
- Mantener el conocimiento sobre el estado de los flujos activos.
- Modificar el campo tipo de servicio (TOS, *type of service*) en las cabeceras de los paquetes IP ascendentes sobre la base de la política del operador de red.
- Obtener del AN la QoS J.112 requerida.
- Aplicar adecuadamente los mecanismos de QoS J.112.

El AN es responsable de lo siguiente:

- Proporcionar al CM la QoS requerida sobre la base de la configuración de la política.
- Atribuir la anchura de banda 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 especificaciones de filtro definidas.
- Aplicar la política al campo TOS de los paquetes procedentes de la red J.112 fijando los valores del mismo según sea la política del operador de red.
- Modificar el campo TOS de las cabeceras de paquetes IP descendentes sobre la base de la política del operador de red.
- Aplicar la conformación de tráfico y la política de acuerdo con 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 conocimiento sobre 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. En una red troncal DiffServ, los dispositivos de la misma 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 del SDP o protocolo de descripción de sesión), en la capa de red (por ejemplo, RSVP) y en capa del enlace de datos (por ejemplo, QoS J.112). Asimismo, los requisitos para la imposición de la política y los vínculos de sistema que existen entre los sistemas de soporte de operaciones (OSS, *operation support systems*) de provisión de abonado, el control de admisión en la red troncal IP y el control de admisión en la red J.112, crean la necesidad de interfaces adicionales entre componentes de la red IPCablecom.

En UIT-T J.160, relativa al marco arquitectónico de IPCablecom, se hace una descripción detallada del marco arquitectónico de QoS, tal como se muestra en la figura 1.

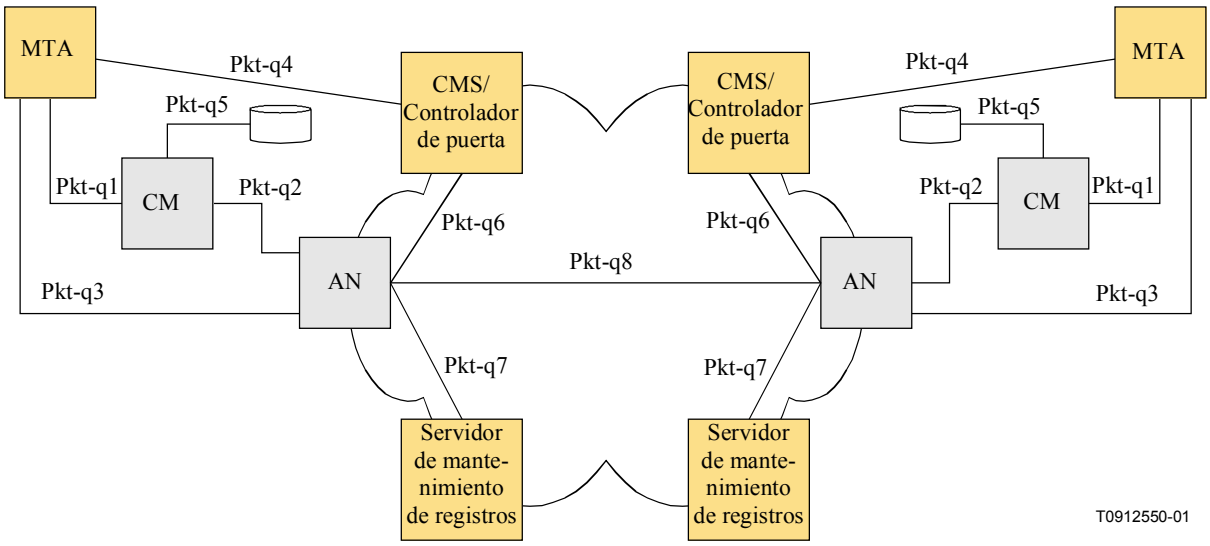


Figura 1/J.163 – Interfaces de señalización de QoS en una red IPCablecom

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 variaciones de protocolo. Todas las interfaces, excepto la pkt-q5 se utilizan para la QoS dinámica. En el cuadro 1 se identifica someramente cada interfaz y como se utilizan en la especificación de QoS dinámica (DQoS, *dynamic QoS specification*). Se muestran dos alternativas para esta especificación: primero, una interfaz general que es aplicable a los MTA integrados o a los MTA autónomos; segundo, una interfaz facultativa que sólo está disponible en 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-AN	QoS J.112, iniciada por el AN	QoS J.112, iniciada por el CM
pkt-q3	MTA-AN	RSVP+	No disponible
pkt-q4	MTA-GC/CMS	NCS/DCS	NCS/DCS
pkt-q5	CM-Servidor de aprovisionamiento	No disponible	No disponible
pkt-q6	GC-AN	Gestión de puerta	Gestión de puerta
pkt-q7	AN-RKS	Facturación	Facturación
pkt-q8	AN-AN	Gestión de puerta	Gestión de puerta

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 y sus parámetros de QoS de tráfico y reglas de clasificación asociadas.
- Sincronización: utilizada para sincronizar la paquetización y la planificación al objeto de minimizar el retardo y la fluctuación de fase.
- Transporte: utilizada para procesar paquetes en el tren de medios y realizar el adecuado procesamiento de QoS de cada paquete.

Esta interfaz se define conceptualmente en UIT-T J.112. Para MTA autónomos no se define ejemplar alguno del mismo.

pkt-q2: Interfaz de QoS J.112 entre CM y AN

Es la interfaz de QoS J.112 (control, planificación y transporte). Las funciones de control pueden ser iniciadas desde el CM o el AN. Sin embargo, el AN es el árbitro de la política final y garante de los recursos gracias a la realización del control de admisión para la red J.112. Esta interfaz se define en UIT-T J.112.

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

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 AN, los flujos J.112 se activan utilizando la señalización originada en AN sobre la interfaz pkt-q2.

pkt-q4: Señalización de la capa de aplicación entre GC/CMS y MTA

A través de esta interfaz se señalizan muchos parámetros tales como el tren de medios, las direcciones IP, los números de puertos, así como la selección del códec y las características de paquetización. DCS y NCS son dos ejemplos de señalización de capa de aplicación.

pkt-q5: Señalización entre el sistema de aprovisionamiento 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 AN

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 AN.

pkt-q7: Interfaz entre AN y el servidor de mantenimiento de registros

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

pkt-q8: Interfaz entre AN y AN

Esta interfaz se utiliza para la coordinación de recursos (puertas) entre el AN del MTA local, y el AN del MTA distante. El AN es responsable de la política y asignación de recursos de QoS en la red J.112 que gestiona.

5.5 Marco de referencia para la QoS de IPCablecom

Para que el usuario final considere justificados los costes de un servicio multimedios comercial (por ejemplo, capacidad de comunicaciones vocales), éste puede necesitar 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 como para no interferir las interacciones multimedios normales. Para el servicio de telefonía normal que utiliza 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 absorber una cantidad significativa del retardo total posible, 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 puede considerarse adecuada como para ser considerado como un servicio sustitutivo del 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 señalización por parte de un usuario de una petición de conexión y la recepción de la confirmación desde 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 que un usuario descuelga para atender una llamada y el establecimiento del trayecto vocal sea lo suficientemente corto para que no se recorte el "hola" inicial. Debe ser inferior a 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 sean autenticados y autorizados antes de acceder a la QoS mejorada asociada al servicio. Garantiza que los recursos de red estén disponibles extremo a extremo antes de alertar al MTA de destino. Finalmente, asegura que se contabilice adecuadamente la utilización de recursos, de forma consistente con los convenios del servicio telefónico tradicional de calidad vocal (respecto al cual algunos servicio IPCablecom son similares desde la perspectiva del cliente), y en el cual la tasación sólo se inicia después de que la parte receptora de la comunicación descuelga.

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

---

[1] En 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 de voz y de datos pueden verse degradadas incluso cuando los retardos sean inferiores a 150 ms. Por lo tanto, debe evitarse cualquier aumento en el retardo debido al procesamiento (incluso en conexiones con tiempos de transmisión bastante por debajo de 150 ms), salvo que existan beneficios indudables para el servicio y la aplicación.

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 multimedios. Aún no se ha analizado si las mejoras en la gestión de recursos que presenta esta Recomendación soportarán sin discontinuidad la multidifusión.

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 UIT-T J.112. Los recursos de la red troncal pueden ser gestionados para cada uno de los flujos, o más probablemente, mediante un mecanismo de calidad de servicio agregada. 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.

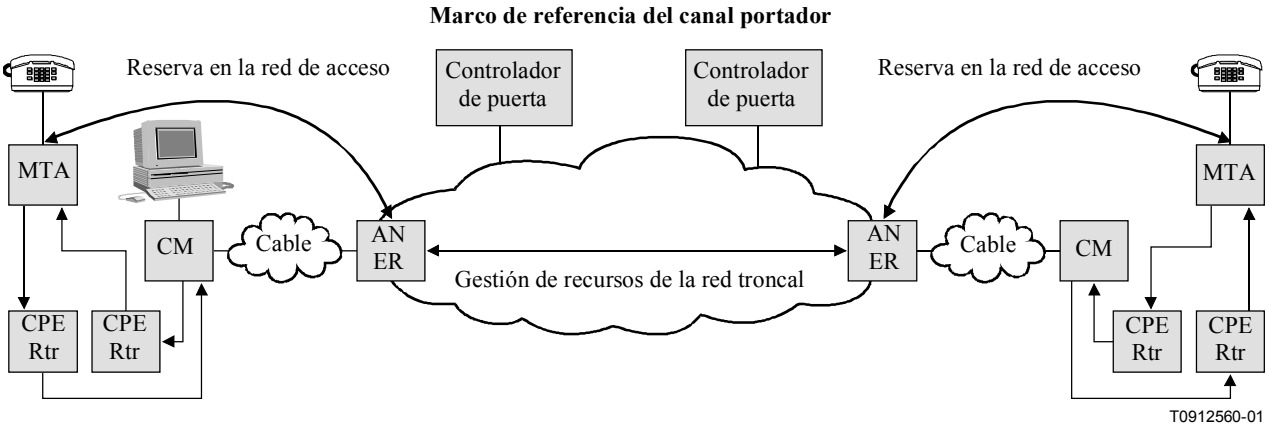


Figura 2/J.163 – Marco de referencia de una sesión

El elemento constructivo definido en términos de QoS y denominado *puerta* constituye un punto de control para la conexión de las redes de acceso a un servicio de alta calidad de la red troncal. Una puerta se implementa mediante un AN 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 reciban 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, las puertas están abiertas para llamadas individuales. La apertura de una puerta implica verificar el control de admisión cuando se recibe del cliente una petición de gestión de recurso para una sesión individual, 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 de 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 y número de puerto de fuente IP específicos hacia una dirección y número de puerto de destino IP específicos.

Una puerta es una entidad lógica que reside en un AN. Un identificador (ID) de puerta se asocia a una sesión individual y tiene significado en la puerta; el ID de puerta es un identificador singular a nivel local del AN, y que es asignado por dicho AN. 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 sobre la base 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.

El controlador de puerta es responsable de la decisión de la política sobre si una puerta debe estar abierta y cuándo. Una puerta se establece con anterioridad a una petición de gestión de recursos. Ello permite que la función política, localizada en el controlador de puerta, sea "sin estados", es decir, que carezca de estados pues 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. Dichos flujos pueden ser transportados en distintos flujos J.112 de la red J.112, como por ejemplo, un enlace de señalización dedicado.

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

El aprovisionamiento de servicios de comunicación vocal sobre redes IP con el mismo nivel de calidad que sobre la red telefónica pública conmutada (RTPC) impone límites a las métricas 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. El proveedor de servicio debe poder controlar el acceso a los recursos de la red a fin de asegurar que está disponible la capacidad extremo a extremo adecuada, incluso en condiciones poco usuales o de sobrecarga. El proveedor de servicio puede tratar de conseguir ingresos adicionales derivados del aprovisionamiento de un servicio de comunicaciones vocales que utilice estas características de calidad mejoradas (es decir, con 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 asegurar que el acceso sólo se proporciona a usuarios autorizados y autenticados de forma específica para cada sesión, sin que se produzca hurto 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.

En las redes J.112 la capacidad es 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 granular. Esta Recomendación sólo trata la QoS de las redes de acceso y es neutra en relación con los esquemas de QoS de la red troncal.

Esta arquitectura se plantea con un elevado grado de generalidad a fin de permitir el desarrollo de nuevos servicios y la ulterior evolución de las arquitecturas de la red. Este objetivo impone diversos requisitos para conseguir una arquitectura de QoS factible, que se describen en las cláusulas siguientes.

5.6.1 Prevención del hurto del servicio

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

- 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, *gate controller*) que participa en la señalización de la

llamada está investido de autoridad para realizar dichas verificaciones y es la única entidad que puede crear una nueva puerta en un AN. 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, de forma consistente con los convenios de los 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. Esto se consigue utilizando puertas y mediante la coordinación entre puertas, que vinculan mecanismos de filtrado de direcciones con la reserva de recursos.

Dado que este servicio puede facturarse por cada utilización que de él se haga, existe un riesgo significativo de fraude y de hurto del servicio. La arquitectura permite al proveedor cobrar por la calidad de servicio ofrecida. Por lo tanto, evita que se produzcan escenarios el hurto de servicio, algunos de los cuales se describen en el apéndice IX.

Los escenarios de hurto de servicio se tratan en esta Recomendación y otras Recomendaciones. Dichos escenarios constituyen 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

Existen dos razones por las que los servicios de comunicación vocal de calidad comercial deben disponer de un protocolo de dos fases para comprometer recursos. En primer lugar, garantiza que los recursos estén disponibles antes de que se señalice a la parte del extremo distante una comunicación entrante. En segundo lugar, garantiza que el registro y la facturación por la utilización no comienzan hasta que el extremo distante haya descolgado, momento en el que también se establece la señal vocal entre las partes. Estas son propiedades que ofrecen los protocolos de señalización de telefonía convencional; se trata de emular exactamente la misma semántica en este caso. Igualmente, si se asigna anchura de banda antes de que el extremo distante haya descolgado, puede producirse el hurto del servicio. La exigencia de que los puntos extremos envíen explícitamente un mensaje de compromiso garantiza que el registro de la utilización se basa en el conocimiento de la misma por la parte extrema y en su actuación explícita.

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 segmentada de recursos

La arquitectura de QoS dinámica realiza una partición de la gestión de recursos en segmentos diferenciados de acceso y de red troncal. La asignación de recursos segmentados es beneficiosa por dos razones:

- Permite que existan diferentes mecanismos de aprovisionamiento de anchura de banda y de señalización para la red del origen, la red del extremo distante y la red troncal.
- Permite que segmentos con pocos recursos escasos mantengan reservas para cada flujo y gestionen cuidadosamente la utilización de los recursos. Al mismo tiempo, cuando los segmentos de la red troncal tienen recursos suficientes como para que la gestión de recursos se realice de forma menos detallada, permite que la red troncal evite mantener el control del estado de cada flujo, mejorando así la escalabilidad.

Cuando la red troncal no requiere una señalización explícita por flujo (como ocurre en el caso de una red troncal con 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).

Potencialmente reduce la cantidad de estados de reserva que se almacenan 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 (por ejemplo, del usuario) y de acceso (para clientes integrados puede, opcionalmente, tratarse de la interfaz de capa MAC J.112). El AN establece una correspondencia entre los mensajes de gestión de recursos y el protocolo de gestión de recursos utilizado en la red troncal (por ejemplo, DiffServ del IETF). También establece una correspondencia entre los mensajes de gestión de recursos y el protocolo de gestión de recursos utilizado en el enlace de acceso (es decir, UIT-T J.112).

5.6.4 Cambio de los recursos durante una sesión

Es posible modificar los recursos asignados a una sesión durante la misma. Ello permite poder realizar cambios durante la sesión, tales como la conmutación desde un códec vocal de baja velocidad a un códec G.711 cuando se detectan tonos de módem, así como la adición de 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 re-reserva es un requisito que permite una utilización eficiente de recursos cuando se invocan servicios tales como llamada en espera. De forma abstracta, la re-reserva toma anchura de banda que fue asignada durante una sesión entre un anfitrión de VoIP y un cliente, y reasigna la misma anchura de banda a una sesión con un cliente distinto.

Es importante entender cabalmente el peligro potencial que supone la desasignación de la anchura de banda de una sesión y volver a realizar una nueva petición para asignar de nuevo anchura de banda. Existe el riesgo de que otro cliente utilice la anchura de banda que permanece entre ambos pasos, dejando a la sesión original sin un trayecto de calidad garantizada. El mecanismo de re-reserva en un solo paso lo evita, ya que la anchura de banda no queda en ningún momento a disposición de otros clientes.

5.6.6 Calidad de funcionamiento de la QoS dinámica

Los mensajes de QoS se realizan en tiempo real mientras los llamantes esperan que los servicios sean activados o modificados. Por lo tanto, es necesario que el protocolo sea rápido. Se minimiza el número de mensajes, especialmente el número de mensajes que transitan la red troncal y el número de mensajes ascendentes J.112. En la red J.112, en la que no hay posibilidad de que sean distintos los trayectos directos e inversos, este protocolo añade varios objetos nuevos al RSVP que permiten que el AN reduzca el retardo actuando como representante, o proxy, del cliente del extremo lejano.

Los mensajes RSVP, los mensajes de gestión J.112 y los mensajes de señalización de llamada (a los que en conjunto se hace referencia como a mensajes de señalización) son todos transportados por la red J.112 en base al mejor esfuerzo. Si el CM también soporta servicios de datos, el servicio basado en el mejor esfuerzo puede ser incapaz de proporcionar el bajo retardo preciso para los mensajes de señalización. En esta situación, el CM PUEDE disponer de un flujo J.112 separado, con QoS mejorada, destinado a transportar tráfico de señalización. El aprovisionamiento de este flujo J.112 separado se hace de la misma forma que la de otros trenes de medios J.112 y PUEDE incluir clasificadores de tal forma que su presencia sea transparente al 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 de sesión que se asigna a cada sesión, siendo ésta una política que ejerce el agente de llamada/controlador de puerta cuando se hace la petición inicial de sesión (por ejemplo, con la primera etapa INVITACIÓN en la RFC 2543 del IETF relativa al SIP, o protocolo de inicio de sesión).

5.6.8 Soporte de redes intermedias

La arquitectura no debe impedir que existan redes intermedias entre el MTA o anfitrión multimedios 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, es posible realizar la asignación de anchura de banda en la red J.112 del OPERADOR DE CABLE cuando existe una red intermedia. Asimismo, es deseable disponer de una solución que permita de forma transparente la reserva de recursos de la red intermedia.

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 abiertos, suficientemente generales, que son compatibles con muchos de los mecanismos de QoS de la red troncal.

5.7 Teoría de la operación

5.7.1 Establecimiento de la sesión básica

La reserva de recursos se divide en dos fases separadas, la reserva y el 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 de forma que el usuario pueda ser facturado por dicha utilización.

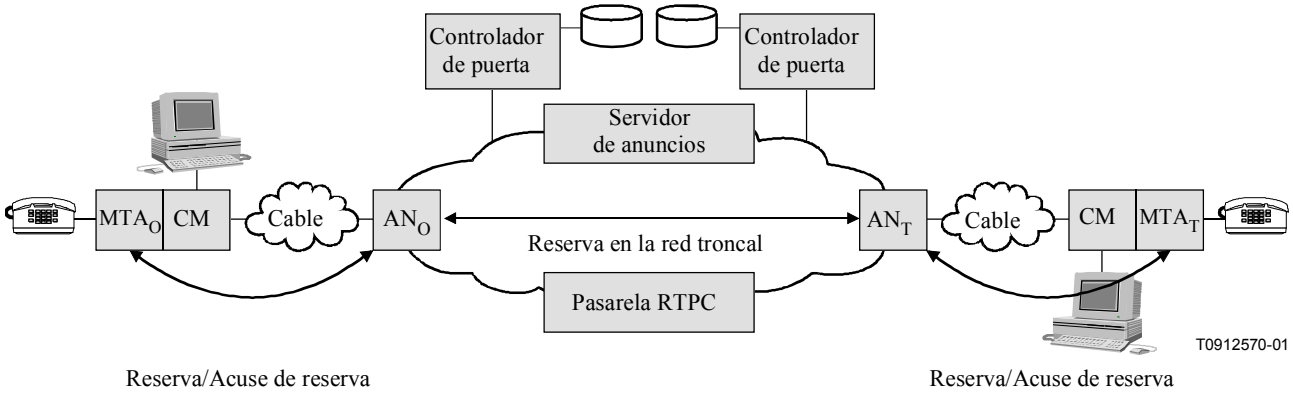


Figura 3/J.163 – Fase 1 de la gestión de recursos

La figura 3 muestra la primera fase del protocolo de gestión de recursos para una aplicación multimedios. 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 realizan a AN_O y AN_T respectivamente una petición de reserva de recursos (mensaje PATH, "trayecto", de RSVP, o mensaje J.112 de la interfaz facultativa para cliente integrados). AN_O y AN_T realizan una verificación del control de admisión en relación con la disponibilidad de recursos (señalización de inicio para la reserva de recursos en la red troncal, si ello es necesario) y envían una respuesta a los MTA respectivos. En el contexto de RSVP,

el mensaje RESV desde el AN (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) que ordena el inicio de la emisión de señal de llamada del teléfono. MTA_T envía una indicación RINGING (tono de llamada activado) al MTA_O indicando 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 AN_T. Cuando MTA_O recibe el mensaje ANSWERED, el MTA_O envía al AN_O un mensaje COMMIT. El mensaje COMMIT hace que los recursos se reasignen para la llamada en las redes J.112. La llegada de los mensajes COMMIT a AN_T y a AN_O hace que éstos abran sus puertas y que se comience a contabilizar la utilización de recursos. Para evitar que se produzcan escenarios de hurto de servicio, los AN coordinan la apertura de las puertas intercambiando mensajes 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).

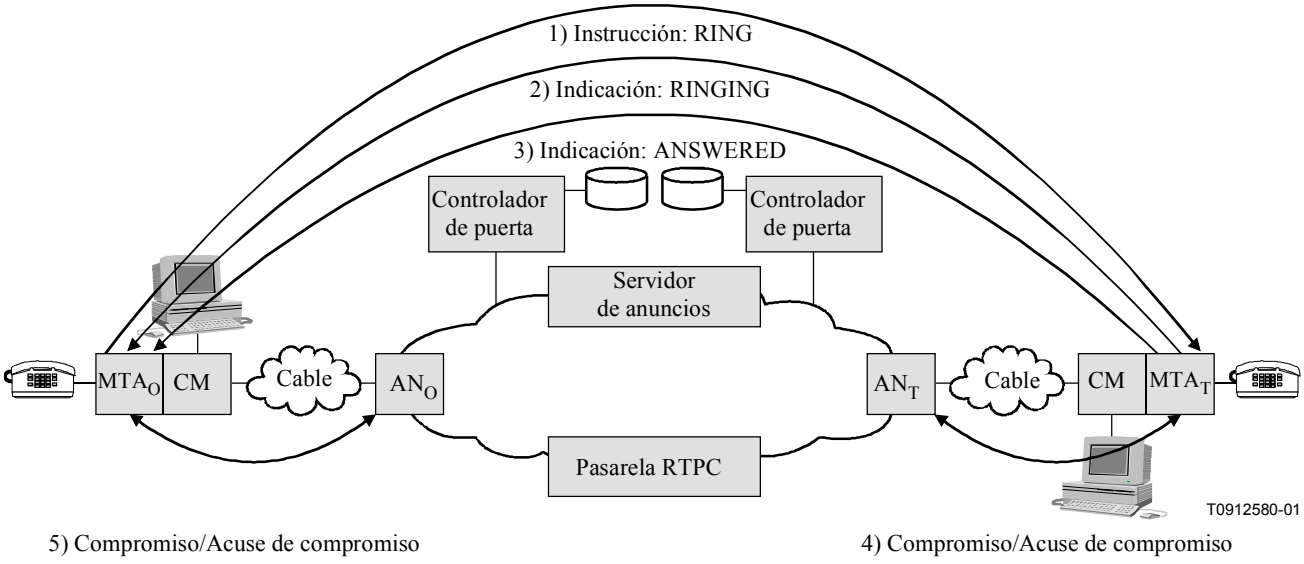


Figura 4/J.163 – Fase 2 de la gestión de recursos

5.7.2 Coordinación de puerta

La señalización de QoS da lugar a la creación de una puerta en cada AN asociado con un cliente que participe en la sesión. Cada puerta mantiene los datos de utilización para la sesión y controla si los paquetes generados por el cliente asociado accede a la QoS mejorada. La coordinación de puertas es necesaria para prevenir el fraude y el hurto de servicio en situaciones en las que un malfuncionamiento o un cliente modificado no inicie los mensajes de señalización esperados. Es esencial que los mecanismos del protocolo sean robustos contra el abuso[2]. Un protocolo de coordinación de puerta garantiza que:

[2] En el apéndice IX se incluyen varios escenarios de hurto de servicio.

- Se evite el establecimiento de una sesión unidireccional sin que ésta sea facturada. Es posible que los clientes pretendan 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.
- Los recursos reservados y comprometidos por dos clientes son consistentes con el resultado de la negociación de capacidad. Si un único cliente paga por una sesión, es importante que los recursos reservados y utilizados sean consistentes con las expectativas de dicho cliente. La coordinación de puertas evita que el receptor de una sesión maliciosa defina características de sesión que produzcan un cargo inesperadamente elevado al originador de la misma.
- Las puertas se abren y se cierran virtualmente de forma simultánea (es decir, unos pocos cientos de milisegundos una tras otra). La coordinación de puerta garantiza la consistencia de los datos de facturación de ambos extremos de la sesión, de tal forma que el coste de la sesión no depende del extremo que paga por ella.

5.7.3 Cambio de los clasificadores de paquetes asociados a una puerta

Una vez que se han establecido un par de puertas, los clientes pueden comunicar a través de la red con una QoS mejorada. Algunas características de los servicios de comunicación vocal comerciales, implican cambiar los clientes que participan en una sesión, por ejemplo, cuando una sesión se transfiere o redirecciona durante una conferencia a tres. Ello requiere que los clasificadores de paquetes asociados con una puerta sean modificados para reflejar la dirección del nuevo cliente. Además, el cambio de los puntos extremos de una sesión puede afectar a la forma en que se factura 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 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 de fase, clasificadores) necesarios para describir los recursos. Los procedimientos exactos para comparar vectores de recursos *n*-dimensionales se incluye en UIT-T J.112.

Cuando se establece por vez primera una sesión, los protocolos QoS dinámica autorizan la utilización de una cantidad máxima de recursos, que viene indicada por el óvalo más externo, que especifica los recursos autorizados. Cuando un cliente hace una reserva durante una sesión, reserva una cierta cantidad de recursos, no superior a los que tiene autorizados. Cuando la sesión está lista para proceder, el cliente compromete una cierta cantidad de recursos, no superior a los recursos reservados. En muchos casos, los recursos comprometidos y reservados son los mismos. Los recursos comprometidos representan los que están siendo actualmente utilizados por la sesión activa, y los recursos reservados representan aquellos elegidos por el cliente y que fueron seleccionados para el control de admisión, pero que no están siendo necesariamente utilizados por el cliente.

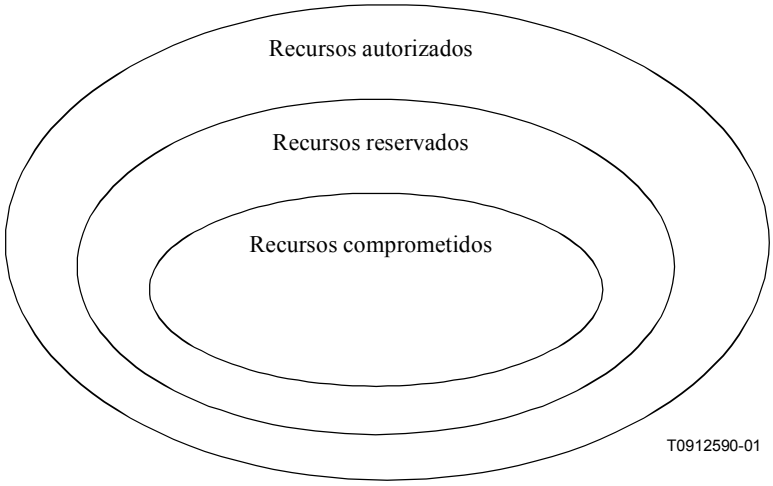


Figura 5/J.163 – Recursos autorizados, reservados y comprometidos

Las autorizaciones sólo afectan a futuras peticiones de reserva de recursos. 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, como por ejemplo ocurre en el manejo de datos en la modalidad de mejor esfuerzo. Estos recursos no están disponibles para otras reservas (es decir, no se permite la sobre suscripción). El máximo número de recursos que pueden ser reservados de una vez constituye una decisión de política por parte del AN y queda fuera del alcance de la QoS dinámica.

El exceso de recursos reservados por encima de los comprometidos se libera salvo que el cliente solicite de forma explícita que se mantengan mediante operaciones de refresco de reserva periódicas. Se recomienda que dicha situación no se mantenga durante largos periodos de tiempo, pues ello reduce la capacidad global del sistema. Sin embargo, existen situaciones (por ejemplo, el servicio de llamada en espera, en los que la llamada retenida requiere recursos adicionales a los de la llamada activa) en lo que son necesarias las reservas en exceso.

5.7.5 Control de admisión y clases de sesión

Está previsto que una puerta de un AN 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 pueda proporcionar los parámetros necesarios y/o las políticas de control de admisión alternativas en el AN y en el controlador de puerta. Por ejemplo, se podría definir una clase de sesión para comunicaciones de voz normales y una clase de sesión solapada para llamadas de emergencia a fin de permitir la atribución de hasta el 50% y el 70% respectivamente de los recursos totales a estas clases de llamada, dejando el restante 30-50% de la anchura de banda disponible para otros servicios de, probablemente, menor prioridad. Las clases de sesión pueden, además, permitir la interrupción o retirada de recursos que ya han sido reservados, en cuyo caso, es el proveedor de servicio quien define la política que gobierna dichas interrupciones. Cuando el controlador de puerta comunica a la puerta en el AN la envolvente autorizada mediante el mensaje establecimiento de puerta, el controlador 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 de sesión 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 envolvente autorizada y exista anchura de banda disponible en la red. La utilización de una envolvente autorizada de QoS que ha sido previamente autorizada por el controlador de puerta que actúa como punto de decisión de política 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. Esto significa, esencialmente, que la utilización de recursos hasta los límites de la envolvente queda autorizada previamente, pero NO pre-reservada. La asignación exitosa de recursos en el marco de la envolvente autorizada requiere una decisión del control de admisión, y no está garantizada. 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. Cada uno de los cambios que se produzcan en el compromiso de recursos dentro de los límites de la decisión de control de admisión, no requiere una ulterior reserva. Todas las peticiones de reserva que pasen el control de admisión DEBEN estar incluidas en la envolvente de autorizaciones.

5.7.7 Vinculación dinámica de recursos (re-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 que se identifiquen explícitamente un conjunto de recursos de la capa de red (tal como la reserva de anchura de banda), y permite que haya una o más puertas asociadas con dichos recursos. Las primitivas de señalización permiten que los recursos asociados con una puerta puedan *compartirse* con otra puerta del mismo AN. Ello mejora la eficiencia con la que se utilizan los recursos en la red J.112.

Cuando se conmuta alternativamente entre dos sesiones en un escenario de llamada en espera, un cliente necesita mantener en reserva suficientes recursos para cualquiera de las sesiones, las cuales, en general, no necesitarán la misma cantidad de recursos. Por lo tanto, la operación de recompromiso puede modificar los recursos comprometidos. Sin embargo, en este caso no se modifican los recursos reservados, pues el cliente no se ve de nuevo sometido al control de admisión cuando conmuta de una sesión a otra.

Si bien los recursos comprometidos están siempre asociados con la sesión activa en curso (y con su correspondiente flujo IP), los recursos reservados pueden estar vinculados a diferentes flujos y diferentes puertas en instantes distintos. Se utiliza un asa, denominada identificador de recurso, para identificar un conjunto de recursos reservados al objeto de vincular un flujo a dichos recursos.

5.7.8 Soporte de la facturación

La señalización de QoS puede utilizarse para soportar una amplia gama de modelos de facturación, exclusivamente en base al tren de registros de eventos procedente del AN. Debido a que la puerta se encuentra en el trayecto de los datos y que participa en las interacciones de la gestión de recursos con un cliente, es el elemento que contabiliza los recursos utilizados. La puerta en el AN es el lugar adecuado para realizar la contabilización de los recursos, ya que el AN está directamente implicado en la gestión de los recursos proporcionados a un cliente. También es importante contabilizar los recursos utilizados en el AN a fin de tener en cuenta los posibles fallos del cliente. Si un cliente que participa en una sesión falla, el AN DEBE detectarlo y detener la contabilización de la sesión. Esto

puede realizarse utilizando el estado blando mediante un mensaje de refresco de gestión de recursos (transmitiendo periódicamente mensajes RSVP-PATH durante una sesión activa), supervisando el flujo de paquetes en el trayecto de datos para aplicaciones de medios continuos o mediante cualquier otro mecanismo (tal como el mantenimiento de estación) que realice el AN. Además, y dado que la puerta mantiene el estado para flujos que han sido autorizados por un controlador de puerta específico del servicio, la puerta se utiliza para mantener información específica del servicio relacionada con la tasación, como por ejemplo, el número de cuenta del abonado que pagará la sesión. La función política que ejerce el controlador de puerta queda pues es una situación sin estado.

Es necesario que, con cada cambio de QoS, el AN genere y transmita un mensaje de evento a un servidor de mantenimiento de registros, tal 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 AN recibe un mensaje de reserva de recursos de un MTA, verifica en primer lugar que la anchura de banda adecuada, ascendente y descendente, se encuentra disponible en el canal de acceso utilizando información de planificación disponible a nivel local. Si esta verificación tiene éxito, el AN 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 AN puede establecer cualquier correspondencia entre la tecnología específica de la red troncal y la reserva de recursos necesaria. Ello permite que la arquitectura acomode diferentes tecnologías de la red troncal, a elección del proveedor de servicio. Los mecanismos específicos para la reserva de QoS en la red troncal queda fuera del alcance de esta Recomendación.

En la red J.112 se utiliza un modelo bidireccional para la reserva de recursos con encaminamiento simétrico. Se utiliza un modelo unidireccional para la reserva de recursos en la red troncal, que permite asimetrías en el encaminamiento. Por lo tanto, cuando el MTA_O realiza una reserva al AN, 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. Por lo tanto, cuando el MTA_O recibe la respuesta del MTA_T conoce los 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), en la que exista anchura de banda suficiente para el transporte de conversaciones vocales, pero en la que el acceso a dicha anchura de banda esté controlado. El acceso a la anchura de banda y el tratamiento diferenciado se realizan sobre la base de los paquetes que tienen la adecuada codificación de bits 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 campo DS mantiene la retrocompatibilidad con la utilización actual de los bits de precedencia IP del byte tipo de servicio (TOS) de IPv4 [IETF RFC 2474]. Es conveniente poder fijar el punto de código DiffServ de los paquetes que van a entrar a la red troncal del proveedor desde el AN. Dado que los recursos que dichos paquetes consuman en la red troncal dependen en gran medida de esta marca, esta arquitectura proporciona a las entidades de red el control de dicha marcación. Ello permite que sea el proveedor de red y de servicio quien controle la utilización de una QoS mejorada, en lugar de estar basado en la confianza depositada en el MTA. El proveedor puede establecer políticas en el AN que determinen como se debe fijar el DSCP en los flujos que pasan por el AN. Dichas políticas se envían al AN desde el CMS/GC 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. El RSVP realiza dicha transferencia mediante el objeto DCLASS propuesto por el IETF. El AN necesita aplicar la política a 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.

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

Para cumplir los requisitos previamente descritos, el RSVP y la arquitectura de servicios integrados de la RFC 2210 del IETF se utilizan como bases del mecanismo de señalización para el aprovisionamiento de la QoS local. La versión de la especificación actual del RSVP, debe ser mejorada a fin de cumplir los requisitos de la arquitectura de QoS dinámica.

El RSVP y la arquitectura de servicios integrados especifica los parámetros de QoS en términos genéricos independientes de la tecnología de la capa 2 subyacente. Es necesario especificar una forma establecer la correspondencia entre las especificaciones de tráfico generales y las especificaciones 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 depende de mensajes de gestión de recursos que se transmitan de extremo a extremo.
- El intercambio relativo a la gestión de recursos entre el MAT y el AN reserva recursos en ambos sentidos en la red de área local (es decir, operada por el cliente) y en las redes J.112. Ello permite que un AN actúe como representante (o *proxy*) del punto extremo distante, con el consiguiente beneficio pues se minimiza el número de mensajes necesarios para la gestión de recursos en las redes J.112 de anchura de banda limitada, reduciendo el retardo posterior a la marcación y al descolgado.
- La posible existencia de encaminadores RSVP en la parte de área local de la red (es decir, la operada por el cliente). En este entorno es necesario poder realizar 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 para vincular un único conjunto de recursos a un grupo de varias reservas, en base a la información del MTA de que en cada instante sólo estará activa una de las reservas del grupo.
- El soporte de la activación de recursos en dos fases disponibles 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 AN realiza la primera fase, el control de admisión, enviando el MTA al AN un mensaje separado para que se realice la activación.

La operación de la calidad de servicio dinámica no hace referencia al RSVP normalizado, que puede o no estar soportado. Independientemente de ello, los mensajes RSVP normalizados no producen la activación o disparo de las operaciones de QoS dinámica que se especifican en esta Recomendación.

6.1 Visión general de las extensiones de RSVP

6.1.1 Operación segmentada

Tal como se define en la RFC 2205 del IETF, el RSVP está diseñado para ser ejecutado entre dos computadoras 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 AN. En esta cláusula se ilustra como el RSVP puede soportar un modelo segmentado.

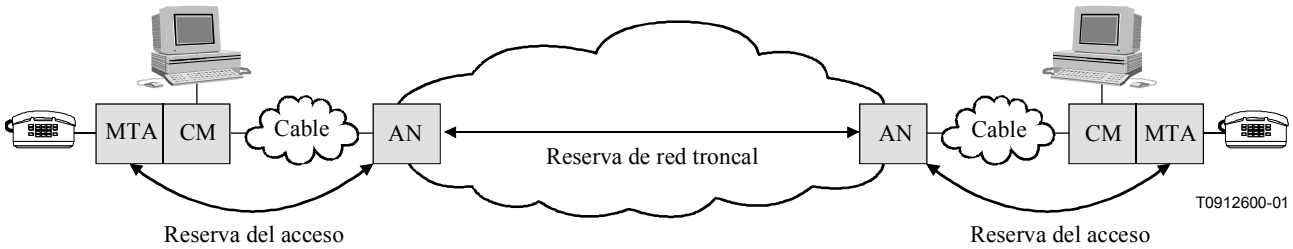


Figura 6/J.163 – Modelo de señalización segmentada

En el modelo segmentado, un MTA se comunica con el AN. Además del escenario sencillo que se muestra en la figura 6, esta Recomendación permite escenarios más complejos, tales como los que se producen cuando hay 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 AN 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 AN 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. Ello minimiza los cambios 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 fluyen en el mismo sentido que los datos y los mensajes RESV lo hacen en sentido opuesto. Para realizar una reserva bidireccional, es necesario añadir nuevos objetos RSVP para definir ambos sentidos. El AN 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 AN inicia un mensaje PATH que tiene la apariencia de que procede del cliente distante.

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

Si el AN 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 necesita hacer saber al AN que la compresión o supresión puede aplicarse 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 [draft-davie-intserv-compress-02].

El MTA añade el parámetro indicación de compresión (*Compression_Hint*) que se describe en [draft-davie-intserv-compress-02] a la Tspec de emisor que identifica el tipo o tipos de compresión o supresión de cabecera que pueden aplicarse a los datos. El parámetro indicación de compresión contiene una campo indicación que advierte sobre cuál es el tipo o los tipos de compresión o

supresión posibles, así como si el usuario utiliza sumas de control UDP o IP y/o IP-Ident (identificación IP); si éstos no se utilizan, dichos campos pueden también estar comprimidos o suprimidos. Si un campo de la cabecera IP no se comprime o se suprime, la suma de control IP NO DEBE suprimirse ni comprimirse.

Para señalizar a la red J.112 la supresión de la cabecera, el AN utiliza los datos que proporciona el campo indicación del parámetro indicación 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 tamaño del contador de testigo del MTA. Si un enlace no soporta la supresión de cabecera, se ignora el parámetro indicación de compresión y se utiliza la especificación completa Tspec.

Cuando se suprime la cabecera en un enlace J.112, es asimismo necesario comunicar al AN el *contenido* de la 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 AN. 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. Debido a que los mensajes PATH se procesan en todos los tramos intermedios entre el cliente y el AN, un mensaje PATH entrante tendrá el mismo valor de TTL que 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 AN puede utilizar el contenido de PATH para conocer los valores de los campos que serán suprimidos. El AN utiliza mensajes MAC J.112 para indicar al CM que la supresión debería afectar a un flujo en particular y ordena la supresión de los campos pertinentes dada la presencia o ausencia de las sumas de control UDP.

El AN puede asimismo ordenar al CM la supresión del campo identificación IP. Este campo sólo se utiliza cuando se realiza la fragmentación. Dado que este campo cambia con cada paquete, su valor no puede transportarse utilizando RSVP ni mensajes MAC. Su supresión o no supresión depende de si el paquete puede ser ulteriormente fragmentado. No es necesario que el MTA envíe al AN información alguna sobre la supresión de este campo; el AN 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 AN puede utilizar distintos algoritmos de programación para flujos que utilicen VAD y, por tanto, necesita saber qué flujo puede ser tratado con VAD. El objeto de compresibilidad transportado en Tspec DEBE contener un valor que indica que el flujo de datos para el que se solicita esta reserva puede ser tratado con VAD (es decir, aún no ha realizado la detección de silencio en el MTA, se trata de voz, no facsímil ni tampoco datos).

6.1.4 Vinculación dinámica de recursos

El modelo de QoS dinámica exige poder modificar dinámicamente la vinculación entre recursos y flujos. Por ejemplo, para la llamada en espera puede ser deseable retener suficientes recursos para una única sesión en la red J.112, transfiriendo la asignación de tales recursos de un llamante a otro. Si bien esta capacidad ha sido sugerida para el protocolo RSVP, no se incluyó en la versión 1 del mismo.

En RSVP, el "asa" para un conjunto de recursos reservados es el objeto sesión. Dado que la sesión contiene la dirección de destino del flujo, la reasignación de recursos a un flujo con una dirección de destino distinta requeriría un cambio en el objeto sesión. El cambio de la dirección de fuente del flujo puede realizarse mediante una nueva especificación de filtro en el mensaje RESV.

Para acomodar esta funcionalidad, se añade el objeto identificador de recurso 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, es decir, en este caso el AN.

Esto se ilustra en la figura 7. Cuando un MTA emite una petición de reserva para un nuevo flujo, indica al AN que esta sesión está dispuesta a compartir recursos para esta nueva puerta (puerta 2) con una puerta que haya sido creada anteriormente (puerta 1), incluyendo en la petición el ID de recurso. 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 que tome la nueva sesión. El acceso a la reserva compartida ocurre de forma mutuamente excluyente: un MTA debe emitir un mensaje de compromiso para indicar al AN 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 AN para identificar el flujo actualmente activo cuando el usuario pasa de una sesión a otra.

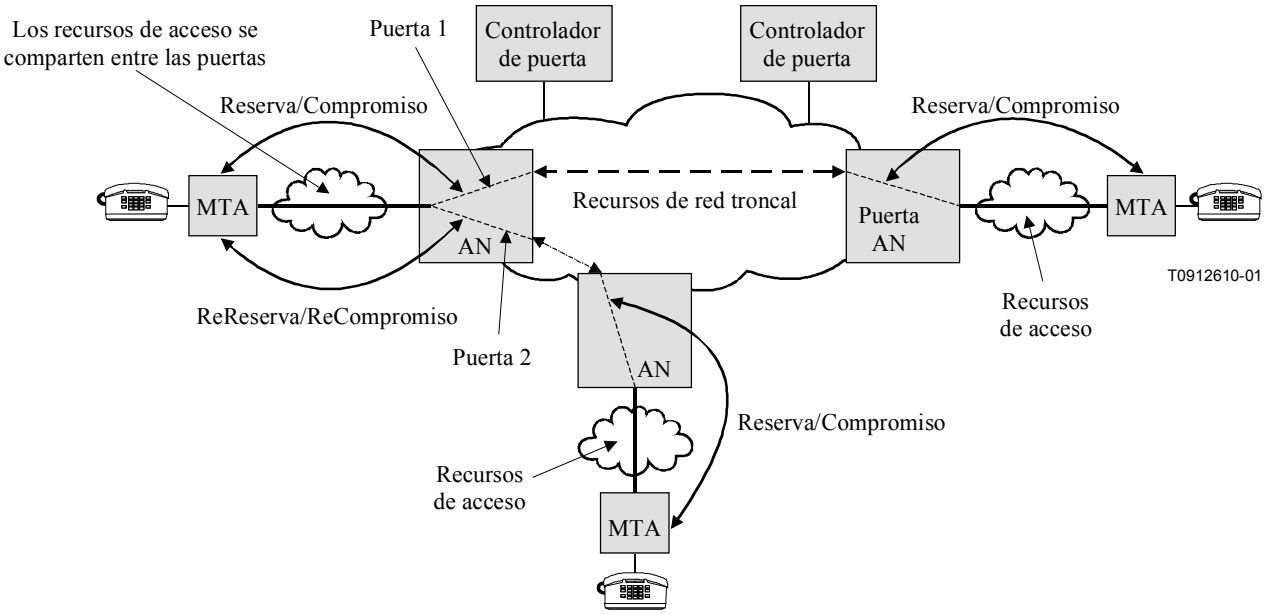


Figura 7/J.163 – Compartición de las reservas de recursos entre puertas

En el modelo segmentado, el AN incluye el ID de recurso en el primer mensaje RESV que envía al MTA. El MTA puede incluir el ID de recurso en subsiguientes mensajes que hagan referencia a los recursos en cuestión. Aún más importante, si el MTA desea establecer una nueva sesión y reutilizar los recursos de una sesión existente, incluye en el mensaje PATH el ID de recurso asociado con la sesión anterior y lo envía al AN. Un mensaje PATH que contenga el ID de recurso de un conjunto actualmente asignado de recursos, añade una nueva vinculación entre un flujo (tal como se identifica 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 AN para este conjunto de recursos. Ello incluye la posible adición de un nuevo conjunto de Tspec y de Rspec para incluir múltiples códecs tal como se describe en la cláusula 6.2.

El RSVP permite que la magnitud de las reservas varíe 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 DEBE fracasar 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 DEBE fracasar en el control de admisión.

Un encaminador que no pueda interpretar este nuevo objeto (por ejemplo, en la red de cliente), intentará simplemente instalar lo que parece ser una nueva reserva sin reutilizar recursos previamente atribuidos. Dado que no es probable que la anchura de banda disponible en la red originaria local sea menor que la disponible en la red J.112, tampoco es probable que ello constituya un problema. La reserva anterior expira si no se refresca. Si la carencia de recursos se convierte en un problema en la red del cliente, es necesario actualizar los encaminadores en la red originaria para que soporte este nuevo objeto. Nótese que siempre merece la pena 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 de fase excesivas 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 dinámico de IPCablecom es que la reserva constituye un proceso en dos fases, una fase de reserva seguida de una fase de compromiso. El protocolo RSVP se utiliza para la fase de reserva, de forma que el AN no proporciona realmente los recursos hasta la segunda etapa del proceso.

Debido a que en la fase de compromiso sólo participa un MTA y una puerta local, se compone de un mensaje unidifusión desde el MTA al AN. 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 los datos de política incluidos en otros mensajes RSVP. La especificación de QoS dinámica incluye un ID de puerta como parte de los datos de la política, que DEBE estar incluido en los mensajes RSVP-PATH.

6.2 Especificaciones de flujo de RSVP

La arquitectura de servicios integrados del IETF utiliza descripciones de propósito general (independientes de la capa 2) de las características del tráfico y de los requisitos de recursos de un flujo. La descripción del tráfico se conoce como Tspec, los requisitos de los recursos se incluyen en una Rspec y la combinación de ambos se denomina especificación de flujos (*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 CODEC IPCablecom J.167) figuran los requisitos de la correspondencia que debe establecerse entre descripciones de alto nivel (por ejemplo, SDP utilizado en aplicaciones de VoIP) y las especificaciones de flujo. En los anexos A y B se especifica cómo el AN y el MTA deben establecer las correspondencias entre especificaciones de flujo y parámetros de capa 2 J.112.

La modalidad de servicios integrados (*IntServ*) define actualmente dos tipos de servicios, de carga controlada y garantizado, siendo este último el más adecuado para aplicaciones sensibles al retardo. Cuando se hace una reserva para servicios garantizados, la especificación de flujo 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

unidad mínima sujeta a la política (m) – bytes

tamaño máximo del datagrama (M) – bytes

Rspec (especificación de recursos)

tasa reservada (R) – bytes/segundo

término de inactividad (S) – microsegundos

Los términos de las Tspec son en su mayoría autoexplicativos. 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 la cabeceras IP y de orden superior) que genera la fuente. La unidad mínima supervisada, m, es normalmente el menor tamaño de paquete que genera la fuente; si éste emite un paquete más pequeño, se considerará un paquete de tamaño m a los efectos de aplicación de la política.

A fin de entender cabalmente la Rspec, es útil comprender 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 anteriormente definidos, y C_{tot} y D_{tot} son "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. DEBE ser mayor o igual que el valor "r" de Tspec a fin de 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 en el retardo que experimenta el flujo.

Debido a que no está permitido que $R < r$, un nodo que haga una reserva puede realizar el cálculo anterior y determinar que el límite del retardo es más estricto de lo necesario. En tal caso, el nodo puede hacer $R = r$ y que S tome 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 de fase más de lo que se desprende del límite del retardo. En general, el retardo mínimo que puede experimentar un paquete es el de la velocidad de la luz, y el máximo es el límite antes identificado; la fluctuación de fase máxima es la diferencia entre ambos. Por lo tanto, la fluctuación de fase puede controlarse mediante una selección adecuada de R y S.

Existen diversas situaciones en las que una reserva debe cubrir una gama de posibles especificaciones de flujo. Por ejemplo, para algunas aplicaciones resulta recomendable 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.

En casos como este, el MTA DEBE generar múltiples Tspec. Las Tspec segunda y posteriores DEBEN marcarse como Tspec componentes (véase 6.3.6) y contener los parámetros de la especificación de flujo de un códec individual. La primera Tspec DEBE formarse, para cada uno de los componentes de la descripción de flujo, tomando la máxima utilización de recursos de cualquiera de las Tspec componentes siguientes. A ello se denomina límite mínimo superior (LUB, *least-upper-*

bound). Mediante el LUB incluido en una Tspec RSVP normalizado, cualquier encaminador que no esté familiarizado con estas extensiones atribuirá recursos suficientes (y posiblemente más que suficientes) para transportar cualquiera de las alternativas.

Si sólo se toma el LUB de dos especificaciones de flujo, se produce cierta pérdida de información. Por ejemplo, supóngase que el códec A es G.726-24 con paquetes de 20 ms, lo cual requiere que Tspec sea:

dimensión del contador (b) = 100 bytes

tasa del contador (r) = 5000 bytes/segundo

tasa de cresta (p) = 5000 bytes/segundo

unidad mínima sujeta a la política (m) = 100 bytes

tamaño máximo del datagrama (M) = 100 bytes

mientras que el códec B es G.726-40 con paquetes de 10 ms, lo cual requiere que Tspec sea:

dimensión del contador (b) = 90 bytes

tasa del contador (r) = 9000 bytes/segundo

tasa de cresta (p) = 9000 bytes/segundo

unidad mínima sujeta a la política (m) = 90 bytes

tamaño máximo del datagrama (M) = 90 bytes

Analizando el códec A, se concluye que es necesario una concesión para el transporte paquetes IP de un tamaño de 100 bytes cada 20 ms (M/r = 0,2 s), mientras que el códec B requiere una concesión para la distribución de paquetes de 90 bytes cada 10 ms. Sin embargo, el LUB de las dos Tspec es:

dimensión del contador (b) = 100 bytes

tasa del contador (r) = 9000 bytes/segundo

tasa de cresta (p) = 9000 bytes/segundo

unidad mínima sujeta a la política (m) = 100 bytes

tamaño máximo del datagrama (M) =100 bytes

con lo cual se dispone de una concesión para 100 bytes cada 11,1 ms (M/r = 100/9), cifra que no resulta adecuada para ninguna de las sesiones. Por este motivo, cuando se realiza la reserva es necesario abarcar dos o más especificaciones de flujo distintas, cada componente de la especificación de flujo DEBE estar incluido en los mensajes RSVP adecuados.

6.3 Definición de objetos RSVP adicionales

Se deben 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 fijados, de forma 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 inversa (Reverse Rspec)

Objeto Rspec inversa: Clase = 226, Tipo C = 1.

130 (h)	0 (i)	2 (j)
Velocidad [R] (número en coma flotante IEEE de 32 bits)		
Término de inactividad [S, *slack*] (entero de 32 bits)		

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

(i) – Banderas del parámetro 130 (ninguna fijada).

(j) – Longitud del parámetro 130, 2 palabras, sin incluir la cabecera del parámetro.

Véase en la RFC 2210 del IETF la explicación de los campos.

La Rspec inversa se aplica a los datos que envía el MTA, es decir, datos ascendentes en la red J.112. Está incluido en el mensaje PATH que envía el MTA, y se convierte en el objeto Rspec directa del mensaje RESV que genera el AN en su cometido de representación del punto extremo distante.

6.3.2 Sesión inversa (Reverse-Session)

Objeto sesión inversa IPv4: Clase = 226, Tipo C = 2.

Dirección IPv4 de destino (4 bytes)		
ID de protocolo	Banderas	Puerto destino

El objeto sesión inversa IPv4 describe la información de destino del tren de datos que debe recibir el MTA, es decir, en sentido descendente en la red J.112 y se convierte en el objeto de sesión del mensaje PATH que genera el AN en su cometido de representación del punto extremo distante.

6.3.3 Plantilla de emisor inversa (Reverse-Sender-Template)

Objeto plantilla de emisor inversa IPv4: Clase = 226, Tipo C = 3.

Dirección de fuente IPv4 (4 bytes)		
Reservado	Reservado	Puerto origen

El objeto plantilla de emisor inversa IPv4 describe la información de fuente del tren de datos que debe recibir el MTA, es decir, descendente en la red J.112. Se convierte en el objeto plantilla de emisor del mensaje PATH que genera el AN en su cometido de representación del punto extremo distante.

6.3.4 Tspec de emisor inversa (Reverse-Sender-Tspec)

Objeto Tspec de emisor inversa: Clase = 226, Tipo C = 4. Son los mismos campos que en Tspec de emisor que sed escribe en la modalidad de servicios integrados en presencia de flujos comprimibles [draft-davie-intserv-compress-02].

0 (a) ¦ Reservado		10 (b)
1 (c)	0¦ Reservado	9 (d)
127 (e)	0 (f)	5 (g)
Tasa del contador de testigos [r] (número en coma flotante de 32 bits del IEEE)		
Tamaño del contador de testigos [b] (número en coma flotante de 32 bits del IEEE)		
Velocidad de cresta de datos [p] (número en coma flotante de 32 bits del IEEE)		
Unidad mínima sujeta a la política [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, 9 palabras sin incluir la cabecera.

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

(f) – Banderas del parámetro 127 (ninguna fijada).

(g) – Longitud de parámetro 127, 5 palabras sin incluir la cabecera.

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

(i) – Banderas del parámetro 126 (ninguna fijada).

(j) – Longitud del parámetro 126, 2 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 Y no suprimir el campo identificación IP ni el campo suma de control IP.

0x????0002 No suprimir el control de suma de 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 suprimir los campos identificación IP y suma de control IP

NOTA – ???? – (Por determinar) Asignación de numeración del IANA para IP Cablecom.

(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 CODEC utilizado. Véase en RFC 2210 del IETF la explicación relativa a los campos.

El objeto Tspec de emisor inversa describe el flujo de datos que debe enviar el MTA, es decir, ascendente en la red J.112. Se convierte en el objeto Tspec de emisor en el mensaje PATH generado por el AN en su cometido de representación del punto extremo restante.

6.3.5 Rspec directa (Forward-Rspec)

Objeto Rspec directa, Clase = 226, Tipo C = 5. Los mismos campos que Rspec inversa.

130 (h)	0 (i)	2 (j)
Tasa [R] (punto en coma flotante de 32 bits del IEEE.		
Término de inactividad [S] (entero de 32 bits)		

La Rspec directa se aplica a los datos que fluyen hacia el MTA, es decir, descendentes en la red J.112. Este objeto aparece en el mensaje PATH que envía el MTA, y los contenidos se incorporan en el objeto especificación de flujo del mensaje RESV devuelto.

6.3.6 Tspec componente (Component-Tspec)

Objeto Tspec componente: Clase = 226, Tipo C = 6. Son los mismos campos que TSpec de emisor definidos para el caso de servicios integrados (*IntServ*) en presencia de flujos comprimibles [draft-davie-intserv-compress-02]

0 (a) ¦ Reservado		10 (b)
1 (c)	0¦ Reservado	9 (d)
127 (e)	0 (f)	5 (g)
Tasa del contador de testigos [r] (número en coma flotante de 32 bits del IEEE)		
Tamaño del contador de testigos [b] (número en coma flotante de 32 bits del IEEE)		
Velocidad de cresta de datos [p] (número en coma flotante de 32 bits del IEEE)		
Unidad mínima sujeta a la política [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, 9 palabras sin incluir la cabecera.

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

(f) – Banderas del parámetro 127 (ninguna fijada).

(g) – Longitud de parámetro 127, 5 palabras sin incluir la cabecera.

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

(i) – Banderas del parámetro 126 (ninguna fijada).

(j) – Longitud del parámetro 126, 2 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 Y no suprimir el campo identificación IP (IP-Ident) ni el campo suma de control IP (IP-Checksum).

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 – ???? – (Por determinar) Asignación de numeración del IANA al IP Cablecom.

(l) – Valor del facto 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 CODEC utilizado.

6.3.7 Identificador de recurso (Resource-ID)

Objeto identificador de recurso: 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 utilizado para ulteriores cambios de recursos. También se incluye en los mensajes PATH enviados por el MTA para solicitar la compartición de recursos entre varias sesiones.

6.3.8 Identificador de puerta (Gate-ID)

Objeto identificador de puerta: Clase = 226, Tipo C = 8.

ID de puerta (entero de 32 bits)

El objeto ID de puerta incluido en los mensajes PATH del MTA para identificar la autorización del recurso adecuado en el AN.

6.3.9 Entidad compromiso (Commit-Entity)

Objeto entidad compromiso IPv4: Clase = 226, Tipo C = 9.

Dirección de destino IPv4 (4 bytes)	
Reservado	Puerto de destino

El objeto entidad compromiso se devuelve en un mensaje RESV desde el AN, e indica la dirección de destino y el número de puerto al que el MTA debe enviar el mensaje COMMIT.

6.3.10 Clase D (DClass)

Objeto Clase D: Clase = 225, Tipo C = 1.

No utilizado	No utilizado	No utilizado	DSCP

El objeto Clase D se devuelve en un mensaje RESV procedente del AN, e indica el DSCP que DEBERÍA utilizar el MTA cuando envíe al AN paquetes de datos en relación con esta reserva. La utilización del objeto Clase D se describe en el documento utilización y formato del objeto DCLASS con señalización RSVP [draft-bernet-dclass-01].

6.4 Definición de mensajes RSVP

En esta cláusula se definen los mensajes RSVP mejorados que DEBE generar el MTA y que DEBE soportar el AN.

Los mensajes RSVP DEBEN enviarse como datagramas IP "en bruto" con número de protocolo 46. El mensaje RSVP-PATH DEBE enviarse con la opción alerta del encaminador RFC 2113 del IETF en la cabecera IP. Cada mensaje RSVP DEBE ocupar exactamente un datagrama IP.

Todos los mensajes RSVP DEBEN constar de una cabecera común, seguida de un número variable de objetos de longitud variable. La cabecera común DEBE ser la siguiente:

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

Los valores de cada campo DEBEN ser conforme a lo especificado en la RFC 2205 del IETF.

Cada objeto DEBE constar de 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 DEBEN ser según se especifica en la RFC 2205 del IETF.

El formato del mensaje RSVP-PATH y del mensaje RSVP-RESV conformes con esta Recomendación DEBEN contener los objetos siguientes (los elementos en cursiva se definen en esta Recomendación, los restantes en la RFC 2205 y/o RFC 2210 del IETF). En el caso de los objetos que no se definen en esta Recomendación, DEBEN seguirse las reglas de ordenación de objetos de la RFC 2205 del IETF. No existen requisitos de ordenación para los objetos <Resource-ID>, <Gate-ID>, y <Commit-Entity>. Además, <Reverse-Rspec> y <Downstream-Flowspec> DEBEN seguir al objeto <Sender-Tspec>. Si <Component-Item> se incluye en el mensaje, <Component-Item> DEBE aparecer en el mensaje PATH después de la tripleta <Sender-Tspec><Reverse-Rspec><Downstream-Flowspec>. Los objetos definidos en <Downstream-Flowspec> y <Component-Item> DEBEN seguir el orden que se muestra en su BNF siguiente:

<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> [<*Component-Item*> …]

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

<*Component-Item*> *::=* <*Component-Tspec*> <*Reverse-Rspec*>
<*Downstream-Flowspec*>

<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 del mensaje para reserva ascendente

Un mensaje RSVP-PATH (trayecto RSVP) normalizado contiene, como mínimo, los objetos siguientes:

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

Sin embargo, en el modelo segmentado es necesario entregar al AN toda la información que le permita realizar una reserva bidireccional en el enlace J.112. También es necesario permitirle enviar al MTA un mensaje RSVP-RESV (reserva RSVP). Un mensaje RSVP-RESV normalizado contiene, como mínimo, los objetos siguientes:

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

El AN DEBE generar dicho mensaje hacia el MTA después de recibir un mensaje RSVP-PATH del MTA. El único objeto que no puede obtenerse a partir de RSVP-PATH o de información local es la especificación de flujo. El objeto especificación de filtro, que consta de la dirección IP y el puerto de fuente que debe utilizar el MTA, se obtiene de plantilla de emisor del mensaje PATH. Casi todo lo contenido en la especificación de flujo puede derivarse de la Tspec de emisor del mensaje PATH. Las excepciones son los valores 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 tal como se indica en la RFC 2210 del IETF. Está incluida en el objeto Rspec inversa, descrito en 6.3.2.

6.4.2 Objetos del mensaje para reserva descendente

El MTA DEBE proporcionar suficiente información para permitir que el AN construya un mensaje RSVP-PATH para el flujo de datos descendente habiendo recibido solamente 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 (AN->MTA).

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

Estos objetos tienen sus definiciones RSVP normales, y se aplican al tren de datos símplex que fluye desde el punto extremo distante hasta el MTA. En el mensaje RSVP-PATH que envía el MTA, se les asignan nuevos códigos de objetos (tal como se ha señalado anteriormente) y nuevos nombres sesión inversa, plantilla de emisor inversa, Tspec de emisor inversa). El objeto sesión inversa DEBE contener la dirección IP del MTA, el tipo de protocolo y el puerto (si se aplica) sobre el que recibe los datos de este flujo. La plantilla de emisor inversa DEBE contener la dirección IP del punto extremo distante, o bien, todos ceros si se desea que la fuente sea una elección libre. La plantilla de emisor inversa DEBE contener el número de puerto, si se aplica y se conoce, o en otro caso ser cero. La Tspec de emisor inversa DEBE contener la información TSpec que describe el flujo de datos desde el punto extremo distante. El AN DEBE utilizar su propia dirección como valor de tramo RSVP y elegir un valor para el campo valores de tiempo que indique la frecuencia con la que refrescará el mensaje RSVP-PATH. Aunque el AN no necesite generar el mensaje RSVP-PATH para enviarlo al MTA, esa información es necesaria a fin de que pueda realizar una reserva y crear clasificadores de paquetes en el sentido descendente.

Una vez dada la información anterior, la única información adicional que el AN requiere para realizar la reserva en el sentido descendente es Rspec. De nuevo, se le asigna un nuevo objeto y un nombre, Rspec directa. Contiene los mismos elementos de información y se codifica de la misma forma que una Rspec convencional.

Nótese que Rspec directa se aplica a los datos que fluyen hacia el MTA, lo cual significa que lo envía el MTA en el mismo sentido en que se envía el 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 un Rspec inversa en el sentido opuesto al RSVP-RESV que normalmente transportaría esta información.

6.4.3 Objetos de mensaje para soportar múltiples especificaciones de flujo

En el caso de múltiples códecs que se describe en 6.2, puede ser necesario un mensaje PATH para transportar múltiples Tspec y Rspec. Al mismo tiempo, los dispositivos RSVP situados entre el MTA y el AN necesitan recibir las Tspec y Rspec que constituyen el límite mínimo superior (LUB). Por tanto, cuando los recursos se reservan para incluir múltiples códecs, un objeto Tspec o Rspec normalizado transportado en un mensaje RSVP debería incluir el LUB de los recursos requeridos. Pueden incluirse Tspec y Rspec adicionales en el mensaje PATH, utilizando nuevos tipos de objetos que serán ignorados por los dispositivos RSVP normalizados. Dado que todos los objetos que describen la especificación de flujo descendente y la Rspec inversa son ignorados por el RSVP normalizado, el único objeto necesario es un objeto Tspec componente que PUEDE ser transportado en el mensaje RSVP-PATH. En un mensaje RSVP-PATH pueden existir dos o más de dichos

objetos, además de la Tspec normalizada requerida para transportar el LUB de todos los componentes y que utilizarán los dispositivos de la red del cliente. La interpretación de cada objeto Tspec componente es que los recursos reservados en el enlace J.112 son los adecuados para acomodar cualquier flujo que concuerde con uno de dichas Tspec.

Asimismo, PUEDEN existir múltiples objetos Rspec inversas, sesión inversa, plantilla de emisor inversa, Tspec de emisor inversa y Rspec directas. Dado que es necesario poder identificar correctamente la combinación de parámetros en los sentidos directo e inverso que debe acomodarse en un instante dado, es importante el orden en que tales objetos se encuentran en el mensaje RSVP-PATH. Se REQUIERE utilizar el orden que se presenta en 6.4 anterior.

6.5 Funcionamiento del procedimiento de reserva

En esta cláusula se describe el comportamiento que deben tener el MTA y el AN para realizar de forma cooperativa la reserva de recursos.

Para los fines de este análisis, el punto extremo que se encuentra en comunicación directa con el AN se denomina cliente, y el otro punto extremo de la sesión se denomina punto extremo distante. No se hacen hipótesis sobre los tipos de dispositivos de que realmente se trata (pasarelas, PC, clientes integrados). Se supone que el cliente utiliza RSVP para comunicar sus peticiones de QoS al AN, y tampoco se hacen hipótesis sobre las capacidades del punto extremo distante. El flujo de datos desde el cliente al AN se denomina ascendente y al flujo de datos desde el AN al cliente, descendente.

6.5.1 Establecimiento de la reserva

En el caso del modelo segmentado, la operación del RSVP es la siguiente:

El cliente DEBE enviar un mensaje RSVP-PATH hacia el punto extremo distante de la sesión, que DEBE ser interceptado por el AN. Éste 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 DEBE transportar información sobre los requisitos sobre recursos ascendentes (es decir, Rspec inversa) y descendente (es decir, Tspec de emisor inversa, Rspec directa).

El AN DEBE verificar que la cantidad de recursos solicitados está dentro de los límites autorizados para la sesión, y que dispone de suficientes recursos locales para la reserva. Realiza entonces la reserva de los recursos ascendentes y descendentes y DEBE emitir los mensajes de nivel MAC J.112 para la asignación de los recursos adecuados en el enlace J.112.

El AN DEBE establecer clasificadores para los flujos ascendente y descendente. El clasificador ascendente DEBE contener la dirección IP de fuente del cliente y el número de puerto del objeto plantilla de emisor. El clasificador ascendente DEBE contener el tipo de protocolo, la dirección IP de destino y el número de puerto del objeto sesión. Si el objeto plantilla de emisor inversa está presente y contiene una dirección distinta a 0.0.0.0, el clasificador descendente DEBE incluir esta dirección como la dirección IP de fuente. Si la plantilla de emisor inversa está presente, y contiene un número de puerto distinto a 0, el clasificador descendente DEBE incluir dicho valor como puerto de fuente. El clasificador descendente DEBE contener el tipo de protocolo, la dirección IP de destino y el número de puerto del objeto sesión inversa.

El AN DEBE hacer las reservas de recursos necesarias de red troncal en base al algoritmo definido para la configuración de la red troncal específica.

Si las reservas a nivel de acceso y nivel troncal tienen éxito, el AN DEBE enviar al cliente un mensaje RSVP-RESV. El contenido de RSVP-RESV DEBE derivarse de RSVP-PATH: el objeto sesión se copia de RSVP-PATH, el estilo toma el valor filtro fijado, la especificación de flujo se constituye a partir de Tspec de emisor y Rspec directa, la especificación de filtro toma su valor a partir de la plantilla de emisor, y se genera el ID de recurso que incluye el ID de recurso asignado a los recursos. El objeto entidad compromiso DEBE estar incluido y debe contener la dirección del AN y el número de puerto sobre el que el AN aceptará el mensaje COMMIT (tal como se describe

en 6.6). El objeto DCLASS DEBERÍA estar incluido y su valor fijado 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 AN DEBE generar un RSVP-PATH para reservas en sentido descendente. El contenido de RSVP-PATH DEBE obtenerse del RSVP-PATH recibido del cliente. El objeto sesión DEBE obtenerse del objeto sesión inversa del mensaje RSVP-PATH. Si la dirección contenida en la plantilla de emisor inversa es 0.0.0.0, o el número de puerto es 0, en el RSVP-PATH no se envía ni Tspec de emisor ni plantilla de emisor. Si no es así, la Tspec de emisor se obtiene de la Tspec de emisor inversa, la Rspec directa se obtiene de la Rspec inversa y la plantilla de emisor se obtiene de la plantilla de emisor inversa. Se genera entonces el objeto ID de recurso que contiene el ID de recurso de los recursos asignados. El MTA PUEDE utilizar la Tspec de emisor inversa que envió 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*). Cuando se recibe el mensaje RSVP-RESV, el cliente conoce que se han reservado los recursos necesarios. Si la reserva ha tenido éxito, el cliente sabe en ese momento que dispone de una reserva en ambos sentidos, y puede proceder a enviar la señal de llamada al teléfono en el extremo distante mediante señalización de llamada.

Si la reserva no ha tenido éxito, el AN DEBE enviar al cliente un mensaje RSVP-PATH-ERR, indicando porqué ha fracasado la reserva (por ejemplo, falta de autorización, recursos insuficientes, etc.). Si la causa del fracaso de la reserva es la política, el mensaje RSVP-PATH-ERR DEBE contener un objeto RSVP-ERROR-SPEC con los códigos de error y valores de error siguientes:

- Si RSVP-PATH no contiene el objeto ID de puerta o bien, éste no concuerda con ninguna de las puertas que conoce el AN, se devuelve código de error = 2 (fallo de control de la política) y valor de error = 3 (rechazo genérico de la política).
- En caso de rechazo de RSVP-PATH debido a la no existencia de recursos adicionales para el nivel de prioridad de la puerta, se devuelve el código de error = 1 (fallo del control de admisión) y el valor de error = 2 (anchura de banda solicitada no disponible). En esos casos, el MTA PUEDE tomar una acción especial indicando al usuario el error específico. Si RSVP-PATH falla por razones ajenas a la política, DEBE contener un objeto RSVP-ERROR-SPEC con un código de error y un valor de error definidos en el apéndice B de la RFC 2205 del IETF

El emisor de un RSVP-PATH (MTA o AN) es responsable de instalar la reserva de modo fiable. Cuando el emisor transmite un RSVP-PATH, DEBE recibir un mensaje RSVP-RESV o RSVP-PATH-ERR dentro del intervalo de temporización configurado del temporizador T3 (véase el anexo C).

Cuando un MTA o un AN transmite un mensaje RSVP que requiere acuse de recibo, el emisor DEBE incluir un objeto RSVP-MESSAGE-ID en dicho mensaje, y la bandera acuse de recibo deseado (*ACK_Desired*) del objeto RSVP-MESSAGE-ID DEBE fijarse. El MTA y el AN DEBEN fijar la bandera capacitado para reducción del refresco, en la cabecera común de cada mensaje RSVP. Cuando el MTA o el AN recibe un mensaje RSVP con un objeto RSVP-MESSAGE-ID, DEBE 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 normalizados, 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, el AN NO DEBERÍA retardar el procesamiento de un mensaje RSVP-PATH recibido, pero si decide introducir un retardo, DEBE responder inmediatamente con un mensaje RSVP-ACK, posteriormente seguido de un mensaje RSVP-RESV.

Los mensajes RSVP-ACK transportan uno o más objetos RSVP-MESSAGE-(N)ACK. NO DEBEN contener ningún otro objeto RSVP a excepción de un objeto facultativo RSVP-INTEGRITY. Cuando se incluye, un objeto RSVP-MESSAGE-(N)ACK, DEBE ser el primer objeto del mensaje,

salvo que esté presente un objeto RSVP-INTEGRITY (en cuyo caso, el objeto RSVP-MESSAGE-(N)ACK DEBE ir inmediatamente después del objeto RSVP-INTEGRITY). El AN 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 AN fijan la bandera ACK_Desired, los mensajes sin acuse de recibo DEBEN retransmitirse a intervalos más breves que el intervalo de refresco RSVP normalizado hasta que se acuse recibo del mensaje o hasta que venza el temporizador T3 (véase el anexo C). DEBE utilizarse una velocidad de retransmisión basada en funciones de reducción bien conocidas. DEBE utilizarse un valor de expiración inicial de la retransmisión para el temporizador T6 (véase el anexo C), con una reducción que sea potencia de 2. El proceso de retransmisión rápido finaliza cuando se recibe 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, DEBE asumir que su mensaje RSVP-PATH original o la respuesta desde el otros extremo se han perdido, debiendo reenviar el RSVP-PATH. Dado que todos los mensajes RSVP tienen la misma potencia (idempotentes), no se producen reservas duplicadas.

En IPCablecom, solo los mensajes RSVP-PATH DEBEN incluir objetos RSVP-MESSAGE-ID con la bandera ACK_Desired fijada. 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 tramo del trayecto que funcione con RSVP y que soporte la reducción del refresco 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 AN para dicho RSVP-PATH, el CM lleva a cabo la retransmisión rápida mientras que el MTA autónomo espera a que expire (30 s) su temporizador de refresco RSVP-PATH normal. (El MTA ya no realiza ninguna retransmisión rápida debido a que ha recibido un acuse de recibo.) Si un CM con capacidad de RSVP abandona su 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 el documento relativo a las extensiones de reducción de la tara de refresco RSVP [Draft-ietf-rsvp-refresh-reduct-02] se define un procedimiento de entrega fiable de mensajes RSVP.

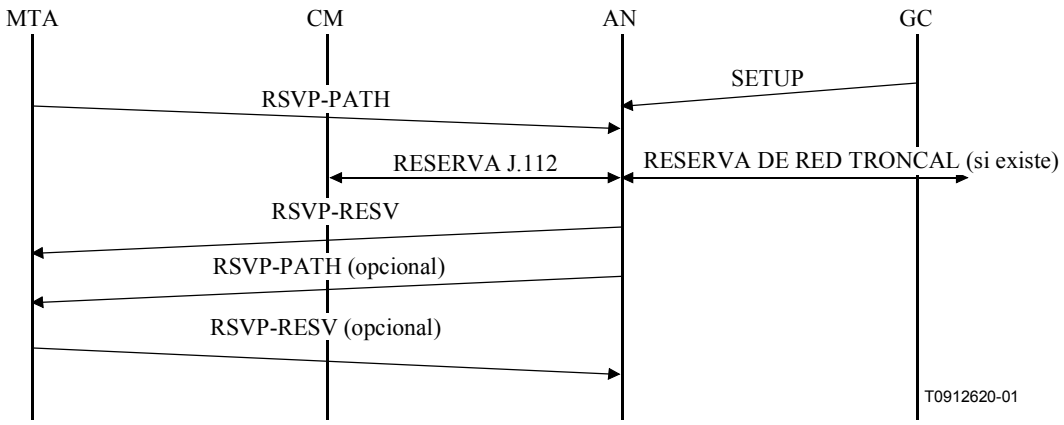


Figura 8/J.163 – Establecimiento de reserva

El AN DEBE aplicar filtros de clasificación de paquetes ascendentes a los flujos J.112. Es decir, el AN DEBE descartar paquetes ascendentes que no concuerden con el conjunto de clasificadores de

paquetes ascendentes del flujo J.112. El filtrado de clasificación de paquetes ascendentes es un requisito opcional del AN en las redes J.112. Esta Recomendación exige su implementación en los flujos J.112 utilizados para transportar trenes de medios IPCablecom. Si un AN decide aplicar los filtros de clasificación ascendentes exclusivamente a los flujos J.112 y no a otros flujos, es el vendedor 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. El RSVP modifica los recursos utilizados mediante cambios en el objeto FLOWSPEC (especificación de flujo) de un mensaje RSVP-RESV y/o mediante cambios en la Tspec de emisor de un mensaje RSVP-PATH. Un cambio de reserva DEBE seguir el mismo proceso que el establecimiento de una nueva reserva. Cuando se trate de la modificación de los recursos de una sesión sin que se deseen aumentar los recursos previamente reservados El control de admisión siempre DEBERÍA superarse con éxito. Debido a que los recursos se describen mediante vectores multidimensionales, una modificación de la reserva que aumente los recursos en un sentido y los disminuya en el otro, DEBE superar el control de admisión. Nótese que para superar el control de admisión, los recursos DEBEN mantenerse dentro del margen de la cantidad de recursos autorizados para la sesión, e igualmente dentro de lo que es la cantidad de recursos disponibles para el AN.

En el caso en que se deba interrumpir una reserva para establecer una sesión con una puerta de mayor prioridad cuando la anchura de banda es insuficiente, el AN DEBE enviar un mensaje RSVP-PATH-ERR y/o PATH-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) DEBE contener un objeto RSVP-ERROR-SPEC con un código de error 2 (fallo de control de la política) y un valor de error 5 (flujo interrumpido).

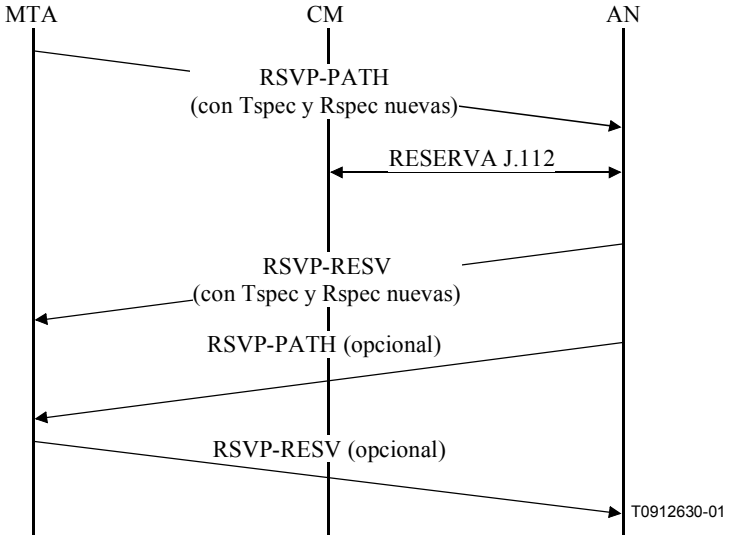


Figura 9/J.163 – Modificación de reserva

6.5.3 Supresión de la reserva

El RSVP proporciona dos mensajes para la supresión explícita del estado de trayecto y de reserva, los mensajes RSVP-PATH-TEAR y RSVP-RESV-TEAR. Para suprimir una reserva en el AN, el MTA DEBERÍA enviar un mensaje RSVP-PATH-TEAR. Para suprimir una reserva existente en

dispositivos RSVP existentes entre el MTA y el AN, el MTA PUEDE enviar un mensaje RSVP-RESV-TEAR. El formato de estos mensajes DEBE ser conforme con la RFC 2205 del IETF, y DEBE incluir el objeto sesión y la plantilla de emisor para permitir que el AN identifique la correspondiente puerta.

Si los estados trayecto y reserva no se refrescan periódicamente, DEBEN temporizar. Ello es adecuado, por ejemplo, cuando falla el MTA. En 6.5.4 se incluye información adicional sobre los mecanismos de refresco.

Cuando el AN recibe un RSVP-PATH-TEAR DEBE responder enviando al MTA un RSVP-RESV-TEAR. El formato de estos mensajes DEBE ser el indicado en la RFC 2205 del IETF.

La versión 1 de RSVP no garantiza la entrega fiable de mensajes RSVP-PATH-TEAR y RSVP-RESV-TEAR, en el supuesto de que en todo caso vencerá la temporización del estado que pretenden suprimir. Sin embargo, para evitar retardos en la supresión (que produce una utilización innecesaria de recursos y que puede producir una facturación excesiva), puede utilizarse el mensaje extensión de fiabilidad a RSVP descrito en [Draft-ietf-mpls-lsp-tunnel-06].

6.5.4 Mantenimiento de la reserva

El RSVP tiene un modelo de estado blando, en el que la reserva temporiza si no se refresca periódicamente. Esta característica se mantiene en el modelo segmentado aquí descrito. Dado que en este modelo es el MTA quien inicia todo el proceso de reserva, el MTA DEBE refrescar periódicamente toda la información de estado RSVP. El MTA DEBE enviar mensajes RSVP-PATH, tal como se define en 6.5.1 dentro del intervalo de tiempo que el AN incluye en el objeto valores de tiempo de RSVP-RESV. Cuando el AN recibe el mensaje RSVP-PATH (también cuando se recibe un mensaje RSVP-PATH habiéndose detectado nodos con capacidad RSVP tal como se describe en 6.5.1) DEBE generar mensajes RSVP-RESV hacia el MTA. Ello mantiene el estado blando del RSVP, lo cual permite garantizar su correcto funcionamiento frente a cambios de encaminamiento y fallos de nodos.

El MTA (o el AN) PUEDE asimismo implementar el modo de refresco simplificado RSVP como otra forma de conservar la anchura de banda ascendente cuando se refresca el estado de la reserva. Permite que nodos RSVP "compriman" sus estados trayecto (o reserva) de múltiples reservas en un único mensaje. En el documento extensiones de la reducción de la tara de refresco RSVP [Draft-ietf-rsvp-refresh-reduct-02] se describe el refresco simplificado de la forma siguiente:

"La extensión de refresco simplificada permite refrescar el estado RSVP sin transmitir mensajes trayecto (*Path*) o reserva (*Resv*) normalizados. Los beneficios de la extensión descrita son que permite disminuir la cantidad de información que debe transmitirse y procesarse para mantener la sincronización de estados de RSVP. Es importante además que la extensión descrita mantenga la capacidad del RSVP para manejar tramos siguientes que no sean RSVP y ajustarse a cambios de encaminamiento. Esta extensión no puede utilizarse con mensajes Path o Resv que presentan cambios en relación con mensajes anteriormente transmitidos, es decir, si se trata de mensajes de activación o disparo.

La extensión de refresco simplificada se basa en la extensión MESSAGE_ID previamente definida. Mediante la extensión de refresco simplificada sólo puede refrescarse un estado que hubiese sido previamente anunciado en mensajes Path y Resv que contuvieran objetos MESSAGE_ID.

La extensión de refresco simplificada utiliza los objetos y el mensaje ACK definido previamente como parte de la extensión de 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 disparo Path y Resv que establecieron el estado. Los campos Message_Identifier se transportan en uno de los tres objetos Srefresh relacionados. Los tres objetos son 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 refrescar todos los estados Resv y Path de sesiones unidifusión. Se compone de una lista de campos Message_Identifier que fueron anunciados originalmente en objetos MESSAGE_ID. Los otros dos objetos se utilizan para refrescar el estado Path de las sesiones multidifusión. Un nodo que recibe un refresco resumido para un trayecto multidifusión necesitará en determinados momentos información de fuente y de grupo. Estos dos objetos proporcionan esta información. Los objetos difieren en la información que contienen y en como se envían. Ambos transportan campos Message_Identifier y las correspondientes direcciones IP de fuente. El 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 MESSAGE_ID MCAST_LIST se utiliza normalmente en enlaces punto a punto.

Un nodo RSVP que reciba un mensaje Srefresh, establece una concordancia entre cada campo Message_Identifier enumerado y un estado Path o Resv instalado. Todos los estados de concordancia se actualizan como si se hubiese recibido un mensaje normal de refresco RSVP. Si no puede encontrarse ningún estado de concordancia, se notifica al emisor del mensaje *Srefresh* mediante un NACK de refresco

Mediante el objeto MESSAGE_ID_NACK se envía un NACK de refresco. Tal como se describe en la cláusula anterior, las reglas para el envío de un objeto MESSAGE_ID_NACK son las mismas que para el envío de un objeto MESSAGE_ID_ACK. Ello incluye el envío del objeto MESSAGE_ID_NACK, ya sea transportado en mensajes RSVP no relacionados o en mensajes ACK RSVP."

En la cláusula 5 de la especificación de las extensiones de la reducción de la tara de refresco RSVP [Draft-ietf-rsvp-refresh-reduct-02] se incluye información sobre la forma de funcionamiento del refresco.

6.6 Definición de mensajes de compromiso

En esta cláusula se definen los mensajes de compromiso que el MTA DEBE generar y que el AN DEBE soportar.

Los mensajes compromiso (*Commit*) DEBEN enviarse como datagramas UDP/IP con número de protocolo 17 (UDP). Cada mensaje *Commit* DEBE ocupar exactamente un datagrama UDP/IP. La dirección IP de destino y el número de puerto que existe en la cabecera UDP DEBEN ser tal como se especifica en el objeto *Commit-Entity* (entidad compromiso) que se devuelve con el mensaje RSVP-RESV. El número de puerto de fuente DEBE ser el puerto en el que el MTA aceptará el mensaje de acuse de recibo.

Los mensajes compromiso DEBEN constar de una cabecera común seguida de un número variable de objetos de longitud variable. La cabecera común DEBE tener el formato siguiente:

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

Los valores de cada campo DEBEN ser como se especifica en la RFC 2205 del IETF. Los tipos de mensajes DEBEN ser los siguientes:

COMMIT	240
COMMIT-ACK	241
COMMIT-ERR	242

Cada objeto DEBE 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		

Los valores de cada campo DEBEN ser tal como se especifica en la RFC 2205 del IETF.

El formato del mensaje COMMIT y del mensaje COMMIT-ACK que cumplan esta Recomendación DEBE ser el siguiente (los elementos en cursiva se definen en 6.3 de esta Recomendación, y todos los demás en la RFC 2205 y/o RFC 2210 del IETF):

<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>

Los objetos sesión (*Session*) y plantilla de emisor (*Sender-Template*) identifican las direcciones IP y los puestos del emisor y del destino, por lo que DEBEN estar presentes. Los recursos comprometidos PUEDEN ser inferiores a los recursos totales reservados (especialmente en un escenario de llamada en espera o de modificación de códec), de tal forma que un mensaje *Commit* (compromiso) PUEDE también contener un objeto <Flowspec> (especificación de flujo) para cada sentido de la sesión. Ello proporciona un mecanismo para aumentar o reducir los recursos comprometidos en tanto que la cantidad de dichos recursos comprometidos no supere los recursos reservados. Nótese que un conjunto de recursos PUEDE retenerse (o congelarse) reduciendo los recursos comprometidos a cero, sin modificar los recursos reservados. Si se omite alguna de las especificaciones de flujo, el AN DEBE hacer que la cantidad de recursos comprometidos en dicho sentido sea igual a la cantidad de recursos reservados.

6.7 Operaciones de compromiso

Un aspecto significativo del modelo de QoS dinámico es que la reserva es un proceso que se realiza en dos fases, con una fase de compromiso que sigue a una fase de reserva. En la cláusula 6.5 anterior se describe la fase de reserva, y en esta se describe la fase de compromiso y su relación con la fase de reserva.

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

Para realizar un COMMIT, el MTA DEBE enviar al AN un mensaje unidifusión. Ello es conveniente debido a que la fase de compromiso sólo implica al MTA y a una puerta. El MTA conoce la dirección del AN y el número de puerto del objeto entidad compromiso del mensaje RSVP-RESV.

Nótese que un mensaje COMMIT difiere sustancialmente de un mensaje RSVP normalizado. Se envía directamente del MTA al AN, en lugar de tramo a tramo tal como ocurre para un mensaje RSVP. Sin embargo, contiene objetos que son sintácticamente iguales a objetos RSVP.

El AN DEBE verificar el valor del ID de puerta, y verificar que el contenido de los objetos sesión y plantilla de emisor concuerdan con reservas previas para el mismo valor del ID de puerta y que, si los objetos sesión inversa y plantilla de emisor inversa están presentes, concuerdan con la reserva

previa con el mismo valor del ID de puerta. El AN DEBE acusar recibo de un mensaje COMMIT con un mensaje COMMIT-ACK o un mensaje COMMIT-ERR.

Cuando un MTA no recibe el acuse de recibo antes de que venza el temporizador T4 (véase el anexo C), el MTA DEBE volver a enviar el mensaje COMMIT, disponiendo de hasta siete intentos.

Si el MTA desea modificar la cantidad de recursos comprometidos dentro de la envolvente reservada, se REQUIEREN otras secuencia COMMIT/COMMIT-ACK.

Si el MTA desea modificar la cantidad de recursos reservados, DEBE repetirse el intercambio de mensajes RSVP-PATH/RSVP-RESV.

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

En esta cláusula se describen las interfaces entre el AN 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 AN es necesaria para la gestión de la puerta y para el servicio de control de admisión de la QoS de IPCablecom. Además, realizar una facturación exacta a los abonados exige que el AN 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 de política común abierta (COPS, *common open policy service*) para el transporte de mensajes de QoS de IPCablecom entre el controlador de puerta y el AN

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

Una "puerta" de QoS dinámica IPCablecom es una entidad de control de la política implementada en al AN para controlar el acceso a servicios de QoS mejorada de una red J.112 para un flujo IP. Las puertas son unidireccionales pues una puerta controla 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.

Si bien una puerta dispone, al igual que un clasificador, de una N-tupla, no es idéntica a un clasificador. El AN DEBE establecer la puerta cuando se autoriza el flujo, existiendo hasta que es explícitamente deshabilitada para terminar la autorización del flujo. Un clasificador J.112 PUEDE establecerse y quedar asociado a una puerta. Una puerta PUEDE existir antes y después que el clasificador que ella autoriza. Una puerta PUEDE considerarse asociada con dos, uno o ningún clasificador.

Un AN que sea conforme a esta Recomendación NO DEBE crear dinámicamente un clasificador con un intercambio de mensajes MAC J.112 salvo que esté autorizada para hacerlo porque exista una puerta para dicho clasificador. Las puertas tienen un identificador, denominado identificador de puerta (ID de puerta), asociado a las mismas. El ID de puerta, que es administrado localmente por el AN en el que esté la puerta, PUEDE estar asociado con una o más puertas unidireccionales. En el caso de una sesión punto a punto, típicamente existen dos puertas unidireccionales, asociadas con un único ID de puerta. Además, existen clasificadores J.112 para cada flujo unidireccional establecido.

7.1.1 Clasificador

Un clasificador es una séxtupla con los elementos siguientes:

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

Si existe un flujo ascendente y un flujo descendente asociado (que forman parte de la misma sesión), DEBEN existir clasificadores separados para cada uno de ellos. El clasificador se actualiza mediante el mensaje RSVP para la reserva realizada para los flujos ascendente y descendente. El flujo de datos de la sesión DEBE concordar con el clasificador a fin de recibir la calidad de servicio asociada con la reserva RSVP. Ulteriores reservas pueden modificar el clasificador.

7.1.2 Puerta

Una puerta está asociada con un flujo unidireccional e incluye lo siguiente:

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

El ID de puerta (que se describe) en la cláusula siguiente, es un identificador de 32 bits que se asigna a partir del espacio local del AN en el que reside la puerta. El mismo ID de puerta PUEDE ser compartido por hasta dos puertas. Típicamente, 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 que un clasificador, descritos en la cláusula anterior. El IP de fuente es la dirección IP (tal como la ve el AN) del originador del flujo. 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. Para determinados parámetros seleccionados del clasificador de prototipo existe libertad de elección. En la señalización de llamada multimedios no se señaliza el puerto UDP de fuente, por lo que 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 poder soportar los dos protocolos de señalización de llamada IPCablecom (DCS y 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. Si así ocurre, su valor en los parámetros de puerta es cero.

Cuando se fija la bandera compromiso automático, los recursos se comprometen inmediatamente tras la reserva. En una aplicación de telefonía, esta facilidad se utiliza típicamente en la puerta descendente del originador de una llamada cuando el destino es una pasarela hacia la RTPC. Cuando el MTA de origen reserva el recurso, el flujo descendente se habilita de forma que el distante devuelva la señal de llamada, y el originador de la llamada puede escuchar la indicación de señal de llamada, los tonos de progresión de llamada y los anuncios. En 7.1.4 se encuentra una descripción más detallada.

Cuando se fija bandera compromiso no permitido, el AN ignora cualquier mensaje COMMIT dirigido a esta puerta. Un controlador de puerta puede utilizar esta facilidad cuando aún no se conozca la dirección del punto extremo distante, y por lo tanto, ésta se especifica como de libre elección en el clasificador prototipo. En una aplicación de ese tipo, el controlador de puerta actualiza normalmente el clasificador prototipo de la puerta antes de que el MTA emita el mensaje COMMIT; la utilización de esta bandera previene algunos escenarios de hurto de servicio.

Las envolventes autorizadas y reservadas forman parte de las especificaciones de flujo de RSVP (tanto las T-spec como las R-spec), tal como se describe 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) DEBE compararse con lo autorizado para el identificador de puerta asociado al sentido de la petición del recurso. Los recursos autorizados se especifican en la envolvente autorizada. Asimismo se verifica la posibilidad de libre elección de la puerta para determinadas entradas.

El ID de recurso es un identificador local de 32 bits que se asigna a partir del espacio local del AN en el que reside la puerta. Un identificador de recursos puede ser compartido por cualquier número de puertas y, por lo tanto, compartir éstas un conjunto común de recursos con la única restricción de que sólo una de dichas puertas de cada sentido puede tener recursos comprometidos.

7.1.3 Identificador de puerta

Un ID de puerta es un identificador único signado localmente por el AN en el que reside la puerta. El ID de puerta es un identificador de 32 bits. 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 y consta de una única puerta ascendente y una única puerta descendente.

El ID de puerta DEBE estar asociado con la información siguiente:

- Una o dos puertas, que DEBEN formar parte de una de las siguientes combinaciones:
- Una única puerta ascendente.
- Una única puerta descendente.
- Una única puerta ascendente y una única puerta descendente [esta sería típicamente una implementación bidireccional].
- Información de coordinación de puerta.
- Dirección: puerto del AN distante (u otra entidad) con la que se debe coordinar la asignación de recursos para este conjunto de puertas.
- ID de puerta asignado en el AN distante (u otra entidad) para el conjunto de puertas distantes.
- Clave de seguridad para la comunicación con el AN distante (u otra entidad).
- Bandera sin-coordinación-de-puerta, que cuando está fijada, hace que el AN no realice la coordinación de puerta, es decir, no se exige la recepción de un mensaje de apertura de puerta desde el AN distante (u otra entidad).
- Bandera sin-apertura-de-puerta, que cuando está fijada, el AN no envía un mensaje de apertura de puerta al AN distante (u otra entidad).
- Información de contabilidad y facturación
- Dirección: puerto del servidor de mantenimiento de registros primario que debe recibir los registros de eventos.
- Dirección: puerto del servidor de mantenimiento de registros secundario que debe utilizarse 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 de facturación que debe enviarse al servidor de mantenimiento de registros con cada registro de evento inicio de QoS/parada de QoS.
- Información adicional de facturación que, si se facilita, se utiliza para generar mensajes de eventos respuesta de llamada y desconexión de llamada.

El ID de puerta DEBE ser único entre todos los valores de las puertas actualmente atribuidas por el AN. El valor de la cantidad de 32 bits NO DEBERÍA elegirse de entre un conjunto reducido de valores de enteros, ya que la posesión del 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 valores de ID de puerta de la forma siguiente: se hace una partición de la palabra de 32 bits en dos, una parte índice y una parte aleatoria. La parte índice identifica la puerta realizando una indexación respecto a un cuadro de valores reducido, mientras que la parte aleatoria proporciona un cierto nivel de indeterminación con respecto al valor.

Las banderas sin-apertura-de-puerta y sin-coordinación-de-puerta se combinan para ofrecer la flexibilidad necesaria al controlador de puerta en relación con las conexiones con elementos que no son AN, con elementos AN que no cumplen la especificación o con sistemas que no son IPCablecom. El agente de llamada NCS proporciona normalmente su propia dirección como dirección de AN distante, y fija la bandera sin-apertura-de-puerta. Cuando se completa la llamada, el agente de llamada genera un mensaje apertura de puerta que envía al AN; éste arranca el temporizador T2 (véase 7.1.4) y obliga a que el MTA comprometa recursos. Cuando la llamada se termina debido a errores (el MTA no puede indicar dicho evento), el agente de llamada recibe notificación de colgado en el mensaje cierre de puerta. La utilización de la bandera sin-apertura-de-puerta reduce la carga de proceso en el agente de llamada NCS sin pérdida de funcionalidad.

La bandera sin-coordinación-de-puerta se utiliza normalmente cuando el punto extremo distante es un sistema que no es IPCablecom y no puede realizar los procedimientos de coordinación de puerta. Cuando se combina con la bandera sin-apertura-de-puerta, la puerta funciona con independencia del otro punto extremo. En 7.1.4 se analiza con detalle el efecto de estas dos banderas utilizando el diagrama de transición de estados.

7.1.4 Diagrama de transición de estados

Se considera que las puertas tienen los estados siguientes:

- Asignada – es el estado inicial de una puerta a petición del controlador de puerta (GC).
- Autorizada – el GC ha autorizado el flujo con los límites de recursos definidos.
- Reservada – se han reservado los recursos para el flujo.
- Comprometida– los recursos se están utilizando.
- Comprometida distante y Comprometida local – estados transitorios que se producen cuando una puerta ejecuta el protocolo de coordinación de puerta con la puerta distante.

El AN DEBE soportar los estados y las transiciones de puerta que se muestran y describen en esta cláusula. Todas las puertas a las que el AN asigna el mismo ID de puerta DEBEN realizar simultáneamente la transición a través de los estados que se muestran en la figura 10.

El AN crea una puerta mediante una instrucción asignación de puerta o una instrucción establecimiento de puerta emitida por el controlador de puerta (GC). En ambos casos, el AN asigna un identificador inequívoco, denominado ID de puerta, que se devuelve al GC. Si la puerta ha sido creada mediante un mensaje establecimiento de puerta, el AN DEBE marcar la puerta con el estado "autorizada" y DEBE arrancar el temporizador T1. Si la puerta ha sido creada mediante un mensaje asignación de puerta, el AN DEBE marcar la puerta con el estado "asignada" arranca el temporizador T0, y DEBE esperar una instrucción establecimiento de puerta, momento en que la puerta se DEBE marcar con el estado "autorizada". Si el temporizador T0 expira y la puerta está en el estado "asignada" o el temporizador T1 expira estando la puerta en el estado "autorizada," el AN DEBE suprimir la puerta. El temporizador T0 limita el tiempo que el ID de puerta sigue siendo válido sin haberse especificado parámetros de puerta. El temporizador T1 limita el tiempo durante el que la autorización sigue siendo válida.

Una puerta que se encuentre en el estado "autorizada" 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 AN DEBE 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 AN DEBE implementar al menos dos políticas de control de admisión, una para comunicaciones normales de voz y otra para comunicaciones de emergencia. Estas dos políticas DEBEN tener parámetros de provisión que, como mínimo, especifiquen:

1) una 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 PUEDE asimismo especificar si una nueva sesión de dicho 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 se realizan con éxito, la puerta DEBE marcarse con el estado "reservada". Si no tienen éxito, la puerta permanece en el estado "autorizada". Nótese que la reserva que realmente realiza el MTA puede ser por una cantidad menor que la autorizada, por ejemplo, reserva solamente en sentido ascendente cuando una pareja de puertas se establecieron autorizando flujos ascendentes y descendentes. Si la puerta se marcó con la bandera "compromiso-automático", los recursos reservados quedan inmediatamente comprometidos, pero el estado de la puerta no se modifica.

En el estado "reservada", la puerta espera que el MTA comprometa los recursos. La instrucción (compromiso) del MTA es un mensaje UDP multidifusión o una petición equivalente a través de la interfaz de capa MAC. La instrucción Commit se sincroniza normalmente con la puerta distante mediante los mensajes de coordinación; salvo que los dos clientes de ambos puntos extremos generen las instrucciones Commit casi simultáneamente, la autorización se cancela. Si la puerta aún se encuentra en el estado "reservada" y el temporizador T1 expira (es decir, el MTA no emite la instrucción Commit), el AN DEBE liberar los recursos reservados, DEBE responder con Commit_Err y NO DEBE cambiar el estado de la puerta.

Si estando el AN en el estado "reservada", recibe del MTA una instrucción Commit, y está habilitada la bandera sin-coordinación-de-puerta, el AN DEBE marcar la puerta con el estado "comprometida" y detener el temporizador T1. Salvo que esté fijada la bandera sin-apertura-de-puerta, el AN DEBE enviar un mensaje apertura-de-puerta a la entidad de coordinación de puerta.

Si estando el AN en el estado "reservada", recibe del MTA una instrucción Commit, y no está habilitada la bandera sin-coordinación-de-puerta, el AN DEBE marcar la puerta con el estado "comprometida local" y arrancar el temporizador T2. Salvo que esté fijada la bandera sin-apertura-de-puerta, el AN DEBE enviar un mensaje apertura-de-puerta a la entidad de coordinación de puerta. El temporizador T2 limita el tiempo en que una puerta puede tener recursos comprometidos en un extremo y no en el otro.

En el estado "comprometida local", la puerta ha comprometido los recursos locales, pero espera que el cliente del punto extremo distante comprometa recursos en dicho extremo. Si estando en este estado expiran los temporizadores T1 o T2, el AN DEBE desactivar todos los recursos comprometidos con esta puerta, liberar todos los recursos reservados con la misma, enviar un mensaje cierre-de-puerta (sólo si la puerta ha sido previamente abierta) a la entidad de coordinación de puerta y suprimir la puerta.

Si estando el AN en el estado "comprometida local", recibe un mensaje apertura-de-puerta de la entidad de coordinación de puerta, el AN DEBE detener los temporizadores T1 y T2, y DEBE marcar la puerta con el estado "comprometida".

Si estando el AN en el estado "reservada", recibe un mensaje apertura-de-puerta de la entidad de coordinación de puerta, el AN DEBE marcar la puerta con el estado "comprometida distante" y arrancar el temporizador T2.

En el estado "comprometida distante" se ha notificado a la puerta que el MTA del extremo lejano ha activado recursos, pero no así el MTA local. Si el temporizador T1 o el T2 expira en este estado, el AN DEBE liberar todos los recursos reservados con esta puerta, enviar un mensaje cierre-de-puerta a la entidad de coordinación de puerta y suprimir la puerta. Si cuando se recibe la instrucción Commit está fijada la bandera compromiso-no-permitido, el AN DEBE responder con un mensaje error de compromiso y NO DEBE cambiar el estado de la puerta.

Si estando el AN en el estado "comprometida distante", recibe del MTA una instrucción Commit, el AN DEBE detener los temporizadores T1 y T2, y DEBE marcar la puerta con el estado "comprometida". Salvo que esté fijada la bandera sin-apertura-de-puerta, el AN DEBE enviar un mensaje apertura-de-puerta a la entidad de coordinación de puerta.

Una vez que la puerta se encuentra en el estado "comprometida", ha alcanzado una configuración estable y no tiene temporizadores pendientes ni acciones relativas al vencimiento de los mismos. Se han comprometido recursos tanto en esta puerta como en la correspondiente puerta en la entidad distante. Los recursos siguen comprometidos hasta que el MTA emita una instrucción liberación o la puerta distante señalice su intención de dar por terminada la utilización de los recursos.

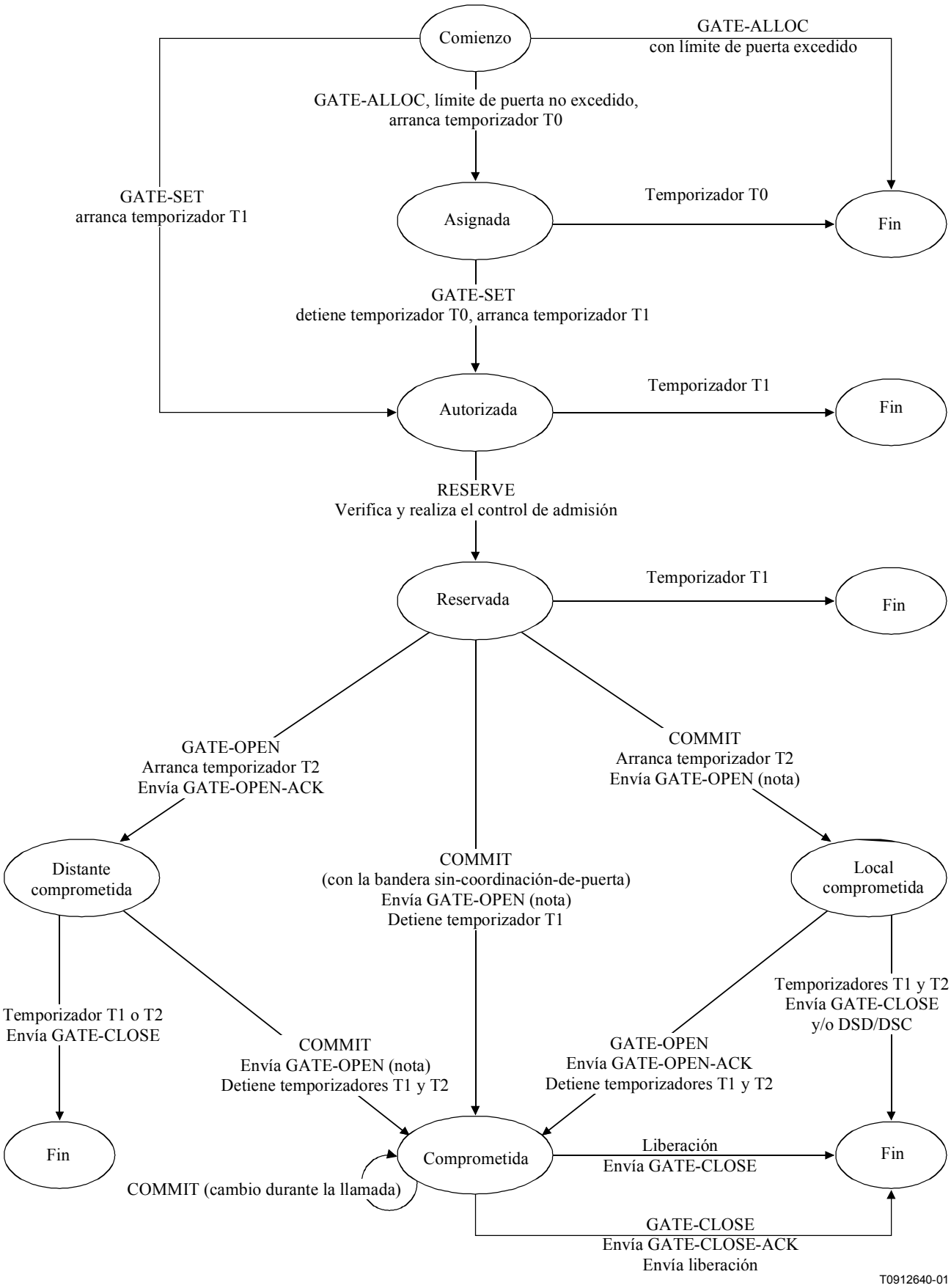
Si estando el AN en el estado "comprometida", recibe un mensaje cierre-de-puerta de la entidad de coordinación de puerta, el AN DEBE desactivar todos los recursos comprometidos para el MTA local, liberar todos los recursos reservados y suprimir la puerta.

Si estando en el estado "comprometida", el AN recibe del MTA una instrucción liberación, ya sea en la forma de mensaje RSVP-PATH-TEAR o a través de la interfaz de capa MAC, o a partir del fallo de un cliente en refrescar una reserva o a partir de mecanismos internos J.112 que detectan un fallo de cliente, el AN DEBE desactivar todos los recursos comprometidos para el MTA, liberar todos los recursos reservados, enviar un mensaje cierre-de-puerta a la entidad de coordinación de puerta y suprimir la puerta.

Mientras el AN esté en el estado "comprometida", DEBE permitir que el MTA inicie cambios en la reserva o en el compromiso de recursos, dentro de los límites de la autorización y el control de admisión local.

7.1.5 Coordinación de puerta

Además de controlar la función local J.112 de clasificación de flujos, las puertas DEBEN comunicarse con sus homólogas distantes para un mismo flujo a fin de confirmar que el lado lejano también tiene el compromiso de facturar por esta sesión. Ello tiene por objetivo evitar diversos escenarios de hurto de servicio, tal como se describe en el apéndice IX. En la cláusula 8 se describe el protocolo para esta comunicación.



NOTA – Envía GATE-OPEN salvo que esté fijada la bandera sin-apertura-de-puerta.

Figura 10/J.163 – Diagrama de transición de estados de una puerta

7.2 Perfil COPS para IPCablecom

El control de admisión de QoS de IPCablecom consiste en la gestión de la asignación de recursos 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 11 se muestran los módulos operacionales de alto nivel. Las políticas administrativas se almacenan como una base de datos de la política que controla el servidor COPS. Si bien en una implementación IntServ típica de COPS es el servidor quien determina los recursos disponibles, una implementación Diffserv lleva la política hasta el cliente de forma que sea éste pueda tomar decisiones de control de admisión.

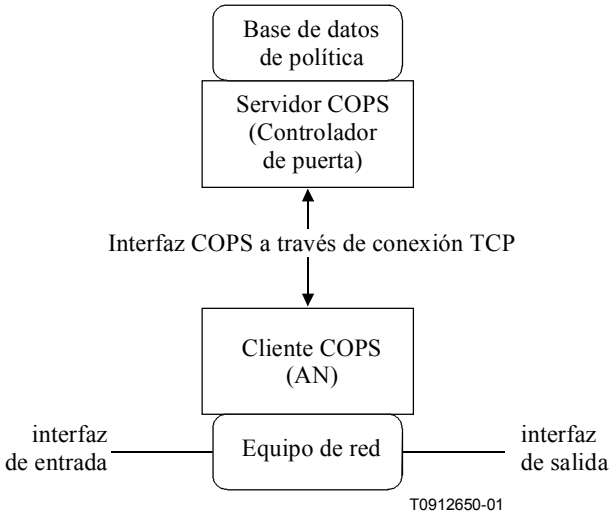


Figura 11/J.163 – Esquema del control de admisión de QoS

Las decisiones de control de admisión de QoS que toma el servidor COPS DEBEN pasar al cliente COPS utilizando COPS. El cliente COPS PUEDE realizar algunas peticiones de control de admisión de QoS al servidor COPS en base a los eventos de red que genera el protocolo de señalización de QoS, o utilizando mecanismos de detección del flujo de datos. El evento de red puede también ser la necesidad de QoS en la gestión de la anchura de banda, por ejemplo, se hace operativa una nueva interfaz con capacidades de QoS.

Las decisiones de política de QoS que toma el servidor COPS PUEDEN hacerse llegar al cliente COPS sobre la base de una petición de servicio de QoS externa, fuera de banda, por ejemplo, una petición desde el AN de terminación o desde un controlador de puerta. Estas decisiones sobre la política PUEDEN ser almacenadas por el cliente COPS en un punto de decisión de política local, pudiendo el AN acceder a dicha información de decisión para tomas decisiones de control de admisión en relación con peticiones de sesión entrantes recibidas en el AN.

El protocolo COPS del IETF proporciona el soporte necesario para las interacciones entre cliente COPS y servidor COPS para la QoS del control de admisión. 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. El mensaje REQ puede contener información específica del cliente que el

servidor utiliza junto con datos de la base de datos de política de admisión de sesión con el fin de tomas decisiones basadas en la política.

- Decisión (DEC): El servidor responde a los mensajes REQ devolviendo DEC al cliente que hizo la petición original. Los mensajes DEC pueden enviarse inmediatamente en respuesta a una REQ (es decir, una DEC solicitada) o en cualquier instante después de cambiar/actualizar una decisión previa (es decir, una DEC no solicitada).
- Información de estado (RPT, *report state*): El cliente COPS envía un mensaje RPT al servidor COPS indicando cambios en el estado de la petición del cliente COPS. 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 puede también utilizar RPT para informar periódicamente al servidor COPS del estado del cliente COPS.
- Supresión del estado de petición (DEL, *delete request state*): El cliente COPS envía un mensaje DEL al servidor COPS para solicitar que se elimine el estado de petición. Puede ser el resultado de una liberación de recursos de QoS por parte del cliente COPS.
- Mantener vivo (KA, *keep alive*): Puede ser enviado por el cliente COPS y por el servidor COPS para la detección de fallos de comunicación.
- Petición de estado de sincronización (SSR, *synchronize state request*)/Compleción de estado de sincronización (SSC, *synchronize state complete*): El servidor COPS envía un SSR solicitando información de estado del cliente COPS. El cliente vuelve a enviar al servidor señales de interrogación de petición para la sincronización, y el cliente envía un mensaje SSC para indicar que se ha completado la sincronización. Debido a que el GC carece de estados, las operaciones SSR/SSC no son importantes en el contexto IPCablecom y no son utilizadas por el AN ni por el GC.

En la arquitectura IPCablecom, el controlador de puerta es una entidad punto de decisión de política (PDP) COPS y el AN es la entidad punto de imposición de política COPS (PEP, *Policy Enforcement Point*).

Los detalles del protocolo COPS figuran en el texto del proyecto de documento IETF RAP-COPS-07. Esta RFC del IETF proporciona una descripción de los protocolos COPS básicos 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*) (es decir, el aprovisionamiento de clientes).En el anexo X se presenta una visión general más detallada del protocolo COPS.

7.3 Formatos de los mensajes del protocolo de control de puerta

Los mensajes del protocolo del control de puerta se transportan en los mensajes de protocolo COPS. COPS utiliza una conexión TCP establecida entre el AN y el controlador de puerta, y utiliza mecanismos especificados en normas que están siendo desarrolladas para garantizar la seguridad del trayecto de comunicación.

7.3.1 Formato común de los mensajes COPS

Cada mensaje COPS consta de una cabecera COPS seguida de un número de objetos tipificados. El GC y el AN DEBEN soportar los mensajes COPS definidos a continuación.

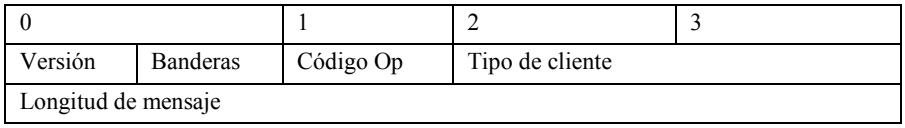


Figura 12/J.163 – Cabecera común de mensajes COPS

Versión es un campo de 4 bits que presenta el número de versión COPS vigente. DEBE ponerse a 1.

Banderas es un campo de 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 DEBE ponerse a 1. En cualquier otro caso (por ejemplo, una decisión no solicitada) la bandera NO DEBE ponerse a 1 (valor = 0). Todas las demás banderas deben ponerse a 0.

Código Op es un campo de 1 byte que 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 vivo (KA)

Tipo de cliente es un identificador de 16 bits. En IPCablecom el tipo de cliente DEBE fijarse a cliente IPCablecom (0x8005). Para mensajes mantener vivo (KA) (Código Op = 9) el tipo de cliente DEBE ponerse a 0, ya que KA se utiliza para la verificación de la conexión más que para la verificación de la sesión del cliente.

Longitud del mensaje es un valor de 32 bits que indica el tamaño del mensaje en octetos. Los mensajes DEBEN estar alineados entre límites establecidos cada 4 bytes, por lo tanto, la longitud DEBE ser múltiplo de cuatro.

A la cabecera común COPS siguen un número variable de objetos. Todos los objetos tienen el mismo formato; cada uno consta de una o más palabras de 32 bits con una cabecera de cuatro octetos de acuerdo con el formato siguiente (véase la figura 13).

0	1	2	3
Longitud		Número-C	Tipo-C
(Contenido de objetos)			

Figura 13/J.163 – Formato de objetos comunes COPS

Longitud es un valor de dos octetos que DEBE incluir el número de octetos (incluida la cabecera) del objeto. Si la longitud en octetos no es un múltiplo de cuatro, se utiliza el relleno al final del objeto de forma que éste quede alineado con el siguiente límite de 32 bits. En el lado de recepción, el límite siguiente del objeto DEBE encontrarse redondeando la longitud del objeto anterior hasta el siguiente 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 el proyecto de documento RAP-COPS-07 del IETF) que se utilizan en esta Recomendación y sus valores de Número C son los siguientes:

1 = Asa

6 = Decisión

8 = Error

9 = Información específica de cliente

10 = Temporizador de mantener vivo

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

7.3.2 Objetos COPS adicionales para el control de puerta

Al igual que ocurre con los tipos de clientes COPS-PR y COPS-RSVP, el tipo de cliente IPCablecom define una serie de formatos de objeto. Estos objetos DEBEN estar situados en un objeto Decisión, Número C = 6, Tipo C = 4 (datos de decisión específicos de cliente) cuando se transportan desde el GC al AN en un mensaje decisión. También DEBEN situarse en un objeto ClientSI (información específica de cliente), Número C = 9, Tipo C = 1 (señalización de cliente SI) cuando se transportan desde un AN al GC en un mensaje informe. Se codifican de forma similar a los objetos específicos de cliente para COPS-PR; a continuación se incluyen codificaciones concretas. Al igual que en COPS-PR, estos objetos se enumeran utilizando un espacio de numeración específico del cliente, que es independiente del espacio de numeración de objetos COPS de máximo nivel. Por este motivo, los números y tipos de objetos se representan como Número S y Tipo S respectivamente.

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

7.3.2.1 Identificador de transacción (Transaction-ID)

El ID de transacción contiene un testigo que utiliza el GC para hacer corresponder las respuestas del AN 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	

Identificador de transacción es una cantidad de 16 bits que PUEDE ser utilizada por el GC para hacer corresponder respuestas a instrucciones.

Tipo de instrucción de puerta DEBE tomar 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

7.3.2.2 Identificador de abonado (Subscriber-ID)

El ID de abonado identifica el abonado para esta petición de servicio. Su utilización principal es evitar ataques de denegación de servicio.

Longitud = 8	Número S = 2	Tipo S = 1
Dirección IP v4 (32 bits)		

o:

Longitud = 20	Número S = 2	Tipo S = 2
Dirección IP v6 (128 bits)		

7.3.2.3 Identificador de puerta (Gate-ID)

Este objeto identifica la puerta o el conjunto de puertas a las que se hace referencia en el mensaje instrucción, o que asigna el AN para un mensaje de respuesta.

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

7.3.2.4 Cómputo 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
Contador (32 bits)		

7.3.2.5 Especificación de puerta (Gate-spec)

Longitud = 60 u 88 ó 116, etc.		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)		
Campo DS	Reservado	Reservado	Reservado	
Valor del temporizador T1				
Valor del temporizador T2				
Velocidad del 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 cresta de los datos (p) (número en coma flotante de 32 bits del IEEE)				
Unidad mínima sujeta a la política [m] (entero de 32 bits)				
Tamaño mínimo 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)				

Conjuntos adicionales de valores de r, b, p, m, M, R y S, según sea necesario para describir la autorización	Alt #2 de espec de flujo, etc.

Sentido puede ser 0 para una puerta en sentido descendente, o 1 para una puerta en sentido ascendente.

ID de protocolo es el valor para el que debe existir concordancia en la cabecera IP, siendo cero si no hay tal concordancia.

Las banderas se definen de la forma siguiente:

0x01 Compromiso automático, si está fijada, los recursos se comprometen inmediatamente después de la reserva.

0x02 Compromiso no permitido, si está fijada, hace que el AN ignore cualquier mensaje COMMIT para esta puerta.

Las restantes quedan en reserva y DEBEN ser cero.

Clase de sesión identifica la política de control de admisión adecuada o los parámetros que deben aplicarse a esta puerta. Los valores permitidos son lo siguientes:

0x00 No especificado

0x01 Sesión de VoIP de prioridad normal

0x02 Sesión de VoIP de alta prioridad (por ejemplo, E.911).

Los restantes valores están actualmente en reserva.

Dirección IP de fuente y Dirección IP de destino son una pareja de direcciones IPv4 de 32 bits, o cero cuando no exista concordancia (es decir, cuando se trate de un caso de libre elección que permite la concordancia con cualquier petición del MTA).

Puerto de fuente y Puerto de destino son una pareja de valores de 16 bits, o cero si no existe concordancia.

Los valores de r, b, p, m, M, R y S se describen en 6.2. La especificación de puerta PUEDE contener múltiples conjuntos de estos valores para especificar autorizaciones complejas (tal como se describe en 6.2).

El campo DS queda definido mediante la estructura siguiente:

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

A fin de conseguir la retrocompatibilidad con las implementaciones actuales de sistemas y utilizar la precedencia IP tal como se define en RFC 2474 del IETF y RFC 791 del IETF, 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

Los valores del temporizador T1 y del temporizador T2 se expresan en milisegundos y se utilizan en el diagrama de transición de puerta que se describe en 8.1.4. Si en un único mensaje COPS existen múltiples objetos especificación de puerta, los valores de T1 y T2 DEBEN ser idénticos en todas las ocurrencias de los mismos.

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

Longitud		Número S = 6	Tipo S = 1
Dirección IP del AN (32 bits)			
Puerto de AN (16 bits)		Banderas, abajo definidas	
ID de puerta distante			
Algoritmo	Clave de seguridad		

Dirección IP del AN es la dirección del AN distante con el que se realiza la coordinación de puerta.

Puerto de AN es el número de puerto para los mensajes enviados para la coordinación de puerta. Si el número de puerto no está disponible para el controlador de puerta, se pone a cero. Un valor cero hace que el AN ignore este campo.

Las banderas se definen de la forma siguiente:

0x0001 Sin-coordinación-de-puerta, si está fijado, no se realiza la coordinación de puerta. El AN no precisa entonces recibir una apertura de puerta de la entidad distante.

0x0002 Sin-apertura-de-puerta, si está fijado hace que el AN no envíe el mensaje apertura de puerta cuando se procesa un mensaje compromiso.

Los restantes quedan en reserva y DEBEN ser cero.

ID de puerta distante es el ID de puerta que el AN distante asigna a la puerta o al conjunto de puertas.

Algoritmo es un campo de 1 byte que tomar uno de los siguientes valores decimales:

100 = MAC basado en MD5, tal como especifica Radius en RFC 2138 del IETF.

En futuras versiones de esta Recomendación se podrán incorporar alternativas adicionales para el algoritmo de autenticación.

Clave de seguridad es una clave de longitud variable que se utiliza para verificar la autenticación en los mensajes de coordinación de puerta. La longitud de la clave es un valor inferior en 17 a la longitud del objeto.

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

Este objeto contiene toda la información necesaria para soportar los mensajes de los eventos arranque de QoS (QoS-Start) y de parada de QoS (QoS-Stop), tal como se especifica y requiere en UIT-T J.164.

Longitud = 36	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 de facturación (16 bytes)		

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

Puerto del servidor de mantenimiento de registros primario es el número de puerto de los eventos de registros enviados.

Los valores de las banderas son los siguientes:

0x01 Indicador de procesamiento en lotes. Si está fijado, el AN DEBE acumular registros de eventos en un fichero por lotes que debe enviar al servidor de mantenimiento de registros a intervalos periódicos. Si está a cero, el AN DEBE enviar los registros de eventos al servidor de mantenimiento de registros en tiempo real.

Los restantes quedan en reserva y DEBEN ser cero.

Dirección IP del servidor de mantenimiento de registros secundario es la dirección del sistema de mantenimiento de registros secundario al que se envían los registros si el servidor de mantenimiento de registros primario está indisponible.

Puerto del servidor de mantenimiento de registros secundario es el número de puerto de registros de eventos enviados.

ID de correlación de facturación es el identificador asignado por el CMS a todos los registros relacionados con esta sesión.

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

Este objeto contiene toda la información necesaria para soportar los mensajes de eventos respuesta de llamada y desconexión de llamada. Si este objeto está presente en la instrucción GATE-SET, el AN DEBE generar los mensajes de evento respuesta de llamada y desconexión de llamada.

Longitud = 84	Número S = 8	Tipo S = 1
Número de la parte llamada		
		Reservado
Número de encaminamiento		
		Reservado
Número tasado		
		Reservado
Número de encaminamiento de ubicación		
		Reservado

7.3.2.9 Error de IPCablecom (IPCablecom-Error)

Es un objeto de error específico de cliente que se define de la forma siguiente.

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 = ID de puerta ilegal

3 = Valor de clase de sesión ilegal

4 = Límite de puerta excedido por el abonado

127 = Otro, error no especificado

El código de sub-error se reserva para una utilización futura.

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

Longitud = 20	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	

Dirección IP de DF para CDC es la dirección IP de la función de distribución (DF, *delivery function*) de vigilancia electrónica a la que se envían los eventos de mensajes duplicados.

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

Las banderas se definen de la forma siguiente:

0x0001 DUP-EVENT. Si está a uno, el AN DEBE enviar una copia duplicada de todos los mensajes de eventos relacionados con esta puerta (por ejemplo, inicio de QoS, parada de QoS y, posiblemente respuesta de llamada y desconexión de llamada) a la dirección IP de DF para CDC.

0x0002 DUP-CONTENT. Si está a uno, el AN DEBE enviar una copia duplicada de todos los paquetes en los que exista concordancia entre el clasificador o clasificadores de esta puerta y la dirección IP de DF para CCC.

Los restantes están reservados y DEBEN ser cero.

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

Puerto de DF para CCC es el número de puerto para el contenido de llamadas duplicada.

7.3.2.11 Parámetros de descripción de sesión (Session-Description-Parameters)

Longitud =	Número S = 11	Tipo S = 1
Cadenas SDP		

Cadenas SDP es a descripción de sesión (SDP, *session description*) del tren de paquetes ascendente seguido de un octeto NULO, seguido de la descripción de sesión (SDP) del tren de datos descendente. Se añade un relleno suficiente de octetos NULOS para que la longitud total sea un múltiplo de cuatro octetos.

Si este objeto está presente en el mensaje establecimiento de puerta, el AN DEBE incluir esta información en el mensaje de evento inicio de QoS.

7.3.2.12 Puerto de coordinación de puerta (Gate-Coordination-Port)

Este objeto contiene el número del puerto UDP que utiliza un AN para los mensajes de coordinación de puerta entrantes.

Longitud = 8	Número S = 12	Tipo S = 1
Puerto de AN (16 bits)	Reservado	

Este objeto estaría normalmente incluido en el mensaje GATE-ALLOC-ACK que envía un AN en respuesta a un GATE-ALLOC. Sin embargo, si se utiliza un mensaje GATE-SET para asignar una puerta en lugar de GATE-ALLOC, este objeto debe estar presente en el mensaje GATE-SET-ACK.

7.3.3 Definición de mensajes de control de puerta

Los mensajes que realizan el control de puerta entre el GC y el AN DEBEN definirse y tener el formato que se indica a continuación. Nótese que los mensajes desde el GC al AN con mensajes de decisión COPS, y los mensajes desde el AN al GC son mensajes de informe COPS.

<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-Coordination-Port>
<Gate-Alloc-Err> := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
<IPCablecom-Error>
<Gate-Set> := <Decision-Header> <Transaction-ID> <Subscriber-ID>
[<Activity-Count>] [<Gate-ID>]
[<Remote-Gate-Info>]
[<Event-Generation-Info>]
[<Media-Connection-Event-Info>]
[<Electronic-Surveillance-Parameters>]
[<Session-Description-Parameters>]
<Gate-Spec> [<Gate-Spec>]
<Gate-Set-Ack> := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
<Gate-ID> <Activity-Count>
[<Gate-Coordination-Port>]
<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> [<Remote-Gate-Info>]
[<Event-Generation-Info>]
[<Media-Connection-Event-Info>]
<Gate-Spec> [<Gate-Spec>]
<Gate-Info-Err> := <ClientSI-Header> <Transaction-ID> <Gate-ID>
<IPCablecom-Err>
<Gate-Delete> := <Decision-Header> <Transaction-ID> <Gate-ID>
<Gate-Delete-Ack> := <ClientSI-Header> <Transaction-ID> <Gate-ID>
<Gate-Delete-Err> := <ClientSI-Header> <Transaction-ID> <Gate-ID>
<IPCablecom-Err>

El objeto contexto (NUM-C = 2, TIPO-C = 1) del mensaje de decisión COPS tiene el valor de Tipo-R (bandera de tipo de petición) puesto a 0x08 (petición de configuración) y el valor el 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 AN genere un mensaje informe que indica fallo. El objeto tipo de informe (NUM-C = 12, TIPO-C = 1) incluido en el mensaje informe COPS tiene el campo tipo de informe puesto a 1 (éxito) o 2 (fracaso) dependiendo del resultado de la instrucción de control de puerta. Todos los mensajes informe que incluyen la respuesta del control de puerta deben tener fijado el bit de la bandera de mensaje solicitado en la cabecera COPS.

7.4 Operación del protocolo de control de puerta

7.4.1 Secuencia de inicialización

Cuando el AN (es decir, el punto de imposición de política de COPS) arranca, espera las conexiones TCP sobre el puerto 2126 (asignado por IANA). Cualquier controlador de puerta que necesite contactar al AN DEBE establecer una conexión TCP con él a través de dicho puerto. Es previsible que varios controladores de puerta establezcan conexiones COPS con un único AN. Cuando se establece la conexión TCP entre el AN y el GC, el AN envía información sobre sí mismo al GC mediante un mensaje CLIENT-OPEN. Esta información incluye el identificador de AN (AN-ID) facilitado en el objeto identificación de PEP (PEPID, *PEP identification*). El AN DEBERÍA omitir el objeto última dirección PDP (*LastPDPAddr*) del mensaje CLIENT-OPEN.

En respuesta, el controlador de acceso envía un mensaje CLIENT-ACCEPT. Este mensaje incluye el objeto temporizador mantener vivos, que informa al AN del máximo intervalo entre mensajes mantener vivo.

El AN envía entonces un mensaje REQUEST, incluyendo el objeto asa y el objeto 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 asa contiene un número que elige el AN. El único requisito impuesto a ese número es que un AN NO DEBE utilizar el mismo número para dos mensajes de petición (REQUEST) distintos en una única conexión COPS; en el entorno IPCablecom el asa no tiene otro significado en el protocolo. Con ello se completa la secuencia de inicialización, que se muestra en la figura 14.

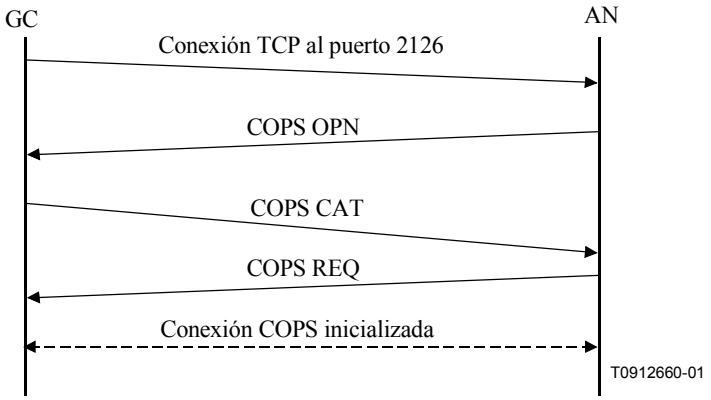


Figura 14/J.163 – Establecimiento de conexión COPS

El AN DEBE enviar periódicamente al GC un mensaje COPS KEEP-ALIVE (KA). Cuando recibe el mensaje COPS KA, el GC DEBE devolver al AN el mensaje COPS KA. Esta transacción se muestra y documenta completamente en RFC 2748 del IETF. DEBE realizarse tan a menudo como se especifica en el objeto temporizador de mantener vivos, que se devuelve en el mensaje CLIENT-ACCEPT. EL mensaje KEEP-ALIVE se envía con el tipo de cliente puesto a cero.

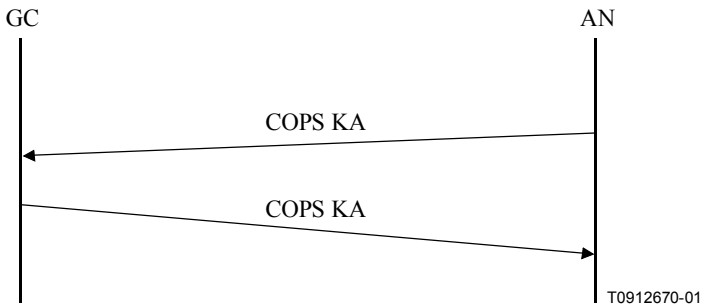


Figura 15/J.163 – Intercambio del mensaje COPS mantener vivo (KA)

7.4.2 Secuencia de operación

El protocolo entre el controlador de puerta y el AN 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 AN. 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. En las subcláusulas siguientes se describen los procedimientos para dichos mensajes. Todos se envían utilizando objetos específicos de cliente dentro del objeto de decisión de mensajes COPS DECISION. Las respuestas desde el AN se envían como un mensaje REPORT-STATE con objetos específicos de cliente en el objeto ClientSI.

Los mensajes DECISION y REPORT-STATE DEBEN contener la misma asa que la utilizada en el mensaje REQUEST inicial enviado por el AN 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 política y de tráfico para la puerta o conjunto de puertas, y establece la información de facturación y coordinación de puerta.

GATE-INFO es un mecanismo mediante el que el controlador de puerta puede determinar cuál es el estado actual y los valores de parámetros de una puerta o conjunto de puertas existentes.

El AN DEBE enviar periódicamente al GC un mensaje mantener vivo (KA) para facilitar la detección de fallos de la conexión TCP. El controlador de puerta registra cuándo se reciben los mensajes KA. Si el controlador de puerta no ha recibido del AN un KA cuando especifica RFC 2748 del IETF, o bien si el controlador de puerta no ha recibido una indicación de error de la conexión TCP, DEBE deshacer la conexión TCP e intentar restablecerla antes de que se produzca la siguiente solicitud de asignación de puerta de dicho AN.

GATE-DELETE permite en ciertas circunstancias (véase las cláusulas siguientes) que un controlador de puerta suprima una puerta recién asignada.

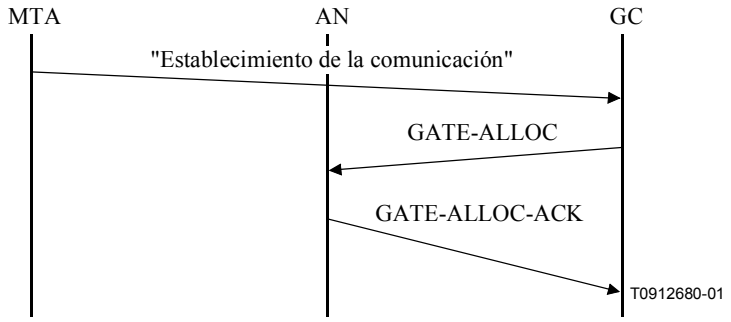
7.4.3 Procedimientos para la asignación de una nueva puerta

El controlador de puerta envía al AN un mensaje GATE-ALLOC al tiempo que se envía el mensaje establecimiento de la comunicación (*Call_Set-up*) desde el MTA de origen [por ejemplo, "mensaje invitación (etapa 1)" cuando se utiliza DCS], tal como se muestra en la figura 16.

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 AN compara el número de puertas actualmente asignadas al ID de abonado indicado con el campo cómputo del objeto cómputo de actividad del mensaje GATE-ALLOC. Si el número actual de puertas es mayor o igual al campo cómputo de GATE-ALLOC, el AN DEBE devolver un mensaje GATE-ALLOC-ERR. Si el número actual de puertas es mayor que el campo cómputo de GATE-ALLOC, es probable que el abonado haya sido reaprovisionado para tener un límite de puerta inferior que antes. En este caso, las sesiones actuales del abonado no se ven afectadas, pero el AN rechazará cualquier nueva sesión de dicho abonado hasta que el cómputo de sesiones del abonado sea inferior al valor especificado en el campo cómputo.

Si el objeto cómputo de actividad no está presente, el AN no realiza la verificación de límite de puerta. Un GC que desee reducir el tiempo de establecimiento de la comunicación PUEDE realizar la verificación de límite de puerta al recibir GATE-ALLOC-ACK en lugar de que sea el AN quien realice la verificación, de forma que el GC pueda realizar simultáneamente las opciones de asignación de puerta (GATE-ALLOC) y el análisis de la política de abonado. Cuando los resultados de ambas operaciones están disponibles, el GC puede realizar la verificación del límite de puerta. Si la verificación tiene resultado negativo, el GC DEBE enviar al AN un mensaje GATE-DELETE para suprimir la puerta que fue asignada incorrectamente (véase 7.4.6). El GC PUEDE incluir el objeto cómputo de actividad en subsiguientes mensajes GATE-ALLOC para dicho abonado una vez que la política se ha almacenado en una memoria intermedia.

El diagrama siguiente (véase la figura 16) es un ejemplo de la señalización GATE-ALLOC.



NOTA – Como ejemplo, el mensaje "Establecimiento de la comunicación" se refiere, en este contexto, a "invitación con/sin señal de llamada", cuando se utiliza el DCS.

Figura 16/J.163 – Ejemplo de señalización de asignación de puerta (GATE-ALLOC)

El AN DEBE responder al mensaje GATE-ALLOC con un GATE-ALLOC-ACK (que indica éxito) o con GATE-ALLOC-ERR (que indica fracaso). DEBE existir concordancia entre el ID de transacción de la respuesta y el ID de transacción de la petición.

En una respuesta GATE-ALLOC-ERR se informa de todos los errores habidos en la asignación de puertas. El objeto IPCablecomError contiene una los siguientes códigos de error:

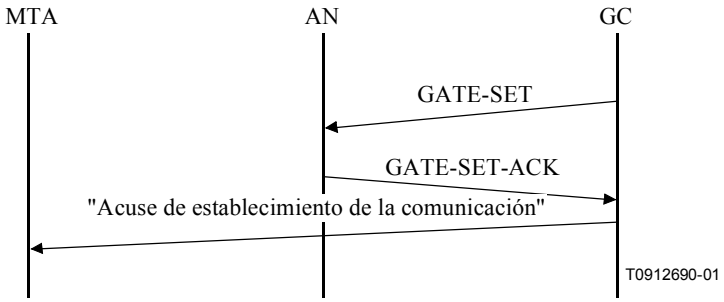
1 = No hay puertas disponibles en este momento.

4 = El abonado ha excedido el límite de puertas.

127 = Otros, error no especificado.

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

El controlador de puerta envía al AN el mensaje GATE-SET para inicializar o modificar los parámetros operacionales de la puerta o puertas. La figura 17 es un ejemplo de la señalización GATE-SET.



NOTA – Como ejemplo, el mensaje "Acuse de establecimiento de la comunicación" se refiere, en este contexto, al mensaje "200 OK" que se devuelve tras "invitación con/sin señal de llamada" cuando se utiliza el DCS.

Figura 17/J.163 – Ejemplo de señalización de establecimiento de puerta

Si en el mensaje GATE-SET existe un objeto ID de puerta, la petición consiste en modificar una puerta existente. Si el objeto ID de puerta no existe en el mensaje GATE-SET, se trata de una petición para asignar una nueva puerta, y el objeto cómputo de actividad PUEDE estar presente de forma que el AN determine si el abonado ha superado el numero máximo de puertas simultáneas.

El mensaje GATE-SET DEBE contener exactamente uno o dos objetos especificación de puerta, que pueden describir una o ninguna puerta ascendente, y una o ninguna puerta descendente.

El AN DEBE responder a un mensaje GATE-SET con GATE-SET-ACK (que indica éxito) o con GATE-SET-ERR (que indica fracaso). El ID de transacción de la respuesta DEBE 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 ilegal.

3 = Valor de clase de sesión ilegal.

4 = El abonado ha superado el límite de puertas.

127 = Otros, error no especificado.

Cuando el AN maneja una petición de reserva de un MTA, DEBE determinar la puerta adecuada utilizando el objeto RSVP ID de puerta, o mediante el TLV del bloque de autorización. El AN DEBE verificar que la petición de reserva se encuentra dentro de los límites autorizados especificados para la puerta.

El AN actualiza la petición de reserva en base a los parámetros de puerta. Si se fija la bandera compromiso automático, el AN DEBE tomar las acciones adecuadas en la capa MAC J.112 para comprometer inmediatamente los recursos. El AN DEBE fijar sobrescribir tipo-de-servicio-IP (*IP-Type-Of-Service-Overwrite*, TOS) mediante el parámetro punto de código DiffServ (DSCP, *Diffserv Code Point*).

El AN DEBE realizar una función de control de admisión en base a los parámetros de política facilitados y al valor de la clase de sesión de la puerta.

Nótese que, en lugar del mensaje GATE-ALLOC, puede utilizarse un mensaje GATE-SET para asignar (y establecer) una puerta. En tal caso, es posible que el número de puerta que utiliza la puerta distante para recibir mensajes de coordinación de puerta no esté disponible para el controlador de puerta. Si así es, el puerto AN del objeto información de puerta distante (incluido en el mensaje GATE-SET) se fija a cero. Ello hace que el AN ignore el número de coordinación de puerta. Sin embargo, cuando el controlador de puerta conoce (posteriormente) el número de puerta utilizado por la puerta distante, debe enviar otro mensaje GATE-SET (con el número de puerta que se incluye en el objeto) para informar al AN sobre dicho puerto.

7.4.5 Procedimientos para la interrogación de una puerta

Cuando un controlador de puerta desea determinar los valores de los parámetros de una puerta, envía al AN un mensaje GATE-INFO. El AN DEBE responder al mensaje GATE-INFO con un GATE-INFO-ACK (que indica éxito) o con GATE-INFO-ERR (que indica fracaso). El ID de transacción de la respuesta DEBE concordar con el ID de transacción de la petición.

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 ilegal.

127 = Otros, error no especificado.

7.4.6 Procedimientos para la supresión de una puerta

En un flujo de llamada normal, un AN 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 la capa MAC J.112 (desde un MTA integrado que no soporta RSVP). El AN también suprime una puerta cuando recibe un mensaje GATE-CLOSE desde un AN distante (modelo DCS) o desde un CMS (modelo NCS).

Normalmente, un controlador de puerta no inicia una operación de supresión de puerta. No obstante, pueden existir algunas situaciones anormales en las que un controlador de puerta puede desear suprimir una puerta del AN. Por ejemplo, si el controlador de puerta conoce (cuando recibe una respuesta GATE-ALLOC-ACK) que un abonado ha superado su límite de puertas, puede desear la supresión de la puerta recién asignada en el AN. En tal caso, PUEDE enviar al AN un mensaje GATE-DELETE (en lugar de permitir que venza la temporización de puerta). Pueden existir otras situaciones en las que puede ser útil la funcionalidad de supresión.

El AN DEBE responder a un mensaje GATE-DELETE con un GATE-DELETE-ACK (que indica éxito) o con GATE-DELETE-ERR (que indica fracaso). El ID de transacción de la respuesta DEBE 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 ilegal.

127 = Otros, error no especificado.

7.4.7 Secuencia de terminación

Cuando un AN cierra su conexión TCP con el GC, PUEDE enviar en primer lugar un mensaje DELETE-REQUEST-STATE (incluyendo el objeto asa utilizado en el mensaje REQUEST). El AN PUEDE enviar a continuación un mensaje CLIENT-CLOSE. Estos mensajes son opcionales porque el GC no tiene estados y porque el protocolo COPS requiere que el servidor COPS suprima automáticamente cualquier estado asociado con el AN cuando se elimina la conexión TCP.

Cuando el controlador de puerta se cierra, DEBERÍA enviar al AN un mensaje COPS cierre de cliente (CC). En el mensaje COPS CC, el controlador de puerta NO DEBERÍA enviar el objeto dirección de redireccionamiento PDP <PDPRedirAddr>. Si un AN recibe un mensaje COPS CC del controlador de puerta con un objeto <PDPRedirAddr>, el AN DEBE ignorarlo mientras procesa el mensaje COPS CC.

8 Interfaz de coordinación de puerta a puerta (pkt-q8)

Para sincronizar la utilización de las puertas, se intercambian mensajes entre ellas. Dichos mensajes incluyen GATE-OPEN (apertura de puerta), GATE-CLOSE (cierre de puerta) y sus correspondientes acuses de recibo. Los mensajes GATE-OPEN se intercambian cuando la puerta ha comprometido recursos activados o modificados como resultado de una instrucción del MTA (véase la figura 18). Los mensajes GATE-CLOSE se intercambian cuando dichos recursos se liberan. Los temporizadores implementados en la puerta imponen controles estrictos en relación con la duración de dichos intercambios.

Se pueden intercambiar mensajes de sincronización de puerta directamente entre los AN o a través de representantes [típicamente el sistema de gestión de llamadas (CMS, *call management system*) de IPCablecom, el cual recibe notificación de los casos de error que se producen en relación con cierres prematuros de puertas]. En la figura 18 se muestra la coordinación directa entre puertas y la figura 19 muestra la coordinación realizada a través de CMS representantes en ambos extremos. Aunque no se muestra, también son posibles configuraciones que tengan sólo un representante en uno de sus extremos.

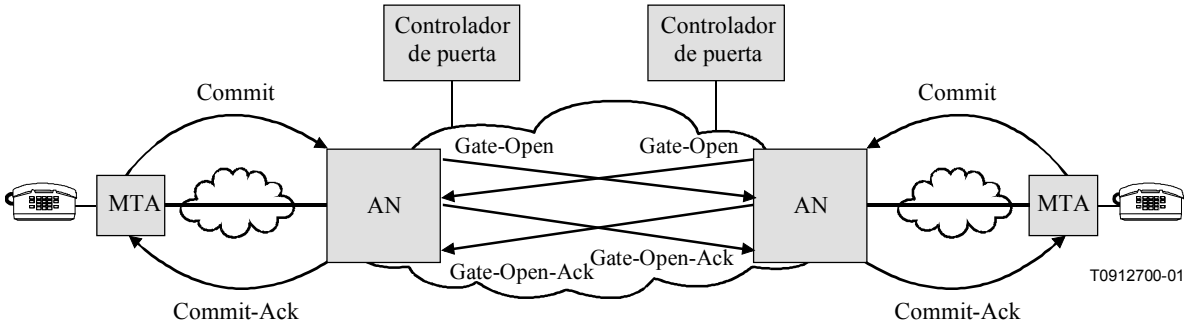


Figura 18/J.163 – Coordinación entre puertas extremo a extremo

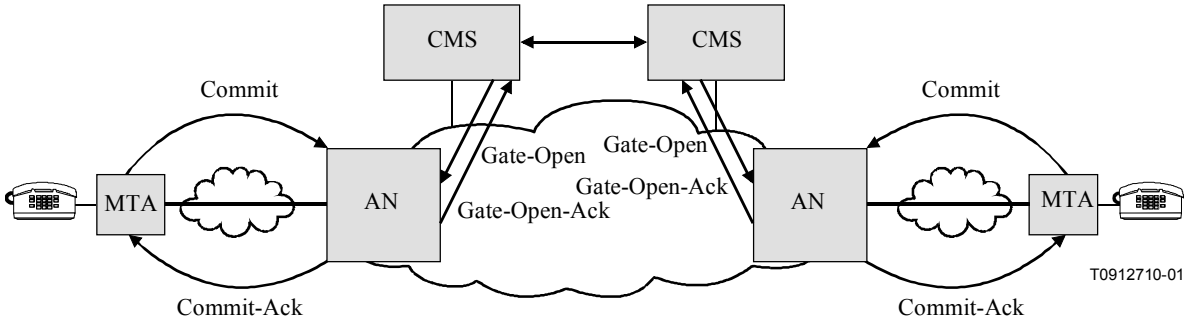


Figura 19/J.163 – Coordinación entre puertas con representante

Inicialmente una puerta se crea mediante una instrucción GATE-SET (establecer puerta) del controlador de puerta. La instrucción GATE-SET contiene información tal como los clasificadores prototipo (es decir, séxtuplas) y especificaciones de flujo para puertas locales y distantes. También contiene la dirección IP y el número de puerto de las AN distantes de forma que puedan realizar la coordinación de puerta a puerta.

8.1 Mensajes de protocolo de puerta a puerta

Los mensajes de protocolo de puerta a puerta se envían como paquetes UDP/IP, donde la instrucción GATE-SET incluye el puerto de destino UDP. El puerto de fuente UDP DEBE ser el puerto en el que el emisor queda a la espera de un acuse de recibo. En el campo de datos UDP debe encapsularse exactamente un mensaje. A continuación se muestra el formato de la cabecera común a todos los mensajes, que es idéntica a las especificaciones de RADIUS, de las cuales está copiada.

Tipo de mensaje	ID de transacción	Longitud del mensaje
Autenticador de mensaje (16 bytes)		
Parámetros ….		

El tipo de mensaje es un octeto e identifica el tipo de paquete. Los códigos de tipo de mensaje se asignan de la forma siguiente:

GATE-OPEN 48

GATE-OPEN-ACK 49

GATE-OPEN-ERR 50

GATE-CLOSE 51

GATE-CLOSE-ACK 52

GATE-CLOSE-ERR 53

ID de transacción es un octeto y permite establecer la correspondencia entre peticiones y respuestas.

Longitud del mensaje ocupa dos octetos e indica la longitud del mensaje incluyendo la cabecera y todos los parámetros.

Autenticador de mensaje es una suma de control MD5 de 16 bytes. Este valor se utiliza para autenticar la petición y la respuesta, y se basa en un secreto compartido entre los dos AN. El autenticador de mensaje incluido en los mensajes GATE-OPEN y GATE-CLOSE contiene una función de aleatorización unidireccional hash MD5 RFC 1321 del IETF calculada sobre un tren de octetos que consta de: tipo de mensaje + identificador de transacción + longitud del mensaje + 16 octetos cero + parámetros + secreto compartido. El autenticador de mensaje para mensajes GATE-OPEN-ACK, GATE-OPEN-ERR y GATE-CLOSE-ACK contiene una función de aleatorización unidireccional hash MD5 unidireccional calculada sobre un tren de octetos que consta de: tipo de mensaje + identificador de transacción + longitud del mensaje + autenticador de mensaje del mensaje de petición + parámetros de respuesta (si los hay) + secreto compartido. El valor resultante de 16 bytes de la función hash MD5 se almacena en el campo autenticador de mensaje del paquete. Este algoritmo de cálculo del autenticador del mensaje es idéntico al descrito en la RFC 2865 del IETF.

Los parámetros se codifican utilizando el estilo tipo-longitud-valor de la RFC 2865 RADIUS del IETF. Los parámetros transportan la petición específica y la información de indicación necesaria para conseguir la coordinación de puerta. El formato del parámetro DEBE ser el siguiente:

Tipo	Longitud	Reservado, DEBE ser cero
Valor ….		

El campo Tipo tiene un octeto y contiene los valores siguientes:

ID de puerta 224

Tspec 225

Tspec inversa 226

Código de error 227

El campo Longitud tiene un octeto y contiene la longitud del parámetro en bytes. Todos los valores de longitud de esta Recomendación son múltiplos de 4.

Cuando el parámetro ID de puerta está presente en un mensaje, tiene el formato siguiente:

224	8	0
Valor del ID de puerta (entero de 32 bits)		

Cuando el parámetro Tspec está presente en un mensaje, tiene el formato siguiente (véase la explicación de los campos en 6.3.1):

225	36	0
0 (a) Reservado		7 (b)
1 (c)	0 Reservado	6 (d)
127 (e)	0 (f)	5 (g)
Velocidad del contador de testigos [r] (número en coma flotante de 32 bits del IEEE)		
Tamaño del contador de testigos [b] (número en coma flotante de 32 bits del IEEE)		
Velocidad de cresta de datos [p] (número en coma flotante de 32 bits del IEEE)		
Unidad mínima sujeta a la política [m] (entero de 32 bits)		
Tamaño máximo de paquete [M] (entero de 32 bits)		

Cuando el parámetro Tspec inversa está presente en un mensaje, tiene el formato siguiente (véase la explicación de los campos en 6.3.5):

226	36	0
0 (a) Reservado		7 (b)
1 (c)	0 Reservado	6 (d)
127 (e)	0 (f)	5 (g)
Velocidad del contador de testigos [r] (número en coma flotante de 32 bits del IEEE)		
Tamaño del contador de testigos [b] (número en coma flotante de 32 bits del IEEE)		
Velocidad de cresta de datos [p] (número en coma flotante de 32 bits del IEEE)		
Unidad mínima sujeta a la política [m] (entero de 32 bits)		
Tamaño máximo de paquete [M] (entero de 32 bits)		

Cuando el parámetro Código de error está presente en un mensaje, tiene el formato siguiente:

227	4	Código de error	Reservado

Los valores de Código de error son los siguientes:

0 Liberación normal, iniciada por el MTA.

1 Cierre iniciado por el AN debido a la ausencia del mantenimiento de la reserva (por ejemplo, mensajes de refresco RSVP).

2 Cierre iniciado por el AN debido a la ausencia de respuestas de capa MAC J.112 (por ejemplo, mantenimiento de la estación).

3 Ha expirado el temporizador T1; no se recibe COMMIT del MTA.

4 Ha expirado el temporizador T2; fallo de coordinación de puerta

5 Cierre iniciado por el AN debido a reasignación de la reserva (por ejemplo, para sesión con prioridad).

6 Cierre iniciado por el AN debido a la falta de concordancia de la reserva.

129 ID de puerta ilegal.

130 Autenticador de mensaje incorrecto.

255 Otros, error no especificado.

8.1.1 GATE-OPEN (apertura de puerta)

El formato del mensaje GATE-OPEN (apertura de puerta) DEBE ser el siguiente:

<GATE-OPEN> ::= <RADIUS-Common-Header> <Gate-ID>
[<Tspec> <Reverse-Tspec>]

El valor del ID de puerta se copia del valor de ID de puerta distante contenido en el objeto información de puerta distante del mensaje establecimiento de puerta.

Cuando un AN genera un mensaje GATE-OPEN, DEBEN estar presentes los objetos Tspec y Tspec inverso.

Los valores del parámetro Tspec se copian del objeto especificación de flujo del mensaje COMMIT, si existe, y si no es así, del objeto Tspec del emisor del mensaje RSVP-PATH que ha iniciado la reserva, o bien, se genera a partir de los mensajes de capa MAC J.112 que han iniciado la operación de compromiso. En todos los casos, indica los recursos comprometidos en el sentido ascendente (directo).

Los valores del parámetro Tspec inversa se copian del objeto Tspec del emisor inversa del mensaje COMMIT, si éste existe, y si no, del objeto Tspec del emisor inversa del mensaje RSVP-PATH que ha iniciado la reserva, o bien, se genera a partir de los mensajes de capa MAC J.112 que han iniciado la operación de compromiso. En todos los casos, indica los recursos comprometidos en el sentido descendente (inverso).

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

El formato de un mensaje GATE-OPEN-ACK DEBE ser el siguiente:

<GATE-OPEN-ACK> ::= <RADIUS-Common-Header>

Este mensaje de acuse de recibo no tiene parámetros. El ID de transacción de la cabecera común sirve para que el receptor identifique el mensaje GATE-OPEN del que se acusa recibo.

8.1.3 GATE-OPEN-ERR (error de apertura de puerta)

El formato de un mensaje GATE-OPEN-ERR DEBE ser el siguiente:

<GATE-OPEN-ERR> ::= <RADIUS-Common-Header> <Error-code>

El ID de transacción de la cabecera común sirve para que el receptor identifique el mensaje GATE-OPEN del que se acusa recibo.

El parámetro Código de error contiene un código de motivo que indica la causa del error.

Si el error es tal que no se reconoce el ID de puerta y, por lo tanto, no se conoce la clave de autenticación adecuada, o si el autenticador de mensaje de GATE-OPEN es incorrecto, el autenticador de mensaje de GATE-OPEN-ERR DEBE ser una copia exacta del autenticador de mensaje de GATE-OPEN.

8.1.4 GATE-CLOSE (cierre de puerta)

El formato de un mensaje GATE-CLOSE DEBE ser el siguiente:

<GATE-CLOSE> ::= <RADIUS-Common-Header> <Gate-ID> [<Error-Code>]

Si el mensaje GATE-CLOSE se genera por una causa distinta a una petición de liberación normal del MTA, el parámetro código de error DEBE existir e indicar la causa del error.

Cuando no haya ninguna puerta abierta NO DEBE utilizarse GATE-CLOSE. Cuando no haya una puerta abierta o el CMS (cuando no actúa como representante del AN distante) solicite el cierre de una puerta, debe utilizarse el mensaje GATE-DELETE.

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

El formato de un mensaje GATE-CLOSE-ACK DEBE ser el siguiente:

<GATE-CLOSE-ACK> ::= <RADIUS-Common-Header>

El ID de transacción de la cabecera común sirve para que el receptor identifique el mensaje GATE-CLOSE del que se acusa recibo.

8.1.6 GATE-CLOSE-ERR (error de cierre de puerta)

El formato de un mensaje GATE-CLOSE-ERR DEBE ser el siguiente:

<GATE-CLOSE-ERR> ::= <RADIUS-Common-Header> <Error-String>

El ID de transacción de la cabecera común sirve para que el receptor identifique el mensaje GATE-CLOSE del que se acusa recibo. El autenticador de mensaje es una copia exacta del autenticador de mensaje de GATE-CLOSE.

8.2 Procedimientos de coordinación de puerta

Cuando el MTA realiza una operación compromiso (tal como se describe en 6.7 para cualquier MTA, o en los anexos A o B para MTA integrados), el AN DEBE enviar un mensaje GATE-OPEN. El mensaje GATE-OPEN DEBE contener las dos especificaciones de flujo (es decir, flujos bidireccionales). El AN DEBE retransmitir el mensaje GATE-OPEN, en base al temporizador T5, hasta la recepción de una respuesta GATE-OPEN-ACK. Después de un determinado número de intentos de retransmisión, el AN declara una pérdida de paquetes inaceptable y cierra la puerta.

Cuando se recibe un mensaje GATE-OPEN, el AN DEBE acusar recibo del mismo con un mensaje GATE-OPEN-ACK.

Si el AN recibe un mensaje GATE-OPEN, pero no tiene registro del ID de puerta, y por lo tanto no conoce la clave de seguridad adecuada, DEBE enviar GATE-OPEN-ERR con un autenticador de mensaje que concuerde con el autenticador de mensaje de GATE-OPEN.

El AN DEBE ignorar un autenticador de mensaje incorrecto cuando el tipo de mensaje sea GATE-OPEN-ERR, el ID de transacción concuerde con un mensaje GATE-OPEN pendiente enviado, y el autenticador de mensaje concuerde con el autenticador de mensaje de GATE-OPEN.

Cuando se produzca una petición de compromiso o cuando se reciba el mensaje GATE-OPEN, cualesquiera ocurra primero, el AN DEBE arrancar el temporizador T2.

Cuando se produzca una petición de compromiso o se reciba el mensaje GATE-OPEN, cualesquiera ocurra a continuación, el AN DEBE cancelar el temporizador T2. Si las especificaciones de flujo no concuerdan, el AN DEBE cerrar la puerta, iniciar la liberación del flujo J.112 y enviar un mensaje GATE-CLOSE.

Si el temporizador T2 expira después de la recepción de una petición de compromiso, sin que se haya recibido un mensaje GATE-OPEN, el AN DEBE cerrar la puerta, iniciar la liberación del flujo J.112 y enviar un mensaje GATE-CLOSE.

El AN DEBE enviar un mensaje GATE-CLOSE cuando reciba un mensaje de liberación explícito del cliente MTA (tal como se describe en 6.5.3 para cualquier MTA, o en los anexos A o B para MTA integrados), o cuando detecta que el cliente ya no genera activamente paquetes y no genera las señales de refresco adecuadas para el flujo asociado a una puerta. El AN también DEBE cerrar una puerta cuando reciba un mensaje GATE-CLOSE. Ello garantiza que las puertas asociadas con una sesión se cierran casi simultáneamente.

Cuando se recibe un mensaje GATE-CLOSE debidamente autentificado, el AN siempre DEBE responder enviando un GATE-CLOSE-ACK a la dirección que figura como dirección de fuente de la instrucción. Después de enviar el GATE-CLOSE-ACK, el AN DEBE mantener el ID de puerta y la clave de autenticación disponible durante al menos 30 segundos para permitir posibles retransmisiones del mensaje GATE-CLOSE.

Si el AN no tiene un registro del ID de puerta, y por lo tanto no conoce la clave de seguridad adecuada, DEBE enviar el GATE-CLOSE-ERR con un autenticador de mensaje que concuerde con el autenticador de mensaje de GATE-CLOSE.

El AN DEBE ignorar un autenticador de mensaje incorrecto cuando el tipo de mensaje sea GATE-CLOSE-ERR, el ID de transacción concuerde con un mensaje GATE-CLOSE pendiente enviado y el autenticador de mensaje concuerde con el autenticador de mensaje de GATE-CLOSE.

8.2.1 Ejemplo de procedimientos para la coordinación de puertas extremo a extremo

Para realizar la coordinación de puertas extremo a extremo, el controlador de puerta entrega a cada puerta la dirección y el ID de puerta del AN distante; cada AN envía y recibe los mensajes GATE-OPEN/GATE-CLOSE hacia y desde el otro.

Una vez que los MTA han completado su señalización de sesión, deben comenzar la sesión realizando una operación compromiso (como se describe en 6.7 para cualquier MTA o en los anexos A o B para MTA integrados) con el AN. Ello hace que el AN abra la puerta. El AN informa entonces al AN distante que la puerta está abierta. El AN local envía un mensaje GATE-OPEN al AN distante y arranca el temporizador T2 descrito en el anexo C. El mensaje GATE-OPEN contiene las dos especificaciones de flujo (es decir, se trata de flujos bidireccionales). El AN distante acusa recibo del mensaje GATE-OPEN con un mensaje GATE-OPEN-ACK.

Además, el AN espera recibir un mensaje GATE-OPEN del AN distante una vez que el MTA distante envía su mensaje COMMIT. Este mensaje GATE-OPEN distante desde el AN distante contiene igualmente las dos especificaciones de flujo. Estos parámetros de especificación de flujo se comparan con los del AN local. Si las especificaciones de flujo concuerdan, se permite que la puerta permanezca abierta.

Para deshabilitar el temporizador T2, se reciben sendos mensajes GATE-OPEN-ACK y GATE-OPEN del AN distante. Si no se recibe GATE-OPEN-ACK del AN distante antes de que venza el temporizador T5 (descrito en el anexo C y cuyo valor es del orden de un retardo de ida y vuelta), el AN retransmite el mensaje GATE-OPEN local para recuperarse de la pérdida. Este método de recuperación a nivel de aplicación se intenta mediante un número determinado de intentos de retransmisión, después de los cuales el AN declara una pérdida de paquetes inaceptable y cierra la puerta. El valor del temporizador T2 debe ser suficientemente grande para permitir la recuperación de los mensajes perdidos. Véase la figura 20.

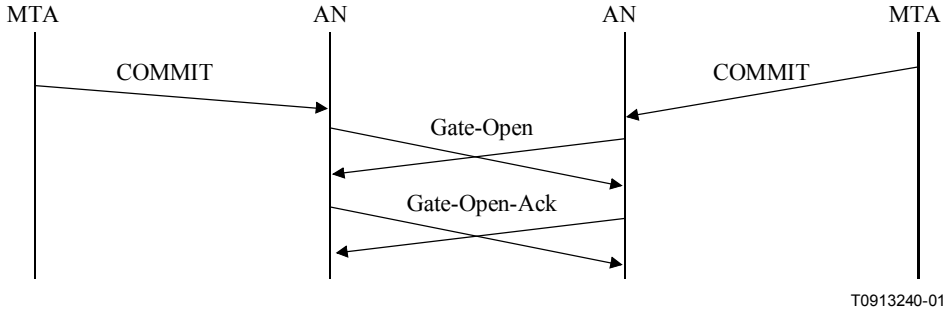


Figura 20/J.163 – Coordinación de puerta durante el mensaje COMMIT

La coordinación de puerta se realiza también mientras la puerta está cerrada. Cada AN envía a su AN par un mensaje GATE-CLOSE cuando recibe un mensaje de liberación explícito del MTA (tal como se describe en 6.5.3 para cualquier MTA, o en los anexos A o B para MTA integrados), o cuando detecta que el cliente ha dejado de generar activamente paquetes y no genera las señales de refresco adecuadas para el flujo asociado con una puerta. Un AN también cierra una puerta cuando recibe un mensaje GATE-CLOSE del AN distante. Esto garantiza que las puertas asociadas con una sesión se cierran casi simultáneamente. Véase la figura 21.

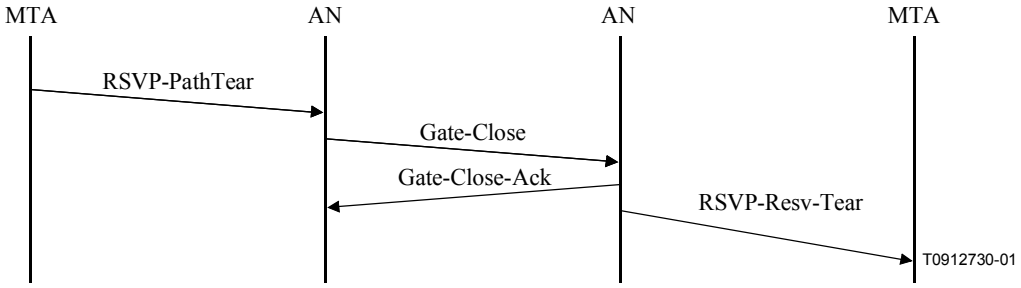


Figura 21/J.163 – Coordinación de puerta durante la liberación

Cuando se recibe un mensaje GATE-CLOSE debidamente autenticado, el AN responde con un GATE-CLOSE-ACK, que se envía a la dirección dada como dirección de fuente de la instrucción. Después de enviar el GATE-CLOSE-ACK, el AN mantiene el ID de puerta y la clave de autenticación disponible durante un periodo de al menos 30 segundos para permitir posibles retransmisiones del mensaje GATE-CLOSE.

8.2.2 Ejemplo de procedimientos para la coordinación de puertas que actúan con representantes

En este ejemplo se muestra cómo un sistema de gestión de llamada (CMS) puede actuar como representante en la coordinación de puertas. El controlador de puerta inicializa cada puerta considerando que la dirección del CMS es la entidad de coordinación distante y que un identificador elegido por el CMS es el ID de puerta. El AN realiza los procedimientos de coordinación de puerta enviando los mensajes GATE-OPEN/GATE-CLOSE al CMS, el cual los pasa a la puerta distante.

Cuando el CMS determina que existen recursos disponibles en el extremo de terminación (distante), ordena al MTA que comprometa recursos. También envía al AN un mensaje GATE-OPEN y arranca el temporizador T5. El AN acusa recibo del mensaje GATE-OPEN con un mensaje GATE_OPEN_ACK, que deshabilita al temporizador T5 en el CMS. Si la GATE_OPEN_ACK no se recibe del AN antes de que expire el temporizador T5, el CMS retransmite el mensaje GATE-OPEN para recuperarse de la pérdida. Este método de recuperación del mensaje a nivel de aplicación se sigue intentando mediante un determinado número de intentos de retransmisión, después de los cuales el CMS declara una pérdida de paquetes inaceptable y cierra la puerta. El valor del temporizador T2 debe ser suficientemente grande para permitir la recuperación de los mensajes perdidos. Cuando se recibe GATE-OPEN del CMS o el mensaje COMMIT del MTA, el AN arranca el temporizador T2.

Para deshabilitar el temporizador T2, el AN debe recibir con éxito un mensaje COMMIT del MTA y un mensaje GATE-OPEN del CMS. Si vence el temporizador T2, el AN inicia un mensaje GATE-CLOSE o un mensaje de capa MAC J.112 (según sea lo más adecuado) a fin de cerrar la puerta y liberar todos los recursos asociados a la misma. Véase la figura 22.

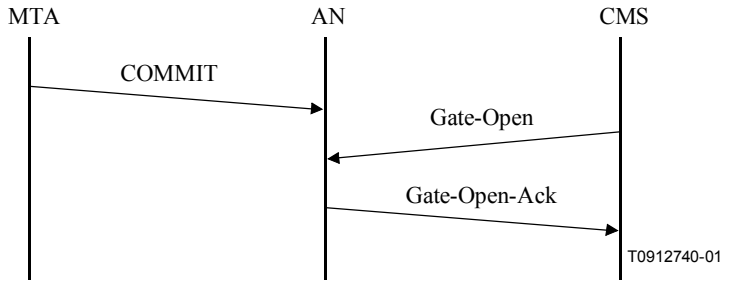


Figura 22/J.163 – Coordinación de puerta durante COMMIT

La coordinación de puerta se realiza cuando la puerta está cerrada. El AN envía un mensaje GATE-CLOSE a su CMS cuando recibe un mensaje de liberación explícita del MTA (tal como se describe en 6.5.3 para cualquier MTA, o en los anexos A o B para los MTA integrados), o cuando detecta que el cliente deja de generar activamente paquetes y no genera las señales de refresco adecuadas para el flujo asociado con una puerta. Un AN también cierra una puerta cuando recibe un mensaje GATE-CLOSE o GATE-DELETE del CMS. Ello garantiza que se cierran aquellas puertas asociadas con un MTA y que no responden.

Cuando se recibe un mensaje GATE-CLOSE debidamente autenticado, el CMS responde con un GATE-CLOSE-ACK, que se envía a la dirección presente en la dirección de fuente de la instrucción. Después de haber enviado GATE-CLOSE-ACK, el CMS mantiene el ID de puerta y la clave de autenticación disponible durante un periodo de al menos 30 segundos para posibles retransmisiones del mensaje GATE-CLOSE. Véase la figura 23.

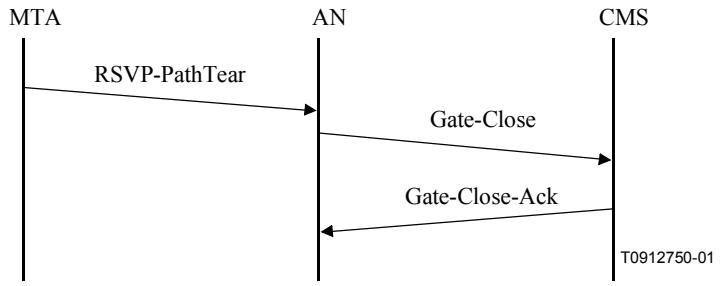


Figura 23/J.163 – Coordinación de puerta durante la liberación

ANEXO A

Requisitos adicionales para implementaciones conformes con el anexo A/J.112

En lugar de utilizar la interfaz pkt-q3 (RSVP+) para solicitar una determinada QoS en la red J.112 tal como se describe en la cláusula 6, un MTA integrado PUEDE reservar dinámicamente recursos de QoS locales utilizando mecanismos definidos en UIT-T J.112. Con este enfoque alternativo, un MTA integrado señaliza directamente su necesidad de QoS en la red de acceso local J.112 utilizando las primitivas MAC definidas en el anexo A/J.112. En contraposición a lo señalado en la cláusula 6, la señalización de QoS utilizando el protocolo MAC J.112 (pkt-q2) la inicia el cable-módem (CM) en lugar del AN a petición del MTA. En el mecanismo que se describe en la cláusula 6, el AN recibe la petición de QoS a través de la interfaz de capa 4 (pkt-q3), mientras que el mecanismo descrito en este anexo utiliza una interfaz de capa MAC (primitivas MAC) entre el MTA y el CM (pkt-q1). Todas las restantes interfaces y señales permanecen inalteradas. En los apéndices VII y VIII se muestran ejemplos ilustrativos de este enfoque.

Un MTA integrado recibe en su interfaz de capa de aplicación los requisitos de QoS para la sesión mediante los pertinentes protocolos de señalización (RFC 2543 del IETF y UIT-T J.162). Una vez que el MTA integrado determina la necesidad de reservar o comprometer recursos de QoS, DEBE iniciar la señalización J.112 para convertir los requisitos de QoS basados en la sesión de la aplicación, en una asignación de recursos basada en flujos J.112 en la red J.112, y la consiguiente creación, cambio y/o supresión de los flujos pertinentes. Tanto si la sesión la origina el MTA integrado, una entidad par o un nodo de red del equipo en las instalaciones del cliente (CPE), el MTA pasa los requisitos de QoS al protocolo MAC J.112 mediante primitivas MAC. Esto hace que se tomen las acciones adecuadas en la capa MAC para crear o modificar J.112 utilizando los mecanismos de los mensajes de establecimiento de la conexión y/o de gestión de enlaces del protocolo MAC J.112.

En las cláusulas siguientes se analiza la correspondencia que establece el MTA entre los requisitos de QoS basados en la sesión de la aplicación y los recursos necesarios en la red J.112, la utilización de primitivas MAC y la asignación de recursos en la red J.112 mediante las dos fases de reserva y compromiso.

A.1 Terminología

En una red que cumpla J.112, anexo A el terminal del lado de cliente puede estar formado por un cable-módem (CM) o un adaptador multimedios (STB, *set-top box*). Ambos dispositivos incorporan una unidad de interfaz de red (NIU, *network interface unit*) que proporciona la interfaz física y lógica entre la red J.112 y el CPE. El nodo de acceso (AN) se implementa, en ese caso, como un

adaptador de red interactivo (INA, *interactive network adapter*) que proporciona la interfaz con la red troncal y con elementos de la arquitectura IPCablecom que se establecen fuera de la red J.112, tal como el CMS y el RKS. Los flujos J.112 se consideran conexiones bidireccionales.

Dado que este anexo sólo se refiere a redes J.112 que satisfacen J.112/anexo A, los términos nodo de acceso (AN) y adaptador de red interactivo (INA) se utilizan indistintamente.

A.2 Correspondencia entre especificaciones de flujo y parámetros de QoS J.112

Un MTA integrado recibe los requisitos de QoS de una aplicación para cada sesión y debe de pasarlos al protocolo MAC J.112 utilizando primitivas MAC. Los requisitos de QoS se reciben en el formato de descripción de servicios de capa superior (por ejemplo, el SDP es utilizada en aplicaciones de VoIP) si el propio MTA inicia la sesión o en el formato de especificaciones de flujo RSVP si la sesión la inicia una entidad par o un nodo de red. Otras especificaciones (por ejemplo, la especificación J.161 del CODEC IPCablecom) definen la correspondencia entre las descripciones de servicios de capa superior y las especificaciones de flujo. En esta cláusula se especifica cómo el MTA DEBE establecer la correspondencia entre los requisitos de QoS y los parámetros de capa MAC J.112. En esta cláusula se supone que el protocolo de transporte utilizado es UDP. Si se utiliza otro protocolo de transporte, se aplican los pertinentes cambios sobre los parámetros MAC aquí definidos, así como en relación con la supresión de la cabecera.

En la red J.112, los recursos se asignan para cada conexión. Una conexión es un flujo de datos unidireccional entre el CM y el INA. La conexión incluye un flujo descendente y un flujo ascendente. Los recursos se reservan en ambos sentidos, ascendente y descendente, y se describen mediante un conjunto de parámetros que, en general, pueden diferir para cada sentido. El protocolo MAC J.112 define varios parámetros de QoS aplicables a los distintos modos de acceso de J.112 Anexo A. Por lo tanto, el MTA especifica en su petición qué parámetros de QoS se asocian con la correspondiente conexión en los sentidos ascendente y descendente.

Para solicitar un modo de acceso específico, el MTA PUEDE utilizar la información de la política que ofrece el operador de la red J.112 y las características de la fuente que se describen en los requisitos de QoS de la sesión. Sin embargo, la decisión final sobre qué recursos se asignan a una conexión particular la toma el INA y DEBE estar basada, asimismo, en la cantidad total de recursos disponibles.

A modo de ejemplo de la correspondencia que se establece entre una descripción de sesión y los parámetros de QoS J.112, considérese una aplicación de VoIP que utilice el códec de audio del G.729 Anexo E y la siguiente descripción SDP:

- c = IN IP4 192.168.73.10
- m = audio 3456 RTP/AVP 96
- a = rtpmap: 96 G729E/8000
- a = ptime: 10

donde "c" contiene la información de la conexión, "m" es el descriptor de los medios que deben transportarse en esta sesión y "a" describe atributos de la sesión. En esta sesión en particular, se incluye un "rtpmap" que especifica los parámetros del códec. El atributo "ptime" indica que un paquete representa 10 ms de audio. La descripción de la sesión y los parámetros MAC J.112 del sentido ascendente pueden hacerse corresponder de la forma siguiente:

- Acceso a velocidad constante.
- Anchura de banda solicitada de 240 células ATM cada 1200 ms (equivalente a 75 kbit/s).
- Asignación cíclica de dos intervalos cada 60 intervalos.

En el ejemplo anterior se supone que se utiliza DirectIP como método de encapsulado ascendente y que la velocidad de datos ascendente es de 3,088 Mbit/s. Cuando se calcula la anchura de banda solicitada, DEBE tenerse en cuenta la tara del método de encapsulado y cualquier tara de protocolo MAC J.112. Utilizando la supresión de cabecera puede potencialmente reducirse de forma significativa el tamaño de la PDU en el sentido ascendente, dependiendo de los campos de las cabeceras que puedan suprimirse.

Se utiliza un clasificador para los paquetes que llegan al CM o al INA se asignen a la conexión adecuada con el fin de garantizar que reciben la QoS pertinente. Para poder establecer un clasificador en ambos puntos de terminación de la red J.112, el MTA integrado puede incluir en su petición parámetros de vinculación de sesión. No obstante, el INA también puede recibir dichos parámetros de la puerta a través de la interfaz de la capa MAC J.112. Los parámetros de vinculación de sesión ascendente son los siguientes:

- Dirección de fuente: dirección IP del MTA.
- Puerto de fuente: número de puerto sobre el que el MTA enviará el tren de medios.
- Dirección de destino: dirección IP del extremo lejano de la conexión tal como se incluye en el parámetro "c" de la descripción SDP.
- Puerto de destino: número de puerto en el que el extremo lejano recibirá el tren de medios tal como se indica en el parámetro "m" de la descripción SDP.
- Protocolo: protocolo de transporte que debe utilizarse (UDP en el ejemplo anterior).

Los parámetros de vinculación de sesión descendente incluyen:

- Dirección de fuente: dirección IP del extremo lejano de la conexión tal como se incluye en el parámetro "c" de la descripción SDP.
- Puerto de fuente: número de puerto sobre el que el extremo lejano enviará el tren de medios; este parámetro no está disponible para el MTA y NO DEBERÍA ser especificado como parte del clasificador.
- Dirección de destino: dirección IP del MTA.
- Puerto de destino: número de puerto en el que el MTA recibirá el tren de medios.
- Protocolo: protocolo de transporte que debe utilizarse (UDP en el ejemplo anterior).

A.3 Utilización de primitivas MAC J.112

Una vez que el MTA integrado ha determinado que deben reservarse o comprometerse recursos de QoS, inicia la señalización J.112 apropiada mediante primitivas MAC. Las primitivas MAC se definen en el anexo A/J.112. En esta cláusula se describe la utilización de primitivas MAC.

La primitiva MAC_RESOURCE_REQ DEBE ser utilizada por el MTA integrado para señalizar una petición de creación, modificación y/o supresión de una conexión. El tipo de recurso que se solicita (incluyendo la petición para liberar los recursos reservados) se indica mediante el parámetro tipo de recurso (*Resource_Type*).

A.3.1 Reserva de recursos

El MTA inicia la reserva de recursos de QoS utilizando la primitiva MAC_RESOURCE_REQ con el parámetro Resource_Type puesto a 1, 2 o 4. El MTA debe incluir el ID de puerta como identificador de la conexión. En J.112/Anexo A figura una descripción más detallada de los parámetros de la primitiva MAC_RESOURCE_REQ. Si el CM recibe este mensaje, invoca la señalización MAC que da lugar al establecimiento de una nueva conexión. Confirma la recepción de la primitiva respondiendo con una primitiva MAC_RESOURCE_CNF. El INA verifica la autorización del MTA para solicitar recursos, así como la disponibilidad de los mismos. Si el INA detecta un ID de conexión que ya esté siendo utilizando como ID de puerta sin que exista la correspondiente conexión, ello indica que los recursos están reservados pero no están aún comprometidos. La

decisión final se realiza de conformidad con Admit_Bit del mensaje <MAC> petición de recurso. Si Admit_Bit está fijado, el INA NO DEBE comprometer aún los recursos. Si está a cero, el INA DEBE comprometer los recursos para la conexión si el control de admisión había tenido éxito. Si los recursos solicitados no están disponibles, se deniega la petición. El CM notifica al MTA el resultado de la petición de recursos con la primitiva MAC_CONNECT_IND o MAC_RESOURCE_DENIED_IND. En la figura A.1 se ilustra el proceso de reserva de recursos.

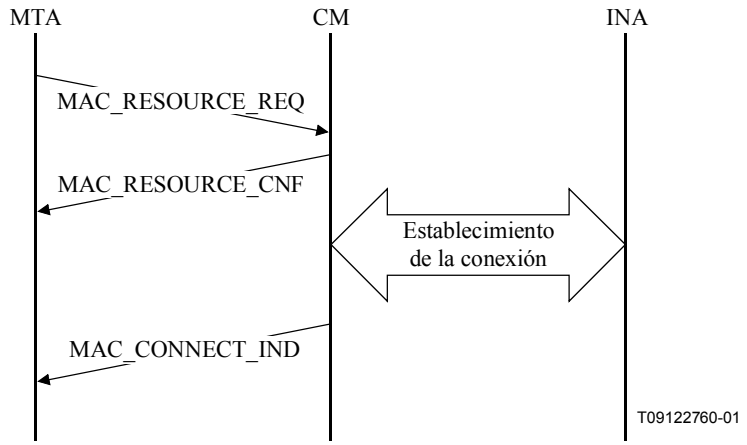


Figura A.1/J.163 – Reserva de recursos mediante primitivas MAC

A.3.2 Compromiso de recursos

El MTA inicia el compromiso de recursos de QoS mediante la primitiva MAC_RESOURCE_REQ cuyo parámetro Resource_Type se pone a 1 u 8. El MTA debe incluir el ID de puerta como ID de conexión. Véase en UIT-T J.112/Anexo A una descripción más detallada de los parámetros de la primitiva MAC_RESOURCE_REQ. Los recursos solicitados mediante este mensaje NO DEBEN ser superiores a los recursos reservados con una petición previa. Si el CM recibe este mensaje, invoca la señalización MAC que produce el reaprovisionamiento de la conexión existente. Confirma la recepción de la primitiva respondiendo con una primitiva MAC_RESOURCE_CNF. Si el INA detecta un ID de conexión que ya está siendo utilizado como ID de puerta en una conexión existente y el Admit_Bit del mensaje <MAC> de petición de recursos recibido a través del CM se pone a cero y los recursos quedan comprometidos. El INA NO DEBERÍA denegar lo solicitado si los recursos se encuentran dentro de la envolvente de reservas. El CM notifica al MTA el resultado de la petición de recursos mediante un MAC_CONNECT_IND o un MAC_RSV_ID_IND. En la figura A.2 se ilustra el proceso de compromiso de recursos.

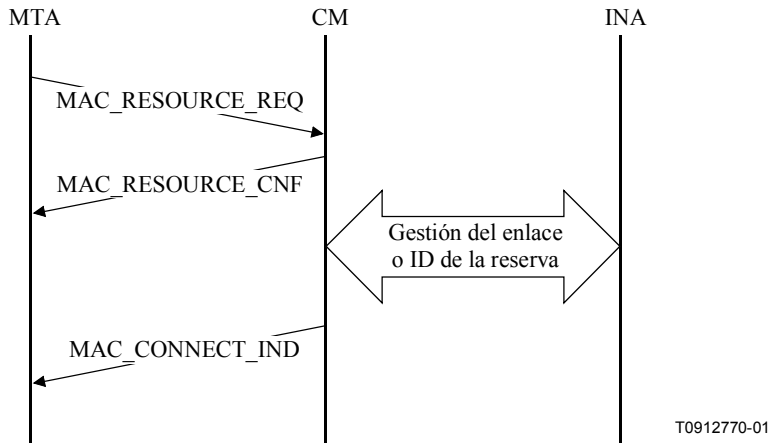


Figura A.2/J.163 – Compromiso de recursos utilizando primitivas MAC

A.3.3 Liberación de recursos

El MTA inicia la liberación de los recursos de QoS utilizando la primitiva MAC_RESOURCE_REQ cuya parámetro Resource_Type está puesto a 16. El MTA debe incluir el ID de puerta como ID de la conexión. En UIT-T J.112/Anexo A figura una descripción más detallada de los parámetros de la primitiva MAC_RESOURCE_REQ. Si el CM recibe este mensaje, invoca a la señalización MAC que da lugar a la supresión de la conexión y, por tanto, la liberación de los recursos asignados a dicha conexión. Confirma la recepción de la primitiva contestando con una primitiva MAC_RESOURCE_CNF. El CM notifica al MTA el resultado de la petición de recursos con MAC_RELEASE_IND. En la figura A.3 se ilustra el proceso de liberación de recursos.

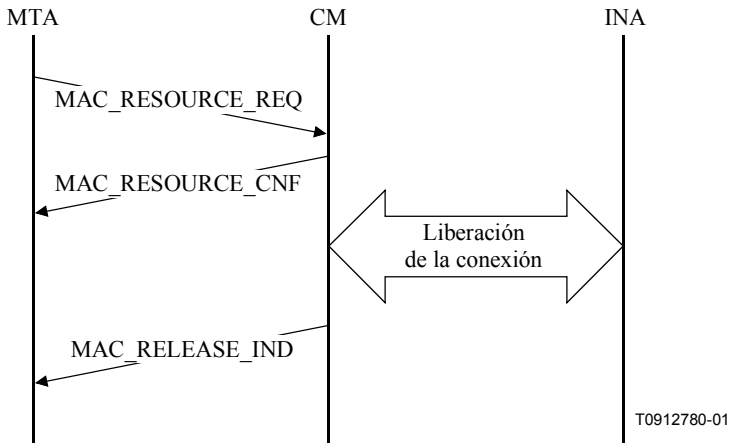


Figura A.3/J.163 – Liberación de recursos utilizando primitivas MAC

A.4 Soporte de la asignación de recursos en dos fases

Para que un servicio de comunicaciones vocales pueda desplegarse comercialmente, es esencial poder distinguir entre los recursos que están reservados para una sesión y los recursos comprometidos para la misma. Ello se debe, por una parte, a la necesidad de garantizar que todos los recursos están disponibles antes de que ambas partes reciban la notificación de que pueden comenzar su conversación. Por otro lado, porque una asignación de recursos en dos fases garantiza que el

registro y la facturación no comiencen hasta que los medios (es decir, el trayecto vocal) no estén dispuestos. En esta cláusula se describe cómo la red J.112 soporta este mecanismo de asignación de recursos.

Un flujo J.112 tiene tres conjuntos asociados de parámetros de QoS. El conjunto de parámetros autorizados viene definido por la política del operador de red y/o el proveedor de servicio y representa la máxima cantidad de recursos que pueden concederse a una sesión en particular. Los recursos se reservan bajo petición. Para comprometer estos recursos, ambas partes tienen que enviar una segunda petición explícita.

Ambos tipos de petición, la operación reserva y compromiso, se realizan mediante mensajes MAC J.112 que inicia el CM. La operación de reserva se lleva a cabo estableciendo una nueva conexión. La asignación y reserva de recursos tiene lugar en el INA. La operación compromiso utiliza el mecanismo de petición de recursos para una conexión existente establecido en el protocolo MAC J.112. En la figura A.4 se ilustra el intercambio de mensajes de las operaciones reserva y compromiso.

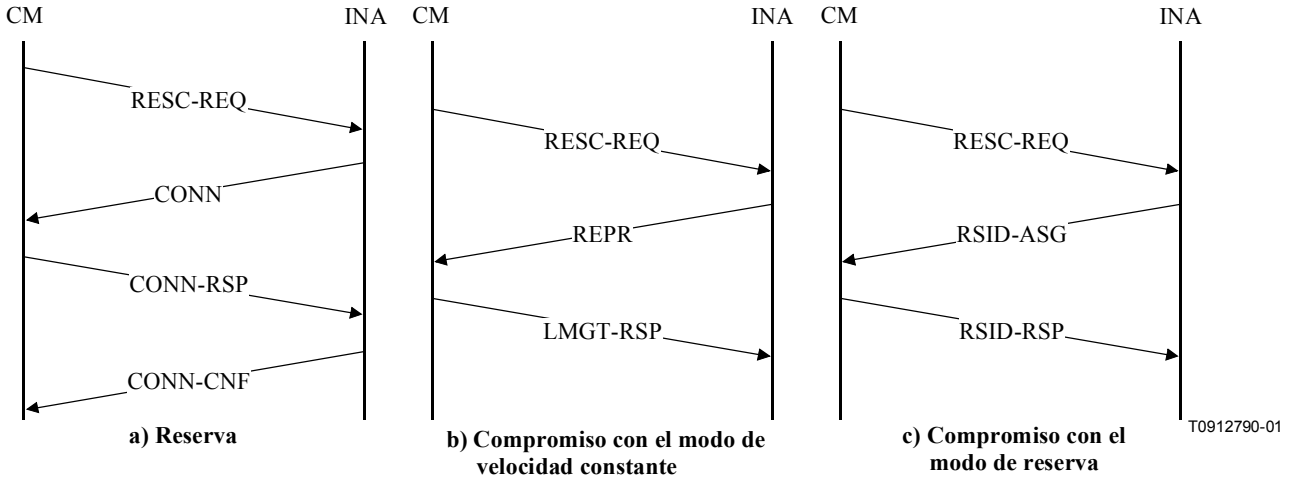


Figura A.4/J.163 – Operaciones de reserva y de compromiso mediante el intercambio de mensajes MAC de J.112/Anexo A

A título de ejemplo, el siguiente mensaje RESC-REQ (petición de recurso) hace que el INA establezca una conexión y que reserve los recursos en sentido ascendente y descendente de la red J.112. Su respuesta es el mensaje CONN (conexión) que se muestra a continuación.

RESC-REQ (Mensaje de petición de recurso)	
ID de petición de recursos	**0x01**
ID de conexión	**ID de puerta**
Campo	
Aux_control_field_included	1
Admit_flag	1
Priority_included	0
Max_packet_size_included	1
Session_binding_US_included	0
Release_requested	0
Reservation_ID_requested	0
Cyclic_assignment_needed	1

RESC-REQ (Mensaje de petición de recurso)	
Requested_bandwidth	240
Maximum_distance_between_slots	60
Encapsulation	DirectIP (1)
Aux_control_field	
IPv6_add	0
Flowspec_DS_included	1
Session_binding_DS_included	0
Frame_length	2
Flowspec_DS	
Max_packet_size	55
Average_bitrate	5 632
Jitter	0

CONN (mensaje de conexión)	
ID de conexión	**ID de puerta**
Session_number	**No es relevante**
Connection_Control_Field_Aux	
Connection_control_field2_included	1
IPv6_add	0
Priority_included	0
Flowspec_DS_included	0
Session_binding_US_included	0
Session_binding_DS_included	0
Encapsulation_included	1
DS_multiprotocol_CBD_included	0
Resource_number	**0x01**
Connection_Control_Field	
DS_ATM_CBD_included	0
DS_MPEG_CBD_included	1
US_ATM_CBD_included	1
Upstream_Channel_Number	0x1
Slot_list_included	0
Cyclic_assignment	0
Frame_Length	**0**
Maximum_Contention_Access_Message_Length	**1**
Maximum_Reservation_Access_Message_Length	**50**
Downstream_MPEG_CBD	
Downstream_Frequency	472 000 000
Program_Number	0xA437

RESC-REQ (Mensaje de petición de recurso)	
Upstream_ATM_CBD	
Upstream_Frequency	20 000 000
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Connection_control_field2	
Upstream_modulation_included	1
Upstream_Modulation	QPSK (1)

Suponiendo que la fuente de medios presenta un comportamiento de tipo CBR, lo más probable es que el MTA solicite una conexión con acceso a velocidad constante con el INA que previamente ha reservado los recursos necesarios. En este caso, tiene lugar el siguiente intercambio de mensajes RESC-REQ y REPR entre el CM y el INA a fin de comprometer recursos.

RESC-REQ (Mensaje petición de recursos)	
ID de la petición de recursos	**0x02**
ID de la conexión	**ID de puerta**
Campo	
Aux_control_field_included	1
Admit_flag	0
Priority_included	0
Max_packet_size_included	1
Session_binding_US_included	0
Release_requested	0
Reservation_ID_requested	0
Cyclic_assignment_needed	1
Requested_bandwidth	240
Maximum_distance_between_slots	60
Encapsulation	DirectIP (1)
Aux_control_field	
IPv6_add	0
Flowspec_DS_included	1
Session_binding_DS_included	0
Frame_length	2
Flowspec_DS	
Max_packet_size	55
Average_bitrate	5 632
Jitter	0

REPR (Reprovision Message)	
Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0
Delete_Reservation_Ids	0
New_Downstream_IB_Frequency_included	0
New_Downstream_OOB_Frequency_included	0
New_Upstream_Frequency_included	0
New_Frame_Length_included	1
New_Cyclical_Assignment_included	1
New_Slot_List_included	0

New_Frame_Length	**2**
Number_of_Connections	**1**
Connection_ID	**ID de puerta**
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_End	0xFFFF

A.5 Mantenimiento de la reserva

Queda en estudio.

ANEXO B

Requisitos adicionales para implementaciones conformes con J.112/Anexos B y C

En lugar de utilizar la interfaz pkt-q3 tal como se describe en la cláusula 6, un MTA integrado PUEDE reservar dinámicamente recursos de QoS locales utilizando exclusivamente los mecanismos definidos en UIT-T J.112. Utilizando este método alternativo, un MTA integrado señaliza directamente la QoS de acceso local utilizando la interfaz del servicio de control MAC que se define en los anexos E a B/J.112. En contraposición a lo indicado en la cláusula 6, es el CM y no el AN quien inicia la señalización de QoS a través de la interfaz J.112 (interfaz pkt-q2). Todas las restantes interfaces permanecen inalteradas. En los apéndices VII y VIII se presenta un ejemplo ilustrativo de este enfoque.

Un MTA integrado señaliza sus requisitos de QoS a nivel de sesión en los protocolos de señalización (SIP, RFC 2543 del IETF, y UIT-T J.162). Una vez que el MTA integrado determina que deben reservarse o comprometerse recursos de QoS, el MTA DEBE iniciar la señalización de flujo de servicio dinámico J.112 para crear, modificar y/o suprimir flujos de servicio y para la asignación de recursos J.112. Tanto si la sesión es iniciada por un MTA integrado, por un nodo par o por un nodo de red, el MTA pasa los requisitos de QoS al MAC J.112 a través de la interfaz del servicio de control MAC. Ello da lugar a la creación o modificación de los flujos de servicio necesarios para la sesión utilizando los mecanismos de mensajería de flujo de servicio dinámico J.112. En la cláusula siguiente se analiza la correspondencia que el MTA establece entre los requisitos de QoS a nivel de sesión y los de J.112, el soporte de J.112 de las dos fases de reserva y compromiso y la utilización de la interfaz del servicio de control MAC J.112.

B.1 Correspondencia entre especificaciones de flujo y parámetros de QoS J.112

Otras especificaciones (por ejemplo, la especificación J.161 del CODEC IPCablecom) incluyen requisitos de correspondencia o concordancia entre descripciones de servicio de alto nivel (por ejemplo, SDP utilizado en aplicaciones de VoIP) y especificaciones de flujo. En esta cláusula se especifican como DEBE establecer el MTA la correspondencia entre especificaciones de flujo y parámetros J.112 de capa 2. En esta Recomendación se asume que el protocolo de transporte utilizado es UDP. Si se utiliza un protocolo de transporte distinto, se deben aplicar los cambios adecuados en los clasificadores y para la supresión de la cabecera de la carga útil.

En UIT-T J.112 se define un conjunto abundante de parámetros de QoS, que en general pueden aplicarse a los flujos de servicio ascendente y descendente. Una codificación de flujo de servicio define el contenido del conjunto de parámetros de QoS aprovisionados, admitidos o activos para un flujo de servicio. Cada conjunto consta de múltiples parámetros de QoS que definen atributos individuales del flujo de servicio.

El MTA DEBE especificar:

- el servicio J.112 que debe utilizarse (por ejemplo, concesión no solicitada, sondeo en tiempo real, etc.),
- los parámetros de QoS que deben asociarse al correspondiente flujo de servicio.

La elección de la clase de servicio afectará tanto al retardo como a la eficiencia. Un servicio de concesión no solicitada introduce un retardo adicional no superior al tiempo existente entre concesiones. Un servicio basado en el sondeo tiene la potencialidad de introducir un mayor retardo dado que el CM espera un ciclo de sondeo para realizar la concesión.

Para decidir si se utiliza el mecanismo de concesión no solicitado o el mecanismo de sondeo en tiempo real, el MTA PUEDE utilizar información sobre la política y las características de la fuente descritas en los requisitos de QoS de la sesión. En general, sólo tiene sentido utilizar concesiones no solicitadas si el recurso tiene características de CBR con un paquete de longitud fija a intervalos regulares.

Para el servicio de concesión no solicitada (UGS, *unsolicited grant service*), el intervalo de la concesión puede fijarse de acuerdo con el tiempo de formación del paquete, aunque pueden utilizarse distintos valores dependiendo de los requisitos de retardo y fluctuación de fase.

Por ejemplo, considérese una aplicación de VoIP que utiliza G.729/Anexo E y el SDP siguiente:

c = IN IP4 10.1.1.10

m = audio 3456 RTP/AVP96

a = rtpmap:96 G729E/8000

a = ptime:10

donde rtpmap especifica los parámetros del códec, y ptime especifica un tiempo de formación de paquete de 10 ms. Puede establecerse una correspondencia entre dichos valores y parámetros de QoS de flujo de servicio ascendente de la forma siguiente:

– Servicio de concesión no solicitado.

– Tamaño de concesión de 86 bytes (55 bytes para el paquete IP, tal como indica la especificación de flujo y 31 bytes de tara de capa MAC J.112).

– Intervalo de concesión de 10 ms.

El tamaño de la PDU ascendente DEBE tener en cuenta la tara Ethernet (18 bytes) así como cualquier tara J.112 (típicamente de 6 a 13 bytes). La supresión de la cabecera de la carga útil puede reducir potencialmente el tamaño de la PDU en hasta 42 bytes, dependiendo de la utilización de la suma de control UDP y del campo de identificación IP, al que se añaden dos bytes de la cabecera ampliada J.112, lo que da el valor del índice PHS.

Si no se utiliza la suma de control del UDP y el campo identificación IP que se debe suprimir – se eliminan 40 bytes de la PDU.

Si se utiliza la suma de control del UDP y el campo identificación IP que se debe suprimir – se eliminan 38 bytes de la PDU.

Si no se utiliza la suma de control del UDP y el campo identificación IP no puede suprimirse – se eliminan 36 bytes de la PDU.

Si se utiliza la suma de control del UDP y el campo identificación IP no puede suprimirse – se eliminan 34 bytes de la PDU.

El clasificador ascendente DEBE fijarse de la forma siguiente. La dirección de fuente es la dirección IP del MTA. El puerto de fuente es el número de puerto por el que el MTA envía el tren de la señal de voz. La dirección de destino es la dirección IP de destino obtenida de c = line de la descripción SDP del extremo lejano. El puerto destino es el número de puerto obtenido de m = line de la descripción SDP del extremo lejano. El tipo de protocolo es UDP.

El clasificador descendente DEBE fijarse de acuerdo con los valores siguientes. La dirección fuente es la dirección IP del MTA distante, que se obtiene de c = line de la descripción SDP del extremo lejano. El puerto de fuente no está disponible en la descripción SDP, y NO DEBERÍA especificarse como parte del clasificador. La dirección de destino es la dirección IP del MTA. El puerto de destino es el puerto local por el que el MTA ha indicado que recibirá los paquetes de datos de la voz. El tipo de protocolo es UDP.

La máscara PHS ascendente DEBE fijarse de acuerdo con los valores a una cadena de bits, un bit para cada byte del paquete, correspondiendo el primer bit al primer byte de la cabecera Ethernet. Todos los bits DEBERÍAN fijarse a uno, a excepción de los bits correspondientes al campo identificación IP, campo suma de control IP y campo suma de control UDP, si dichos campos no pueden suprimirse.

El campo PHS ascendente DEBE fijarse de acuerdo con los valores de la cadena de bytes que el AN debe restaurar al comienzo de cada paquete, que consta del valor de la cabecera Ethernet, la cabecera IP y la cabecera UDP. Si los campos identificación IP, suma de control IP y suma de control UDP no se suprimen, DEBEN obviarse cuando se analice el campo PHS.

El tamaño de PHS descendente DEBERÍA fijarse en 32 bytes. Esta cantidad incluye el SA y el tipo de cabecera Ethernet (8 bytes), la cabecera IP completa (20 bytes), la longitud del paquete UDP y el puerto de destino (4 bytes). No se suprimen el puerto de fuente UDP, la suma de control UDP y la dirección de destino de la cabecera Ethernet.

La máscara PHS descendente DEBERÍA fijarse a 0xFFFFFFFF, indicando que se suprimen todos los bytes arriba señalados, comenzando después del DA Ethernet.

El campo PHS descendente DEBE fijarse de cuerdo con los valores de la cadena de bytes que el CM debe restaurar al comienzo de cada paquete, que consta del valor de la dirección de fuente Ethernet (PUEDE fijarse al valor de la dirección del AN, o PUEDE fijarse a cualquier otro valor que convenga al MTA), la cabecera IP, la longitud del paquete UDP y el valor del puerto de destino.

B.2 Soporte J.112 para reserva de recursos

En UIT-T J.112 no existe una forma definida de pasar información de autorización desde el CM al *módulo de autorización* del AN. El módulo de autorización es una función lógica del AN definida en UIT-T J.112. En esta Recomendación se utiliza una nueva codificación TLV (tipo/longitud/valor) J.112 que pasa al AN 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. La autorización de cada sesión utiliza un asa que se entrega tanto al AN como al MTA y sirve para hacer concordar peticiones con autorizaciones. Este asa es el ID de puerta. Cuando se recibe la información de señalización de llamada, el MTA pasa el ID de puerta al AN utilizando el TLV del bloque de autorización contenido en un mensaje DSA/DSC.

En los mensajes DSA-REQ que figuran en el apéndice VII figura un ejemplo de utilización del bloque de autorización.

B.2.1 Reserva/Compromiso de QoS en dos fases

Un flujo de servicio tiene tres conjuntos asociados de parámetros de calidad de servicio, denominados conjuntos de parámetros de QoS aprovisionados, admitidos o activos. La relación entre ellos es idéntica a la descripción de recursos autorizados, reservados o comprometidos de 5.7.4. Además, es una opción específica J.112 del vendedor soportar, para un único flujo de servicio, múltiples conjuntos de parámetros de QoS admitidos (*AdmittedQoSParameterSet*).

Las operaciones de reserva y compromiso se realizan mediante mensajes de servicio dinámicos J.112, cambiando los valores del AdmittedQoSParameterSet y del ActiveQoSParameterSet del flujo de servicio. En un mensaje adición de servicio dinámica (DSA, *dynamic service addition*) o cambio de servicio dinámico (DSC, *dynamic service change*), la reserva se realiza incluyendo en las codificaciones de flujo de servicio ascendente o descendente el TLV tipo de conjunto de parámetros de QoS (*QoSParameterSetType*) que toma el valor admitido (valor 2). Igualmente, el compromiso se realiza fijando el valor del QoSParameterSetType a activo (valor 4) o admitido+activo (valor 6).

Los intercambios de DSA y DSC entre el CM y el AN son una toma de contacto triple en el sentido de que constan de un mensaje de petición, seguido de una respuesta y un acuse de recibo. Esto se ilustra en la figura B.1.

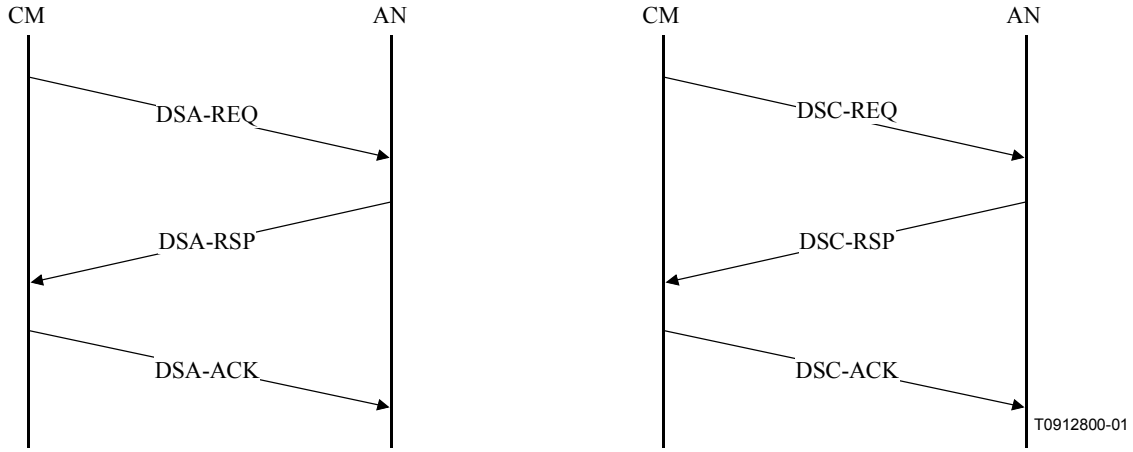


Figura B.1/J.163 – Intercambios DSA y DSC entre CM y AN

Por ejemplo, el mensaje siguiente hace que los flujos ascendentes y descendentes sean admitidos, lo cual significa que los recursos de QoS que se deben utilizar en la red J.112 están reservados.

DSA-REQ (petición de adición de servicio dinámica)

ID de transacción		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowReference	1
	QoSParameterSetType	Admitido (2)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	222
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowReference	2
	QoSParameterSetType	Admitido (2)
	TrafficPriority	3
	MaximumSustainedRate	12 000

En un ejemplo adicional, el mensaje DSC-REQ siguiente hace que el flujo de servicio quede activado, lo cual significa que los recursos de QoS utilizados en la red J.112 están comprometidos.

DSC-REQ (petición de cambio de servicio dinámico)

ID de transacción		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowID	10288
	QoSParameterSetType	Admitido + Activo (6)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	222
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowID	10289
	QoSParameterSetType	Admitido + Activo (6)
	TrafficPriority	3
	MaximumSustainedRate	12 000

Los parámetros tales como fluctuación de fase de concesión tolerada (*ToleratedGrantJitter*) y Prioridad de tráfico (*TrafficPriority*) PUEDEN ser suministrados mediante el proceso de aprovisionamiento o PUEDEN ser determinados mediante la implementación del MTA. Es previsible que la política del AN sustituya los valores propuestos por el MTA.

La especificación de los conjuntos de parámetros admitidos o activados por parte del MTA se realiza mediante las peticiones MAC_CREATE_SERVICE_FLOW y MAC_CHANGE_SERVICE_FLOW. Cuando el flujo de servicio se admite, tiene típicamente asociados uno o varios clasificadores. En el apéndice VII figuran ejemplos adicionales.

B.2.2 Reserva con múltiples especificaciones de flujo de servicio

Existen situaciones en las que una reserva debe abarcar una gama de posibles especificaciones. Por ejemplo, en algunas aplicaciones se desea disponer de una reserva que pueda manejar 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 que el conjunto de parámetros de QoS activos (*ActiveQoSParameterSet*) pueda variar durante una sesión, debe especificarse el pertinente valor de conjunto de parámetros de QoS autorizados (*AuthorizedQoSParameterSet*) mediante políticas en el controlador de puerta.

En el caso UIT-T J.112 es posible (como opción del vendedor) disponer de más de un conjunto de parámetros de QoS admitido. Por ejemplo:

DSA-REQ (petición de adición de servicio dinámica)

TransactionID		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowReference	1
	QoSParameterSetType	Admitido (2)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	111
UpstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowReference	1
	QoSParameterSetType	Admitido (2)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	20 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	444

Esto hace que el AN reserve recursos tales que cualquiera de los flujos descritos pueden ser ulteriormente activados, y que el AN no pueda devolver un error por "recursos insuficientes" durante el intento de activación. No obstante, el AN puede rechazar dicha petición de reserva mediante un 2-rechazo-valores-de-configuración-desconocidos. En ese caso, el MTA DEBE utilizar un enfoque de límite superior mínimo (LUB) para la reserva de recursos.

El límite superior mínimo de dos conjuntos de parámetros se forma tomando, para cada dimensión de la reserva de recursos, el recurso máximo que requiere cualquier especificación de flujo individual. Ello produce normalmente una sobreestimación de los recursos que necesitará el MTA, pero es lo mejor que puede lograrse con las facilidades disponibles. Utilizando las dos especificaciones de servicio del ejemplo anterior, un mensaje DSC-REQ que haya reservado recursos para ambos flujos pero que solo haya comprometido recursos para el primero de ellos sería:

DSC-REQ (petición de cambio dinámico de servicio)

TransactionID		1
Upstream Service Flow (Flujo de servicio ascendente)	ServiceFlowID	10288
	QoSParameterSetType	Admitido (2)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	444
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowID	10288
	QoSParameterSetType	Activo (4)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	111

En la primera especificación de flujo de servicio ascendente (*UpstreamServiceFlow*) el intervalo de concesión nominal (*NominalGrantInterval*) es de 10ms, máximo común divisor de las dos especificaciones de recursos, y el tamaño de concesión no solicitada (*UnsolicitedGrantSize*) es 444 bytes, el valor máximo de las dos especificaciones.

B.2.3 Mantenimiento de la reserva

Si bien el RSVP tiene un modelo de estado blando descrito en 6.5.4, UIT-T J.112 sólo proporciona un mecanismo de temporización a través de la interfaz J.112. Los parámetros de QoS del flujo de servicio "temporización para parámetros de QoS activos" (*TimeoutForActiveQoSParameters*) y "temporización para parámetros de QoS admitidos" (*TimeoutForAdmittedQoSParameters*) permiten terminar una sesión y liberar sus recursos por inactividad.

La temporización para parámetros de QoS activos tiene por objetivo recuperar recursos asignados a CM que hayan desaparecido, se hayan averiado o hayan perdido su conectividad a la red de cable. La transmisión normal de paquetes de datos en el flujo de servicio es suficiente para evitar esta acción de recuperación.

Si el MTA realiza la detección de actividad vocal (VAD) utilizando un tipo de programación de flujo de servicio UGS/AD, durante los periodos de silencio ampliados el MTA DEBE realizar una operación petición de cambio dinámico de servicio (DSC-REQ) para reinicializar el temporizador o bien, DEBE enviar paquetes de datos periódicos en el flujo de servicio. Alternativamente, si el MTA utiliza VAD PUEDE poner este temporizador a cero (es decir, no hay verificación).

Cuando termina una sesión, el AN envía el mensaje cierre de puerta con el código de error adecuado, tal como sed escribe en 8.2.

La temporización para parámetros de QoS admitidos tiene por objeto recuperar recursos que hayan sido reservados pero no comprometidos por el CM. En casos típicos, los parámetros comprometidos son idénticos a los parámetros reservados, lo cual no constituye un problema. Cuando la reserva incluye especificaciones de múltiples flujos de servicio, tal como se describe en B.2.2, o cuando el compromiso es inferior a la reserva, es necesario reinicializar periódicamente el temporizador del AN. Esto se realiza mediante una operación DSC-REQ que reserva los mismos recursos que anteriormente.

B.2.4 Soporte de la vinculación dinámica de recursos

La vinculación dinámica de recursos, tal como se requiere en 5.7.7 y se describe en 6.1.4, se realiza en UIT-T J.112 mediante la utilización de mensajes cambio dinámico de servicio en un flujo de servicio establecido, modificando los clasificadores asociados al flujo de servicio.

B.2.5 Concordancia de parámetros de QoS para la autorización

La puerta que identifica al ID de puerta se parametriza mediante objetos RSVP (especificación de flujo). El módulo de autorización del AN DEBE convertir el parámetro puerta en parámetros de QoS J.112 utilizando las reglas definidas en B.3.4 y 7.1. Los objetos de QoS J.112 resultantes DEBEN verificarse en relación con las correspondientes envolventes de QoS del flujo de servicio.

Por ejemplo, si la autorización ascendente viene dada por:

Profundidad del contador (b) = 120 bytes

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

Velocidad de cresta (p) = 12 000 bytes/segundo

Unidad mínima sujeta a la política (m) = 120 bytes

Tamaño máximo del datagrama (M) = 120 bytes

La autorización se convierte en parámetros de QoS J.112:

Programación: UGS

Intervalo de concesión nominal: 10 ms

Fluctuación de fase tolerada de la concesión: 5 ms

Tamaño de concesión no solicitada: 151 bytes

Estos objetos J.112 convertidos se comparan con la envolvente de recursos del correspondiente flujo de servicio.

B.2.6 Recursos comprometidos automáticamente

Si la puerta individual se ha marcado con la bandera "compromiso automático" (véase 7.3.2.5) los recursos reservados se activan automáticamente, pero el estado de la puerta no se modifica.

Si un MTA integrado sin capacidad RSVP que inicia la reserva de recursos con un mensaje DSA-REQ J.112, el AN DEBE iniciar un intercambio DSC-REQ J.112 con el MTA tan pronto se complete la reserva, con un tipo de conjunto de parámetros de QoS (*QoSParameterSetType*) de admitido + activo (valor 6) para el flujo de servicio que se compromete. En el apéndice VIII se incluye un ejemplo.

B.3 Utilización de la interfaz de servicio de control MAC J.112

Los parámetros de QoS J.112 del flujo de servicio que se derivan de la descripción SDP se señalizan para establecer el flujo o flujos de servicio. En esta cláusula se describe como puede realizarse esto utilizando las interfaces de servicio de control MAC J.112 (anexo E a anexo B/J.112).

En el ámbito de las primitivas de la interfaz del servicio de control MAC J.112, el MTA integrado señaliza los recursos de QoS de la forma siguiente:

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 admitidos y activos del flujo de servicio. El éxito o fracaso de esta primitiva se indica mediante la primitiva respuesta.MAC_CREATE_SERVICE_FLOW.

2) Petición.MAC_CHANGE_SERVICE_FLOW:

   Mediante esta primitiva el MTA integrado puede iniciar un cambio en los conjuntos de parámetros de QoS admitidos y activos. Un posible escenario corresponde al caso en que se retiene al llamado. El éxito o fracaso de la primitiva se indica mediante la primitiva 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 admitidos y activos del flujo de servicio.

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

B.3.1 Establecimiento de la reserva

El MTA inicia la reserva de recursos de QoS mediante la primitiva petición.MAC_CREATE_SERVICE_FLOW. El MTA debe incluir el ID de puerta en el TLV bloque de autorización. Cuando se recibe este mensaje, la capa MAC del CM invoca la señalización DSA enviando al AN una DSA_REQ. El AN DEBE verificar la autorización basada en la ID de puerta (contenida en el TLV del bloque de autorización), y rechazar la petición si la puerta es no

válida o los recursos autorizados son insuficientes para la petición. Cuando se recibe DSA_RSP del AN, el servicio MAC informa de ello a la capa superior utilizando el mensaje respuesta.MAC_CREATE_SERVICE_FLOW. Esto se ilustra en la figura B.1.

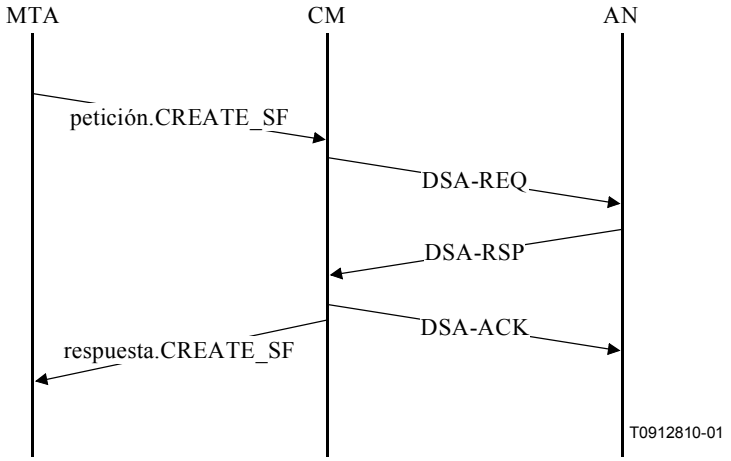


Figura B.1/J.163 – Establecimiento de la reserva

B.3.2 Cambio de la reserva

El MTA inicia cambios en los recursos de QoS utilizando la primitiva petición.MAC_CHANGE_SERVICE_FLOW. Esto se ilustra en la figura B.2.

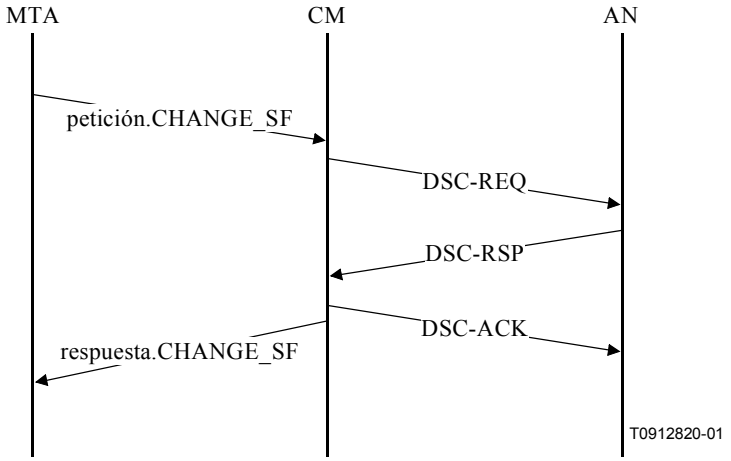


Figura B.2/J.163 – Cambio de la reserva

Cuando se recibe este mensaje, la capa MAC del CM invoca la señalización DSC. Cuando se recibe DSC_RSP del AN, el servicio MAC informa a la capa superior mediante el mensaje respuesta.MAC_CHANGE_SERVICE_FLOW.

B.3.3 Supresión de la reserva

El MTA inicia la desasignación de una reserva de QoS mediante la primitiva petición.MAC_DELETE_SERVICE_FLOW. Cuando se recibe este mensaje, la capa MAC invoca la señalización DSD. Cuando se recibe DSD_RSP del AN, el servicio MAC informa de ello a la capa superior mediante el mensaje respuesta.MAC_DELETE_SERVICE_FLOW. Esto se ilustra en la en la figura B.3.

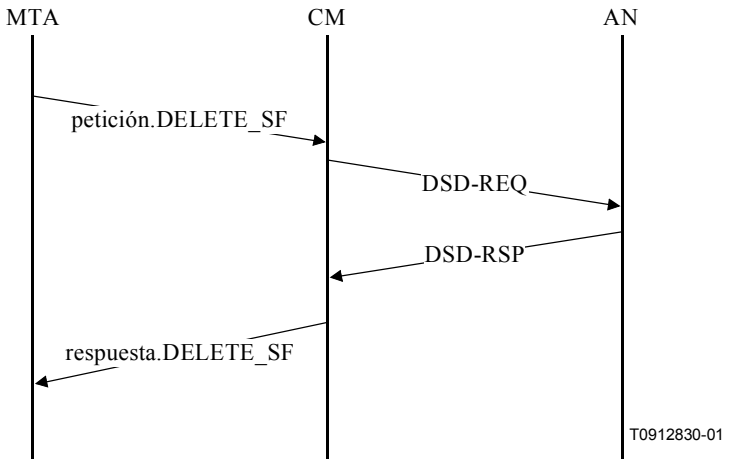


Figura B.3/J.163 – Supresión de la reserva

B.3.4 Correspondencia entre especificaciones de flujo RSVP y parámetros de QoS J.112

Cuando el AN recibe una petición de reserva decide:

- El tipo de servicio J.112 que se debe utilizar (por ejemplo, concesión no solicitada, sondeo en tiempo real, etc.)
- El tipo de parámetros de QoS que se deben asociar con el correspondiente flujo de servicio.

La elección de la clase de servicio afecta al retardo y a la eficiencia. Un servicio de concesión no solicitada introduce un retardo adicional no superior al tiempo entre concesiones. Un servicio de sondeo puede introducir potencialmente un retardo superior ya que el CM espera un ciclo de sondeo para realizar una concesión.

Para decidir si se utiliza el mecanismo de concesión no solicitada o el mecanismo de sondeo en tiempo real, el AN PUEDE utilizar información sobre la política y las características de la fuente descritas en Tspec. En general, sólo tiene sentido utilizar concesiones nos solicitadas si la fuente presenta características del tipo CBR con un tamaño fijo de paquete una vez durante cada intervalo de tiempo fijo. Dicha fuente CBR puede identificarse por el hecho de tener una velocidad de cresta (p) casi igual a la velocidad media (r) en Tspec de emisor, y un tamaño de ráfaga (b) igual al tamaño máximo de paquete (M). Antes de utilizar un modo de concesión no solicitada puede utilizarse información sobre la política para determinar cuánto se acerca p a r y b a M.

En el caso de fuentes del tipo VBR que funcionan a ráfagas, se produce una velocidad de cresta (p) "velocidad media (r) y b" M en el Tspec, y DEBERÍA utilizarse el modo de sondeo en tiempo real.

Para fuentes de VoIP descritas en esta Recomendación, con p = r y M = b, se DEBERÍA utilizar el servicio de concesión no solicitada (UGS).

Una vez que el AN ha elegido un mecanismo de planificación, PUEDE proporcionar información a su vecino RSVP en la forma de una AdSpec. La AdSpec permite al AN indicar en qué medida su comportamiento se desvía del "ideal", es decir, la cantidad de retardo adicional que puede introducir. Este retardo consta de dos partes:

- Una componente fija, por ejemplo, el retardo que puede introducirse mientras se procesa una actualización de encaminamiento, retardos de propagación, etc. (representado como D en la fórmula de retardo anterior).
- Una componente que depende de la velocidad, por ejemplo, debido al intervalo entre concesiones, que disminuye conforme aumenta la velocidad de reserva (representado por C en la fórmula anterior).

El AN PUEDE determinar ambas componentes de retardo en función de si el Tspec de emisor ha elegido un servicio por sondeo o de concesión no solicitada. En el caso de la componente que es función de la velocidad, el AN utiliza el máximo tamaño de datagrama (M) y la velocidad reservada (r) para determinar C. Por ejemplo, si un AN instala una reserva de velocidad de R bytes/segundo, podría realizar una concesión no solicitada con un tamaño de M bytes cada M/R segundos. Por lo tanto, el valor anunciado de C sería M. Si se utiliza un servicio de sondeo en tiempo real, el AN DEBE determinar cuánto tardaría un paquete situado en la cola del CM en recibir una concesión, dado el intervalo de sondeo que se utilizará, los retardos de los enlaces, etc. Dichos factores pueden tener componentes fijas y dependientes de la velocidad que el AN DEBERÍA anunciar consecuentemente.

Para fijar el intervalo de concesión nominal, el AN DEBE utilizar el parámetro velocidad incluido en Rspec (R) y el tamaño máximo de datagrama M. Tal como se ha indicado anteriormente, un intervalo de concesión de M/R proporcionará la velocidad de reserva adecuada. Sin embargo, si el término de inactividad permite introducir un retardo adicional, el AN PUEDE ofrecer concesiones más grandes con una menor frecuencia, por ejemplo, una concesión de 2M bytes cada 2M/R segundos.

En el caso del servicio de concesión no solicitada, el AN DEBE utilizar el "tamaño máximo de datagrama (M)" de la Tspec expresado en bytes a fin de calcular el tamaño de concesión no solicitada en mini intervalos (después de calcular la tara a nivel de enlace) para el canal ascendente en el que se encuentra el cliente llamante.

El otro parámetro clave necesario para el flujo de servicio UGS es la fluctuación de fase admisible de la concesión. Un cliente que precise una fluctuación de fase menos exigente que la correspondiente al mejor caso, PUEDE seleccionar un valor distinto de cero para el término de inactividad S, que da al AN margen adicional para aumentar la fluctuación de fase si ello fuera necesario. En B.3.4.1 se presenta un ejemplo de cálculo de fluctuación de fase.

Para el servicio de sondeo en tiempo real, el intervalo de sondeo PUEDE ser función de la velocidad, o bien, PUEDE ser fijo. Por ejemplo, un intervalo de sondeo de M/R permitiría al CM enviar un paquete de tamaño máximo cada intervalo de sondeo a fin de mantener su velocidad media. PUEDEN utilizarse intervalos de sondeo más largos o más cortos, pero sin que ello afecte al retardo total.

AdSpec PUEDE utilizarse para transportar información sobre el retardo de codificación que introduce el códec del transmisor. Se incluiría en el término D, y el AN DEBE añadir sus propias componentes de retardo al AdSpec en el cálculo de la tolerancia a un aumento de la fluctuación de fase.

El AN utiliza el objeto sesión y la plantilla del emisor para generar el clasificador ascendente y utiliza el objeto de sesión inversa y la plantilla de transmisor inverso para generar el clasificador descendente.

B.3.4.1 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 carga útil de 80 bytes cada 10 ms. La carga útil se encapsula utilizando RTP/UDP/IP, un extra de 40 bytes, dando lugar a un paquete de 120 bytes cada 10 ms. En este caso, Tspec es el siguiente:

Profundidad del contador (b) = 120 bytes

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

Velocidad de cresta (p) = 12 000 bytes/ segundo

Unidad mínima sujeta a la política (m) = 120 bytes

Tamaño máximo de datagrama (M) = 120 bytes

Supóngase que un cliente solicita una reserva utilizando este Tspec y un Rspec con R = r. Un AN que reciba esta petición establecerá un flujo de servicio que utilice el servicio de concesión no solicitada porque p = r y M = b, indicando que se trata de un flujo CBR. Puede utilizar un tamaño de concesión de M bytes a intervalos de M/R = 10ms.

Para calcular la fluctuación de fase, el MTA no conoce cuanto se desvía el AN en su planificación de los que sería el comportamiento ideal. El cliente debería asumir que el AN es ideal, lo cual significa que el retardo que experimentará con el TSpec anterior y su velocidad reservada R = r es simplemente:

b/r + retardos de propagación

Ignorar el retardo de propagación da lugar a un retardo de 10 ms. Supóngase que el cliente está dispuesto a tolerar un retardo de 15 ms para esta sesión (solamente en el trayecto cliente-AN). Ello hace que el término de inactividad (S) tome un valor de 15−10 = 5 ms. Cuando se recibe la reserva, el AN interpreta esto como una indicación de que el cliente acepta una fluctuación de fase 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 AN puede utilizar esta información para determinar que puede utilizar un intervalo de concesión superior, por ejemplo, 20 ms, dado que con ello se aumenta potencialmente el retardo hasta un valor de 20 ms para un paquete que llegue al CM inmediatamente después de una concesión. Existe aún un margen de inactividad de 5 ms, que el AN puede utilizar para fijar la fluctuación de fase de la concesión.

Nótese que este enfoque otorga una considerable flexibilidad al AN para cumplir los requisitos del cliente en lo relativo al retardo que mejor se adapte a las capacidades del AN.

B.3.4.2 Supresión de la cabecera de la carga útil y detección de la actividad vocal

Si el AN y el CM suprimen la cabecera, puede reducirse la anchura de banda necesaria para un flujo de servicio. El cliente DEBE hacer llegar al AN que la supresión puede aplicarse antes de realizar una reserva para asegurar que se reserva la anchura de banda adecuada. La solución general a este problema se describe en draft-davie-intserv-compress-00. El emisor (cliente) añade a la Tspec del emisor un parámetro indicación de compresión, descrito en *Servicios integrados en presencia de flujos comprimibles*, que identifica el tipo de compresión o supresión de cabecera que puede aplicarse a los datos. El parámetro Compression_Hint contiene un campo indicación que informa del tipo o tipos de compresión que son posibles.

Un MTA que quiera que el CM suprima la cabecera DEBE incluir en la Tspec el parámetro Compression_Hint, *servicios integrados en presencia de flujos comprimibles*. Al campo factor de compresión, que es un porcentaje en la gama de 1 a 100, DEBE darse una valor tal que permita ahorrar anchura de banda cuando se utilice la supresión de la cabecera el paquetes (42 bytes). El valor del factor de compresión varía en relación con el perfil de tráfico del CODEC. La indicación DEBE tomar uno de los valores siguientes dependiendo del tipo o tipos de compresión/supresión que desee el MTA:

0x????0001 No se suprime la suma de control del UDP Y no se suprime el campo identificación IP ni el campo suma de control IP.

0x????0002 No se suprime la suma de control del UDP Y se suprimen los campos identificación IP y suma de control IP.

0x????0003 Se suprime la suma de control del UDP Y no se suprime el campo identificación IP ni el campo suma de control IP.

0x????0004 Se suprime la suma de control del UDP Y se suprimen los campos identificación IP y suma de control IP.

NOTA – ???? = número IANA por determinar para IPCablecom).

Nótese 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 Internet de MAX-MTU), es razonable asumir que no se producirá fragmentación. El MTA NO DEBERÍA solicitar la supresión del campo identificación IP si va a enviar paquetes de longitud superior a 576 bytes.

Un AN que esté conectado a un CM que sea capaz de realizar la supresión de la cabecera, utiliza el parámetro Compression_Hint [*servicios integrados en presencia de flujos comprimibles*] para reducir la velocidad efectiva y la profundidad 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 suprime la cabecera en un enlace J.112, también es necesario comunicar al AN el contenido de la cabecera que va a ser suprimida antes de la transmisión del primer paquete de datos, de forma que en el CM y en el AN pueda establecerse el contexto de supresión. 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 (trayecto) se procesan en los tramos intermedios entre el cliente y el AN, un mensaje PATH que llegue contendrá el mismo valor de tiempo para vivir (TTL, *time to live*) que los paquetes de datos, siempre que los mensajes PATH y los paquetes de datos tengan el mismo TTL inicial cuando son enviados por el cliente. El AN DEBE utilizar el contenido de PATH para conocer los valores de los campos que serán suprimidos. El AN DEBE utilizar mensajes MAC J.112 para hacer llegar al CM el hecho de que la supresión se debe utilizar para un flujo en concreto, y para instruirle en la supresión de los campos pertinentes 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 un emisor con libertad de elección, no puede determinarse con exactitud el contenido del campo PHS. El AN DEBE especificar el tamaño de PHS de forma que el CM pueda evaluar con precisión las necesidades de recursos del flujo de servicio.

El mismo enfoque básico permite soportar la detección de actividad vocal (VAD). Un AN puede utilizar diferentes algoritmos de programación para flujos que utilicen VAD y, por lo tanto, necesita saber qué flujos deben tratarse con VAD. El parámetro indicación de compresión incluido en la Tspec DEBE contener el bit bandera que indica que el flujo de datos para el que se ha solicitado esta reserva puede ser tratado con VAD.

ANEXO C

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 estado de la puerta del AN y limita el tiempo que una puerta puede estar asignada sin que se fijen los parámetros de la misma. Ello permite al AN 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.

Este temporizador se reinicia cuando se fijan los parámetros de la puerta.

Cuando este temporizador vence, el AN DEBE considerar que el ID de puerta asignado es no válido.

El valor RECOMENDADO de este temporizador es de 30 segundos.

Temporizador T1

Este temporizador se implementa en la máquina de estado de puerta del AN y limita el tiempo que puede transcurrir entre la autorización y la realización del compromiso.

Este temporizador se arranca siempre que se establece una puerta.

Este temporizador se reinicia cuando se realiza una operación compromiso sobre los recursos autorizados por la puerta.

Cuando este temporizador vence, el AN DEBE revocar cualquier reserva realizada por el MTA que hubiera sido autorizada por esta puerta, libera todos los recursos reservados en el AN, inicia un mensaje GATE-CLOSE para toda puerta que permanezca abierta, y señaliza al CM a través de mensajes MAC J.112 al objeto de liberar recursos que éste hubiese reservado.

El temporizador T1 DEBE tomar el valor incluido en el mensaje GATE-SET. Si el valor del mensaje GATE-SET es cero, el temporizador T1 DEBE tomar un valor por defecto provisionable. El valor RECOMENDADO por defecto se encuentra entre 200-300 segundos.

Temporizador T2

Este temporizador se implementa en la máquina de estado de puerta del AN y limita el tiempo de los estados transitorios de la coordinación de puerta. Es suficientemente largo como para acomodar la pérdida y retransmisión de los mensajes de coordinación de puerta, pero suficientemente corto como para no permitir un hurto significativo del servicio.

Este temporizador se arranca cuando el AN recibe un mensaje COMMIT, o cuando el AN recibe un mensaje GATE-OPEN.

Este temporizador se reinicia cuando el AN ha recibido un mensaje COMMIT y un mensaje GATE-OPEN destinados a la puerta.

Cuando el temporizador expira, el AN DEBE revocar cualquier reserva realizada por el MTA que hubiera sido autorizada por esta puerta, libera todos los recursos reservados en el AN, libera todos los recursos activados por el AN, y señaliza al CM a través de mensajes de capa MAC J.112 mecanismos de señalización específicos para liberar recursos que hubiera reservado o activado y utiliza GATE-CLOSE para cerrar cualquier puerta que estuviese abierta.

El temporizador T2 DEBE tomar el valor incluido en el mensaje GATE-SET. Si el valor de dicho mensaje es cero, el temporizador T2 DEBE tomar un valor por defecto provisionable. El valor RECOMENDADO por defecto es 2 segundos.

Temporizador T3

Este temporizador se implementa en el MTA o en el AN para el manejo de 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 por pérdidas en la red. Es suficientemente corto como para recuperarse rápidamente de los mensajes perdidos y no influir significativamente en el retardo posterior a la marcación, pero suficientemente largo como para permitir que el AN acuse recibo de la petición y todos lo encaminadores intermedios de la red del cliente.

Este temporizador se arranca cuando el MTA o el AN envía un mensaje RSVP que requiera un acuse de recibo (como el RSVP-PATH). Se reinicia cuando el emisor del mensaje del que debe acusarse recibo recibe una respuesta al mismo. En el caso de un mensaje RSVP-PATH, dicha respuesta PUEDE ser RSVP-RESV, RSVP-PATH-ERROR, o RSVP-MESSAGE-ACK, o RSVP-MESSAGE-NACK.

Cuando vence el temporizador, termina el procedimiento de retransmisión RSVP.

El valor RECOMENDADO de este temporizador es 4 segundos (4000 ms).

Temporizador T4

Este temporizador se implementa en el MTA para gestionar mensajes COMMIT. Controla la retransmisión de mensajes COMMIT que puedan haberse perdido en la red. Es suficientemente corto como para recuperarse rápidamente de peticiones de compromiso que se hayan perdido y no influir significativamente en el retardo posterior al descuelgue, pero suficientemente largo para permitir el procesamiento de la petición COMMIT en el AN.

Este temporizador se arranca cuando el MTA envía un mensaje COMMIT.

Este temporizador se reinicia cuando el MTA recibe un mensaje COMMIT-ACK o un mensaje COMMIT-ERR que se reconoce como respuesta al mensaje COMMIT.

Cuando vence el 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 AN (y en el representante del AN) para el procesamiento de la coordinación de puertas. Controla la retransmisión de los mensajes GATE-OPEN y GATE-CLOSE que puedan haberse perdido en la red. Es suficientemente corto como para recuperarse rápidamente de peticiones de mensajes de coordinación de puerta que se hayan perdido, pero suficientemente largo para permitir el procesamiento del mensaje de coordinación de puerta en el AN o en el representante del AN. Este temporizador interactúa en el caso de GATE-OPEN con el temporizador T2 y DEBERÍA ser significativamente más pequeño que él.

Este temporizador se arranca cuando el AN (o el representante del AN) envía un mensaje GATE-OPEN/GATE-CLOSE.

Este temporizador se reinicia cuando el AN (o el representante del AN) recibe un mensaje GATE-OPEN-ACK/GATE-CLOSE-ACK que se identifica como respuesta al mensaje GATE-OPEN/GATE-CLOSE.

Cuando vence el temporizador, el AN (o el representante del AN) vuelve a enviar el mensaje GATE-OPEN/GATE-CLOSE.

La retransmisión del mensaje GATE-OPEN/GATE-CLOSE se repite un número de veces determinado.

El valor RECOMENDADO de este temporizador es 500 ms.

Temporizador T6

Este temporizador se implementa en el MTA o en el AN para gestionar las reservas RSVP. Controla el retardo inicial utilizado por el procedimiento de retransmisión RSVP.

El valor RECOMENDADO de este temporizador es 500 ms.

APÉNDICE I

Ejemplo de correspondencia entre descripciones SDP y especificaciones de flujo RSVP

Los mensajes del protocolo de descripción de sesión (SDP) se utilizan para describir sesiones multimedios al objeto de realizar el anuncio de sesión, la invitación de sesión y otras formas de iniciación de sesión multimedios según la RFC 2327 del IETF. En este apéndice se describe un mecanismo para establecer la correspondencia o concordancia entre descripciones SDP y especificaciones de flujo RSVP.

Una descripción SDP típica contiene muchos campos con información relativa a la descripción de sesión (versión del protocolo, nombre de sesión, líneas de atributo de sesión, etc.), la descripción temporal (tiempo en que la sesión está activa, etc.) y la descripción de medios (nombre y transporte de medios, título de medios, información de conexión, líneas de atributos de medios, etc.). Las dos componentes críticas para establecer la concordancia entre una descripción SDP y un mensaje de especificación de flujo RSVP son el nombre y dirección de transporte de los medios (m) y las líneas de atributo de los medios (a).

El nombre de los medios y la dirección de transporte (m) tienen la forma siguiente:

m=<media> <port> <transport> <fmt list>

La línea o líneas de atributos de medios (a) tienen la forma siguiente:

a=<token>:<value>

Una comunicación de voz IP típica sería de la forma siguiente:

m = audio 3456 RTP/AVP 0

a = ptime: 10

En la línea de la dirección de transporte (m), el primer término define el tipo de medio, que en el caso de una sesión de voz IP es audio. El segundo término define el puerto UDP al que se envían los medios (puerto 3456). El tercer término indica que este tren tiene un perfil de audio/vídeo del protocolo en tiempo real (RTP). Finalmente, el último término es el tipo de carga útil de medios tal como se define en el perfil de audio/vídeo RTP (véase RFC 1890 del IETF). En este caso, el 0 representa un tipo de carga útil estática de un canal de audio con codificación MIC de ley-μ muestreado a 8 kHz. En la línea de atributos de medios (a), el primer término define el tiempo de formación del paquete (10 ms).

Los tipos de carga útil distintos a los definidos en la RFC 1890 del IETF están vinculados dinámicamente utilizando un tipo de carga útil comprendida en la gama 96-127, tal como se define en la RFC 2327 del IETF, 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 de carga útil 96 indica que la carga útil se define localmente para la duración de la sesión, y la línea siguiente indica que el tipo de carga útil 96 está vinculada a la codificación "G726-32" con un reloj a 8000 muestras/s. Para cada uno de los CÓDEC definidos (en función de si se representa en SDP como un tipo de carga útil estática o dinámica) debe haber un cuadro que establezca una correspondencia entre el tipo de carga útil o la representación de la cadena ASCII y los requisitos de anchura de banda para dicho CODEC.

La correspondencia entre el código RTP/AVP y la especificación de flujo RSVP es la que se indica en el cuadro I.1, tal como requiere la especificación J.161 del CÓDEC IPCablecom:

Cuadro I.1/J.163 – Correspondencia entre los parámetros de descripción de sesión y la especificación de flujo RSVP

Parámetros de la descripción de sesión			Parámetros de la especificación de flujo		Comentarios
Código RTP/AVP	Rtpmap	Ptime	Valores b,m,M	Valores r,p	
0	<none>	10	120 bytes	12 000 bytes/s	G.711 utilizando el tipo de carga útil definida por el IETF
0	<none>	20	200 bytes	10 000 bytes/s	
0	<none>	30	280 bytes	9 333 bytes/s	
96-127	PCMU/8000	10	120 bytes	12 000 bytes/s	MIC G.711, 64 kbit/s, CÓDEC por defecto
96-127	PCMU/8000	20	200 bytes	10 000 bytes/s	
96-127	PCMU/8000	30	280 bytes	9 333 bytes/s	
96-127	G726-16/8000	10	60 bytes	6 000 bytes/s	
96-127	G726-16/8000	20	80 bytes	4 000 bytes/s	
96-127	G726-16/8000	30	100 bytes	3 333 bytes/s	
96-127	G726-24/8000	10	70 bytes	7 000 bytes/s	
96-127	G726-24/8000	20	100 bytes	5 000 bytes/s	
96-127	G726-24/8000	30	130 bytes	4 333 bytes/s	
2	<none>	10	80 bytes	8 000 bytes/s	G.726-32, idéntico a G.721, al que el IETF asigna el tipo de carga útil 2
2	<none>	20	120 bytes	6 000 bytes/s	
2	<none>	30	160 bytes	5 333 bytes/s	
96-127	G726-32/8000	10	80 bytes	8 000 bytes/s	
96-127	G726-32/8000	20	120 bytes	6 000 bytes/s	
96-127	G726-32/8000	30	160 bytes	5 333 bytes/s	
96-127	G726-40/8000	10	90 bytes	9 000 bytes/s	
96-127	G726-40/8000	20	140 bytes	7 000 bytes/s	
96-127	G726-40/8000	30	190 bytes	6 333 bytes/s	
15	<none>	10	60 bytes	6 000 bytes/s	G.728, al que el IETF asigna el tipo de carga útil 15
15	<none>	20	80 bytes	4 000 bytes/s	
15	<none>	30	100 bytes	3 333 bytes/s	
96-127	G728/8000	10	60 bytes	6 000 bytes/s	G.728, LD-CELP, 16 kbit/s
96-127	G728/8000	20	80 bytes	4 000 bytes/s	
96-127	G728/8000	30	100 bytes	3 333 bytes/s	
18	<none>	10	50 bytes	5 000 bytes/s	G.729 Anexo A, idéntico a G.729, al que el IETF asigna el tipo de carga útil 18
18	<none>	20	60 bytes	3 000 bytes/s	
18	<none>	30	70 bytes	2 333 bytes/s	
96-127	G729A/8000	10	50 bytes	5 000 bytes/s	G.729 Anexo A, CS-ACEL, 8 kbit/s, tamaño de trama de 10 ms con 5 ms de anticipación
96-127	G729A/8000	20	60 bytes	3 000 bytes/s	
96-127	G729A/8000	30	70 bytes	2 333 bytes/s	
96-127	G729E/8000	10	55 bytes	5 500 bytes/s	G.729 Anexo E, CS-ACELP, 11,8 kbit/s, tamaño de trama de 10 ms con 5 ms de anticipación
96-127	G729E/8000	20	70 bytes	3 500 bytes/s	
96-127	G729E/8000	30	85 bytes	2 833 bytes/s	

APÉNDICE II

Ejemplo de intercambio de mensajes del protocolo para una llamada DCS básica entre elementos de la 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 obvia esta descripción para realizar la especificación de los flujos de señalización de llamada.

Cuando el MTA_O de origen envía un mensaje INVITE y éste llega al GC_O, el GC_O envía al AN_O más cercano al MTA_O de origen una petición GATE-ALLOC. Ésta es una petición para la asignación de un ID de puerta de 32 bits exclusivo en dicho AN_O. Este ID de puerta se comunica al AN_T distante en el mensaje INVITE que envía el GC_O. Además, el AN_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, tal como propone el MTA_O, y puede calcular una "envolvente autorizada" sobre esa base, generando así una instrucción GATE-SET dirigida al AN_T. Alternativamente, GC_T que sólo puede generar en ese instante una instrucción GATE-ALLOC, espera los resultados de los procedimientos de negociación de códec realizados por el MTA_T, calcula una "envolvente de autorización" más precisa después de haber recibido el 200-OK desde el MTA_T, y envía entonces la instrucción GATE-SET. Esto último se muestra en los diagramas de flujo de llamada siguientes. 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 (de acuse de recibo) a fin de determinar los valores del códec finalmente negociados.

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

Una vez que se devuelve el 200-OK al MTA_O, éste 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 en ambos sentidos. El MTA_O de origen envía un ACK para el 200-OK y hace una reserva de recursos. Cuando el ACK llega al MTA_T de terminación, éste 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 AN realiza el control de admisión después de comparar los parámetros con la envolvente autorizada y con la disponibilidad de recursos, confirmando una reserva exitosa mediante un mensaje RSVP-RESV. Mientras tanto, el AN 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, esperan una fase más del protocolo de señalización de llamada, 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 comunicarse. 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 transporta desde cada MTA a su AN local y se genera un mensaje MAC J.112 para comprometer los recursos para el flujo. Cuando los AN acusan recibo de COMMIT, los dos extremos pueden comenzar la comunicación al tiempo que gozan de una QoS mejorada. Cuando cualquiera de los dos AN recibe el mensaje COMMIT, arranca el temporizador T2 que espera la recepción del mensaje apertura de puerta desde el AN distante con su ID de puerta. Cuando se recibe el mensaje COMMIT, los AN también registran el evento inicio de QoS, y el evento respuesta de llamada.

También se indican los mensajes de coordinación de puertas entre los dos AN 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 indica que el temporizador situado en los AN queda deshabilitado.

Cuando se completa la llamada, los MTA envían un mensaje RSVP-PATH-TEAR para cancelar las reservas realizadas. En ese momento, los AN también envían un mensaje de coordinación cierre de puerta al AN distante, y los mensajes de evento parada de QoS y desconexión de llamada al servidor de mantenimiento de registros.

II.1 Ejemplo de flujo de llamada con mensajes de J.112/Anexo A

Véase la figura II.1.

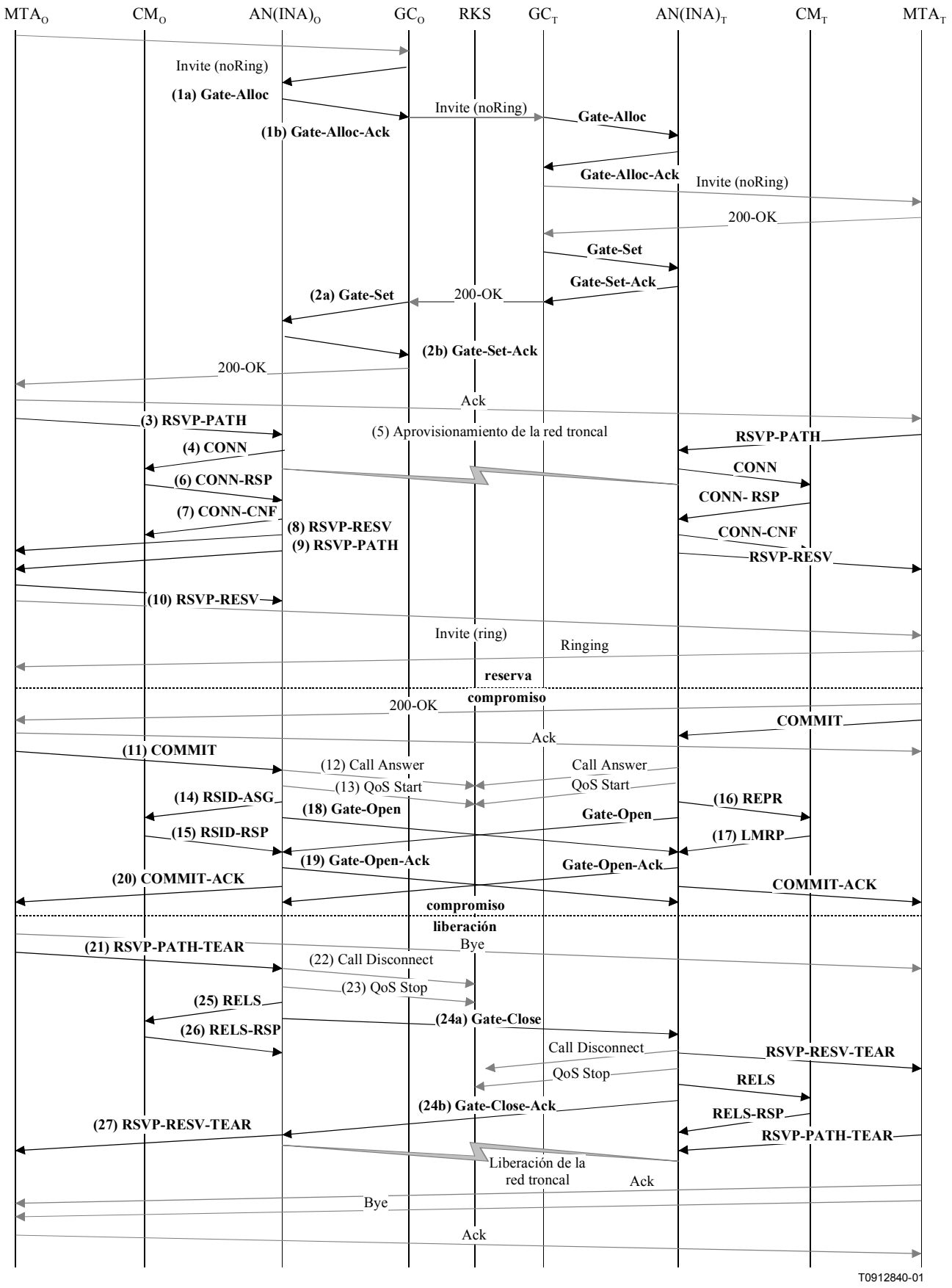


Figura II.1/J.163 – Flujo de llamada básico con mensajes de J.112/Anexo A – DCS

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

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales que utiliza este punto extremo.
Cómputo de actividad		4	Número máximo de puertas permitidas para este abonado.

El ANo verifica la utilización actual de recursos del MTAo, y responde indicando el número de puertas asignadas (1b).

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

ID de transacción		3176	
Abonado		MTAo	Respuesta a la petición de recursos totales que utiliza este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		3	Número total de puertas establecidas para este abonado.
Puerto de coordinación de puerta		4104	Puerto UDP en el que el AN espera los mensajes de coordinación de puerta.

2) Tras intercambios adicionales de señalización, el GCo autoriza a que el ANo inicie la fase de reserva del proceso de asignación de recursos para el nuevo flujo J.112 (2a).

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensaje.
Abonado		MTAo	Petición de la especificación de la puerta previamente asignada.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección	Ant	Información necesaria para la coordinación de puerta.
	Puerto	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 del servidor de mantenimiento de registros.
	ID de correlación de 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	0531-3915-2478	Campos necesarios para la generación de un mensaje de evento respuesta de llamada.
	Número de encaminamiento	0531-3915-2478	
	Número tasado	0531-3915-2480	
	Número de encaminamiento de la ubicación	0531-3915-2478	
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 paquetes para paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	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 del tipo de paquetes para paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

El ANo responde a la instrucción establecimiento de puerta con un acuse de recibo (2b).

GATE-SET-ACK (acuse de establecimiento de puerta

ID de transacción		3177	
Abonado		MTAo	Respuesta a la petición de especificación de la puerta previamente asignada.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		4	Número total de puertas establecidas para este abonado.

3) Cuando el MTAo recibe información de señalización de llamada, envía un mensaje RSVP-PATH, dirigido al MTAt, pero con el bit alerta de encaminador de la cabecera IP fijado. Los encaminadores intermedios de la red en CPE 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 de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	

RSVP-PATH (trayecto RSVP)

Tspec de emisor	b	120	Parámetros de tráfico negociados solicitados para esta llamada. El AN calcula los parámetros reales de QoS ascendentes 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 AN. NOTA – El parámetro supresión de cabecera sólo se utiliza para identificar los flujos en los que se realiza la supresión de cabecera. El contexto de supresión de cabecera se establece utilizando mensajes MAC.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	No	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
Sesión inversa	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al AN 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 inversa	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Tspec de emisor inversa	b	120	Parámetros de tráfico negociados solicitados para esta llamada. El AN calcula los parámetros reales de QoS descendentes utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP, que será ignorado por los encaminadores intermedios. NOTA – El parámetro supresión de cabecera sólo se utiliza para identificar los flujos en los que se realiza la supresión de cabecera. El contexto de supresión de cabecera se establece utilizando mensajes MAC.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	no	
	VAD	Desact.	
Rspec inversa	R	12 000	
	S	0	
ID de puerta		37125	

4) El ANo utiliza el mensaje RSVP-PATH y calcula los parámetros de QoS para el enlace J.112. El ANo envía el mensaje Connect (conexión) siguiente al CMo. Este mensaje se utiliza para establecer los parámetros ascendentes y descendentes. Suponiendo que se utiliza una velocidad ascendente de 3,088 Mbit/s y que los paquetes IP se encapsulan utilizando DirectIP, los recursos en sentido ascendente se calculan como se indica a continuación. Un paquete IP con un tamaño de 120 bytes (de Tspec) incluyendo el indicador de fin AAL 5 de 5 bytes encaja en tres células ATM. Por lo tanto, utilizando el modo de acceso de reserva, el ANo tiene que conceder 3 intervalos cada 10 ms. En el modo de acceso de velocidad constante, es necesaria una asignación cíclica de 3 intervalos cada vez, con una distancia máxima de 60 intervalos. La anchura de banda requerida es de 360 intervalos cada 1200 ms. Sin embargo, en el mensaje Connect no se asignan recursos. Ello indica al CMo que los recursos para este flujo J.112 están reservados pero aún no comprometidos.

CONN

Connection_ID	37125 <Gate ID>
Session_number	<not used>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <yes>
IPv6_add	0 <no>
Priority_included	0 <no>
Flowspec_DS_included	0 <no>
Session_binding_US_included	1 <yes>
Session_binding_DS_included	1 <yes>
Encapsulation_included	1 <yes>
DS_multiprotocol_CBD_included	0 <no>
Resource_number	0x00
Connection_Control_Field	
DS_ATM_CBD_included	0 <no>
DS_MPEG_CBD_included	1 <yes>
US_ATM_CBD_included	1 <yes>
Upstream_Channel_Number	0x1
Slot_list_included	0 <no>
Cyclic_assignment	0 <no>
Frame_Length	0 <no>
Maximum_Contention_Access_Message_Length	1 <slots>
Maximum_Reservation_Access_Message_Length	50 <slots>
Downstream_MPEG_CBD	
Downstream_Frequency	472000000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20000000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Session_binding_US	
US_session_binding_control	0x1F
NIU_client_source_IP_add	MTAo
NIU_client_destination_IP_add	MTAt
NIU_client_source_port	0
NIU_client_destination_port	7000
Upstream_transport_protocol	UDP

CONN

Session_binding_DS	
DS_session_binding_control	0x1F
INA_client_source_IP_add	MTAt
INA_client_destination_IP_add	MTAo
INA_client_source_port	0
INA_client_destination_port	7120
Downstream_transport_protocol	UDP
Connection_control_field2	
Upstream_modulation_included	1 <yes>
Upstream_Modulation	QPSK (1)

5) Simultáneamente con el mensaje N.º 4, el ANo 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 ANo cualquier notificación necesaria para indicar que la reserva se ha realizado con éxito.

6) El CMo verifica los recursos que debe asignar (por ejemplo, contexto de supresión de cabecera, ID de conexiones, contexto del clasificador) e instala los clasificadores. Si la operación se realiza con éxito devuelve el mensaje respuesta de conexión (CONN-RSP, *connect response*) indicando dicha circunstancia.

CONN-RSP

Connection_ID	37125 <Gate ID>

7) Cuando recibe el mensaje respuesta de conexión, el ANo acusa recibo con un mensaje confirmación de conexión (CONN-CONF, *connect confirm*).

CONN-CNF

Connection_ID	37125 <Gate ID>

8) Cuando se completa la reserva J.112, y se ha realizado con éxito la reserva en la red troncal, el ANo responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. El mensaje incluye el ID de recurso que el ANo asigna a este flujo IP. El mensaje RSVP-RESV se envía con la dirección fuente 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 flujo	b	120	Campos que identifican los recursos reservados para este flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva

9) Si la dirección del tramo previo en el mensaje RSVP-PATH difiere de la dirección de fuente, el AN 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, se supone que existe un encaminador intermedio entre el MTAo y el CMo, pero no entre el MTAt y el CMt.

El ANo construye un mensaje RSVP-PATH utilizando la información de trayecto inverso y envía el mensaje al MTAo de origen. El mensaje incluye el objeto ID de recurso.

RSVP-PATH (trayecto RSVP)

Objeto sesión	Protocolo	UDP	Objeto sesión y plantilla de emisor se reproducen como si el mensaje RSVP procediese del extremo lejano.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Tspec de emisor	b	120	El Tspec de emisor procede del Tspec de emisor inverso del mensaje RSVP-PATH del MTAo. Identifica los recursos que serán necesarios en sentido descendente (del MTAt al MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	no	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

10) En respuesta a RSVP-PATH, el MTAo envía al MTAt un mensaje RSVP-RESV (reserva de RSVP). Este mensaje se envía con el bit alerta de encaminador fijado, de forma que todos los encaminadores intermedios interceptan, procesan y reenvían este mensaje hasta que alcanza el ANo.

RSVP-RESV (reserva de 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	b	120	Estos valores también se copian del mensaje RSVP-PATH y especifican la cantidad de recursos reservados para el flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	no	
	VAD	Desact.	
	R	12 000	
	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 llamada (es decir, el otro extremo ha descolgado), el MTAo envía al ANo el mensaje COMMIT. Este mensaje se envía a un puerto UDP del ANo determinado mediante señalización de llamada. El objeto sesión y la plantilla de emisor proporcionan al ANo información suficiente para identificar la "puerta" e identificar los recursos reservados que han sido comprometidos.

COMMIT (compromiso)

Objeto sesión	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino debe 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	

12) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que ha comenzado la conexión de medios. En [UIT-T J.164] se describe el formato de este mensaje.

13) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que se ha concedido a esta llamada una calidad de servicio mejorada. En [UIT-T J.164] se describe el formato de este mensaje.

14) El AN puede comprometer recursos reservados utilizando el modo de acceso de velocidad constante o el modo de acceso de reserva. Cuando se recibe el mensaje COMMIT, el AN debe enviar los mensajes de capa MAC adecuados para completar el establecimiento de un flujo J.112.

En este ejemplo se asume que ANo decide utilizar el modo de acceso de reserva mientras que ANt compromete recursos utilizando el modo de acceso de velocidad constante.

Se utiliza el porteo continuo para acomodar las características de naturaleza CBR de este tráfico. Para iniciar la transmisión, el ANo envía un mensaje asignación de ID de reserva.

RSID-ASG (asignación de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <slots>
GFC_10_Slots	3 <slots>
GFC_01_Slots	1 <slots>

15) El CMo envía un mensaje respuesta de ID de reserva que indica que la operación ha tenido éxito.

RSID-RSP (respuesta de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

16) El ANt en el lado de terminación de la llamada ha decidido proporcionar los recursos solicitados utilizando el modo de acceso de velocidad constante. Para comprometer los recursos e iniciar la transmisión, el ANt envía al CMt un mensaje de reaprovisionamiento.

REPR (reaprovisionamiento)

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <no>
Delete_Reservation_IDs	0 <no>
New_Downstream_IB_Frequency_included	0 <no>
New_Downstream_OOB_Frequency_included	0 <no>
New_Upstream_Frequency_included	0 <no>
New_Frame_Length_included	1 <yes>
New_Cyclical_Assignment_included	1 <yes>
New_Slot_List_included	0 <no>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	1273 <Gate ID>
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

17) El Mt envía un mensaje respuesta de gestión de enlace (LMRP, *link management response*) que indica que la operación ha tenido éxito.

LMRP (respuesta a la gestión de enlace)

Link_Management_Msg_Number	<Reprovision Message Type Value>

18) El ANo envía al ANt distante el mensaje de coordinación de puerta para informarle que en el extremo local se han comprometido los recursos.

GATE-OPEN (apertura de puerta)

ID de transacción		72	Identificador para hacer corresponder este mensaje con su petición.
ID de puerta		1273	ID de puerta en el AN que recibe este mensaje.
Tspec	b	120	Parámetros de tráfico utilizados por los recursos comprometidos para el flujo en el sentido entre el MTAo y el MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Tspec inversa	b	120	Parámetros de tráfico previstos utilizados en el flujo en el sentido entre el MTAt y el MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Suma de control de seguridad para este mensaje.

19) Cuando se recibe el mensaje GATE-OPEN del ANt distante, el ANo responde con un mensaje GATE-OPEN-ACK

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

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su petición.
HMAC			Suma de control de seguridad para este mensaje.

20) El ANo acusa recibo del mensaje COMMIT con un mensaje COMMIT-ACK.

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 ayudar a que el acuse de recibo concuerde 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	

21) Cuando la llamada ha finalizado, el MTAo envía al AN el mensaje RSVP-PATH-TEAR. Para cada reserva RSVP, el MTAo envía un mensaje RSVP-PATH-TEAR separado.

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	

22) El ANo envía al servidor de mantenimiento de registros la notificación de que la conexión de medios ha finalizado. En [UIT-T J.164) se describe el formato de este mensaje de evento.

23) El ANo envía la notificación al servidor de mantenimiento de registros de que la llamada ha finalizado. En [UIT-T J.164] se describe el formato de este mensaje de evento.

24) Cuando recibe RSVP-PATH-TEAR, el ANo envía el mensaje de coordinación de puerta a la dirección incluida en la instrucción GATE-SET anterior, que en el caso de DCS es el ANt que sirve al MTAt (24b).

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su petición.
ID de puerta		1273	ID de puerta en el elemento de red que recibe este mensaje.
HMAC			Suma de control de seguridad para este mensaje.

El ANt responde con un mensaje GATE-CLOSE-ACK (24b).

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su petición.
HMAC			Suma de control de seguridad para este mensaje.

25) Cuando el ANo recibe RSVP-PATH-TEAR, envía un mensaje liberación al CMo indicando el flujo J.112 que debe eliminarse.

RELS (liberación)

Number_of_Connections	1
Connection_ID	37125 <Gate ID>

26) El CMt libera el flujo J.112 y envía al ANo el mensaje respuesta de liberación.

RELS-RSP (respuesta de liberación)

Connection_ID	37125 <Gate ID>

27) El ANo envía al MTAo el mensaje RSVP-RESV-TEAR.

RSVP-RESV-TEAR (deshacer reserva RSVP)

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	

II.2 Ejemplo de flujo de llamada con mensajes de J.112 Anexos B y C

Véase la figura II.2.

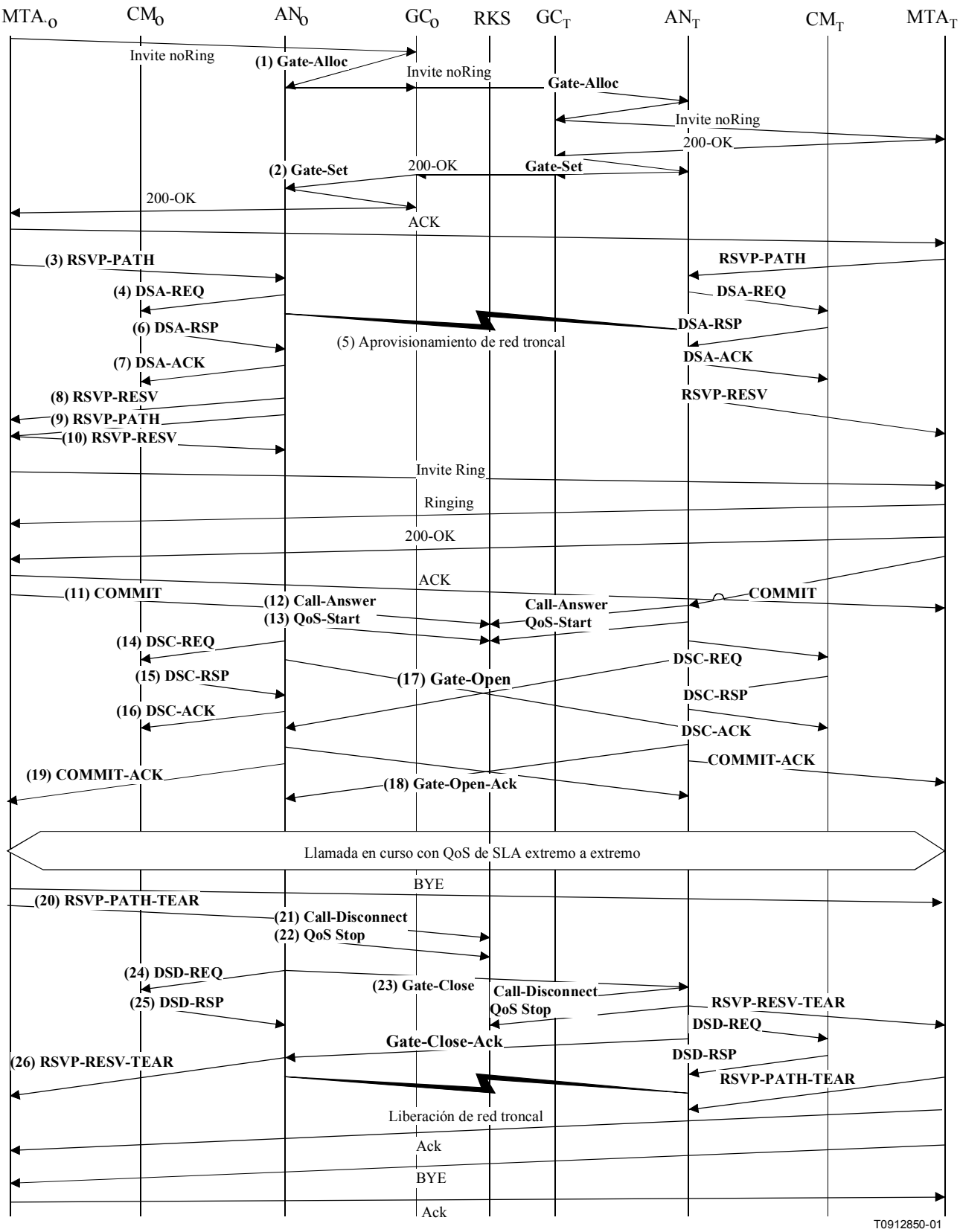


Figura II.2/J.163 – Flujo de llamada básica – Señalización DCS

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

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales utilizados por este punto extremo.
Cómputo de actividad		4	Número máximo de conexiones permitidas por este cliente.

El ANo 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 de los recursos totales que utiliza este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		3	Número total de conexiones establecidas por este cliente.
Puerto de coordinación de puerta		4104	Puerto UDP en el que el AN espera los mensajes de coordinación.

2) Tras un intercambio de señalización adicional, el GCo autoriza que el ANo 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 de los recursos totales utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección de AN	ANt	Información necesaria para la coordinación de puerta.
	Puerto de AN	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 de 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 la generación del mensaje respuesta de llamada.
	Número de encaminamiento	212-555-2222	
	Número tarificado	212-555-1111	
	Número de encaminamiento de la ubicación	212-555-2222	
Especificación de puerta	Dirección	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 para los paquetes ascendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puertas.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

GATE-SET (establecimiento de puerta)

Especificación de puerta	Dirección	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 para los paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para que se complete la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

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

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

ID de transacción		3177	
Abonado		MTAo	Petición de los recursos totales utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		4	Número total de conexiones que establece este cliente.

3) Cuando el MTAo recibe información de señalización de llamada, envía al MTAt un mensaje RSVP-PATH con el bit alerta de encaminador fijado. Los encaminadores intermedios en la LAN originaria interceptan, procesan y reenvían este mensaje como un 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 que 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	

RSVP-PATH (trayecto RSVP)

Tspec de emisor	b	120	Parámetros de tráfico negociados que han sido solicitados para esta llamada. El AN calcula los parámetros reales de QoS ascendente utilizando estos parámetros Tspec y Rspec. Es un objeto RSVP normalizado que será interpretado por todos lo encaminadores intermedios en el trayecto entre el MTA y el AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
Sesión inversa	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al AN 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 inversa	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Tspec de emisor inversa	b	120	Parámetros de tráfico negociados solicitados para esta llamada. El AN calcula los parámetros reales de QoS descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que será ignorado por los encaminadores intermedios.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	0	
	VAD	Desact.	
Rspec inversa	R	12 000	
	S	0	
ID de puerta		37125	

4) El AN utiliza el mensaje RSVP-PATH y calcula los parámetros de QoS para el enlace J.112. El AN envía al CM el siguiente mensaje DSA-REQ (petición DSA). Este mensaje se utiliza para establecer parámetros ascendentes y descendentes. El tamaño de la concesión no solicitada ascendente se calcula como 120 (de Tspec) más 18 (tara de Ethernet) menos 40 (supresión de la cabecera) más 13 (tara de J.112). La supresión de cabecera, especificada con una longitud de 40 en RSVP-PATH, hace referencia a los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se toma del paquete RSVP.

DSA-REQ (petición DSA)

ID de transacción		1
Flujo de servicio ascendente (UpstreamServiceFlow)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)

DSA-REQ (petición DSA)

Flujo de servicio ascendente (UpstreamServiceFlow)	Request/Transmission Policy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
Flujo de servicio descendente (DownstreamServiceFlow)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
Clasificación de paquete ascendente (UpstreamPacketClassification)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
Clasificación de paquete descendente (DownstreamPacketClassification)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAt
	IPDestinationAddress	MTAo
	IPDestinationPort	7120
	IPProtocol	UDP (17)
Supresión de cabecera de carga útil (PayloadHeaderSuppression)	ClassifierIdentifier	3001
	ServiceFlowIdentifier	1001
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42bytes>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Verificación (0)
HMAC		

5) Simultáneamente con el mensaje N.º 2, el AN inicia las reservas necesarias en la red troncal para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos utilizados en la red troncal y queda fuera del ámbito de esta Recomendación. El encaminador de la red troncal envía al AN la notificación que sea precisa para indicar que la reserva ha tenido éxito.

6) El CM verifica los recursos que debe asignar (por ejemplo, espacio del cuadro de supresión de cabecera, los ID de flujos de servicio, espacio del cuadro del clasificador, anchura de banda de la red local) e instala los clasificadores. Si la operación tiene éxito, devuelve el mensaje DSA-RSP indicando dicho éxito.

DSA-RSP (respuesta DSA)

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

7) Cuando el AN recibe el DSA-RSP, acusa recibo mediante un mensaje DSA-ACK.

DSA-ACK (acuse de recibo DSA)

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

8) Una vez que se ha completado la reserva J.112 y se ha realizado con éxito la reserva en la red troncal, el AN responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. Éste incluye el ID de recurso que el AN asigna a esta conexión. El mensaje RSVP-RESV se envía con la dirección de fuente MTA_T y la dirección de destino MTA_O. Todos los encaminadores intermedios interceptarán, la procesarán y reenviarán como un mensaje RSVP-RESV (reserva RSVP) normalizado.

RSVP-RESV (reserva RSVP)

Objeto sesión	Protocolo	UDP	Campos que identifican el flujo IP para el que se ha realizado la reserva.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Especificación de flujo	b	120	Campos que identifican los recursos reservados para este flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

9) Si la dirección del tramo previo difiere de la dirección de fuente, el AN debe generar un mensaje RSVP-PATH para reservar recursos en sentido descendente en todos los encaminadores intermedios. Esta condición solamente se cumple si el MTA no es inmediatamente adyacente al CM.

En este ejemplo, se supone que existe un encaminador intermedio entre el MTAo y su CM, pero no entre el MTAt y su CM.

El AN construye el mensaje RSVP-PATH utilizando la información de trayecto inverso recibida en el mensaje RSVP-PATH y envía el mensaje 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	
Tspec de emisor	b	120	La Tspec de emisor procede de la Tspec de emisor inversa incluida en el mensaje RSVP-PATH del MTAo. Permite identificar los recursos que serán necesarios en el sentido descendente (del MTAt al MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

10) En respuesta a RSVP-PATH(7), el MTAo envía al MTAt el mensaje RSVP-RESV. Este mensaje se envía con el bit "alerta de encaminador" fijado, de forma que todos los encaminadores intermedios interceptan, procesan y reenvían este mensaje hasta que alcanza el AN.

RSVP-RESV (reserva RSVP)

Objeto sesión	Protocolo	UDP	El objeto sesión y la plantilla de emisión se copian del mensaje RSVP-PATH recibido.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Specificación de filtro	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
Especificación de flujo	b	120	Estos valores también se copian del mensaje RSVP-PATH, y especifican la cantidad de recursos reservados para el flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
	R	12 000	
	S	0	
ID de recurso		1	ID de recurso, copiado de RSP-PATH.

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

El objeto sesión y la plantilla de emisor proporcionan al AN información suficiente para identificar la "puerta" y los recursos reservados que han sido comprometidos.

COMMIT (compromiso)

Objeto sesión	Protocolo	UDP	Los elementos de la cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino deben concordar con los 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 ANo envía al servidor de mantenimiento de registros (RKS) el registro de evento que indica que ha comenzado la conexión de medios.

Call-Answer (respuesta de llamada)

Cabecera	Indicación de tiempo	<time>	Hora a la que se registra el evento
	ID de correlación de facturación	<string>	ID de correlación de facturación incluido en establecimiento de puerta
Parte llamada	Número de parte llamada	212-555-2222	Elementos facilitados por el CMS en establecimiento de puerta.
Número de encaminamiento	Número de encaminamiento	212-555-2222	
Número tasado	Número tasado	212-555-1111	
Número de encaminamiento de la ubicación	Número de encaminamiento de la ubicación	212-555-2222	

13) El ANo envía al servidor de mantenimiento de eventos el registro de evento que indica que se ha concedido a esta llamada una conexión con calidad de servicio mejorada.

QoS-START (inicio de QoS)

Cabecera	Indicación de tiempo	<time>	Hora a la que se registra el evento
	ID de correlación de facturación	<string>	ID de correlación incluido en establecimiento de puerta.
Descriptor de QoS	Tipo	UGS	Descripción de la QoS para esta conexión
	Intervalo de concesión	10 ms	
	Fluctuación de fase de la concesión	2 ms	
	Concesión/intervalo	1	
	Tamaño de la concesión	111	
Puerto del MTA	Puerto	7120	

14) El AN determina la reserva que se debe activar y envía al CM un mensaje DSC-REQ (petición DSC) para activar el flujo.

DSC-REQ (petición DSC)

ID de transacción		2
Flujo de servicio ascendente (UpstreamServiceFlow)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
Flujo de servicio descendente (DownstreamServiceFlow)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
Clasificación de paquete ascendente (UpstreamPacketClassification)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Activar (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
Clasificación de paquete descendente (DownstreamPacketClassification)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Activo (1)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

15) El CM envía un mensaje DSC-RSP que indica que la operación ha tenido éxito.

DSC-RSP (respuesta DSC)

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

16) El AN envía un mensaje DSC-ACK para indicar que se ha recibido el mensaje DSC-RSP y está de acuerdo con él.

DSC-ACK (acuse DSC)

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

17) El AN envía al AN distante el mensaje de coordinación de puerta para informarle que los recursos de este extremo han sido comprometidos.

GATE-OPEN (apertura de puerta)

ID de transacción		72	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		1273	ID de puerta en el AN distante.
Tspec	b	120	Parámetros de tráfico comprometidos utilizados en el sentido del MTAo al MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Tspec inversa	b	120	Parámetros de tráfico esperados utilizados en el sentido del MTAt al MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Suma de control de seguridad para este mensaje.

18) El AN distante responde al mensaje GATE-OPEN con:

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

ID de transacción		72	Identificador para hacer corresponder este mensaje con su respuesta
HMAC			Suma de control de seguridad para este mensaje

19) El AN acusa recibo de COMMIT con:

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 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	

20) Cuando la llamada ha finalizado, el MTA envía al AN el mensaje RSVP-PATH-TEAR. Para cada reserva RSVP, el MTA envía un mensaje RSVP-PATH-TEAR independiente.

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	

21) El AN envía al servidor de mantenimiento de registros la notificación de que la conexión de medios ha terminado.

Call-Disconnect (desconexión de llamada)

Cabecera	Indicación de tiempo	<time>	Instante en el que se registra el evento.
	ID de correlación de facturación	<string>	ID de correlación de facturación proporcionado por el mensaje establecimiento de puerta.
Causa de terminación	Causa	1100C	Código de causa tal como definen los mensajes de evento.

22) El AN envía al servidor de mantenimiento de registros la notificación de que la llamada ha finalizado. Este mensaje sólo es una muestra de lo que podría incluirse en un mensaje parada de QoS.

QoS-Stop (parada de QoS)

Indicación de tiempo		<time>	Hora a la que se registra el evento.
Cabecera	Indicación de tiempo	<time>	Hora a la que se registra el evento.
	ID de correlación de facturación	<string>	ID de correlación del mensaje establecimiento de puerta.
SF-ID	SF-ID	1001	Identificador de flujo de servicio.

23) Cuando el AN recibe RSVP-PATH-TEAR, envía el mensaje de coordinación de puerta al correspondiente AN que sirve al MTAt.

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		1273	Identifica el ID de puerta en el AN distante.
HMAC			Suma de control de seguridad para este mensaje.

El AN distante responde con:

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

24) Cuando el AN recibe RSVP-PATH-TEAR, envía al CM un DSD-REQ que indica el ID del flujo de servicio que debe suprimirse.

DSD-REQ (petición DSD)

ID de transacción		3
ID de flujo de servicio		1001
HMAC		

DSD-REQ (petición DSD)

ID de transacción		4
ID de flujo de servicio		2001
HMAC		

25) El CM suprime el ID de flujo de servicio y envía al AN la respuesta.

DSD-RSP (respuesta DSD)

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

DSD-RSP

ID de transacción		3
ID de flujo de servicio		2001
Código de confirmación		Éxito (0)
HMAC		

26) El AN envía al MTA el mensaje RSVP-RESV-TEAR.

RSVP-RESV-TEAR (deshacer reserva RSVP)

Objeto sesión	Protocolo	UDP	Parámetros que identifican el flujo IP que se da por terminado.
	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 sobre una posible relación entre el protocolo de señalización de llamada (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 origen completa la marcación, es decir, el mapa de dígitos indica que se ha introducido 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 al 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 AN_O para asignar un ID de puerta 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 AN_T de terminación (utilizando una instrucción GATE-SET), admitiendo todos los flujos de medios que son aceptables para el originador dentro de la "envolvente autorizada," permitiendo que el puerto de destino sea libremente elegido en el MTA_T. El AN_T asigna asimismo un ID de puerta y lo devuelve al CMS_T. El CMS_T pasa el ID de puerta 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 este punto, el MTA_T conoce el códec de emisión, el códec de recepción, la dirección de destino y el puerto para los paquetes vocales que envía, así como el puerto local para la recepción de paquetes vocales. Por lo tanto, comienza la secuencia de reserva enviando al AN_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 AN_O. Por lo tanto, realiza la operación GATE-SET, incluyendo el ID de puerta distante y la dirección del AN_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. El MTA_O tiene entonces información suficiente para realizar una reserva de recursos. Cuando se completa la reserva, envía al CMS_O un acuse de recibo exitoso. El CMS_T indica entonces al MTA_T que debe advertir al usuario acerca de una llamada entrante. El MTA_T verifica en primer lugar que la reserva de recursos que inició anteriormente se ha completado con éxito y si así es, envía la señal de llamada al teléfono.

Cuando la parte llamada responde, el MTA_T informa al CMS_T con un mensaje notificación, que se ha producido un descolgado. El CMS_T envía entonces una instrucción modificación de conexión al MTA_T haciendo que el modo de conexión sea emisión + recepción; el MTA_T realiza el intercambio COMMIT con el AN_T y envía el acuse de recibo. El CMS_O también envía una instrucción modificación de conexión al MTA_O haciendo que su modo de conexión sea emisión + recepción, y que el MTA_O también realice el intercambio COMMIT con el AN_O. La llamada queda entonces establecida.

Cualquiera de las partes puede iniciar una terminación de llamada enviando un mensaje notificación a su CMS indicando que se ha producido un colgado. En el diagrama, se muestra al MTA_O haciendo esto. El CMS_O responde a la notificación de colgado enviando una instrucción supresión de conexión que dispara la secuencia RSVP-PATH-TEAR (deshacer trayecto RSVP) para liberar los recursos. Se informa al MTA_T del colgado mediante señalización de llamada (una instrucción supresión de conexión que no se muestra en el diagrama) o mediante el mensaje RSVP-RESV-TEAR (deshacer reserva RSVP) de DQoS. Cuando posteriormente cuelga el MTA_T, produce el mismo mensaje notificación, tal como hizo anteriormente el MTA_O, y termina la secuencia.

III.1 Ejemplo de flujo de llamada con mensajes de J.112/Anexo A

Véase la figura III.1.

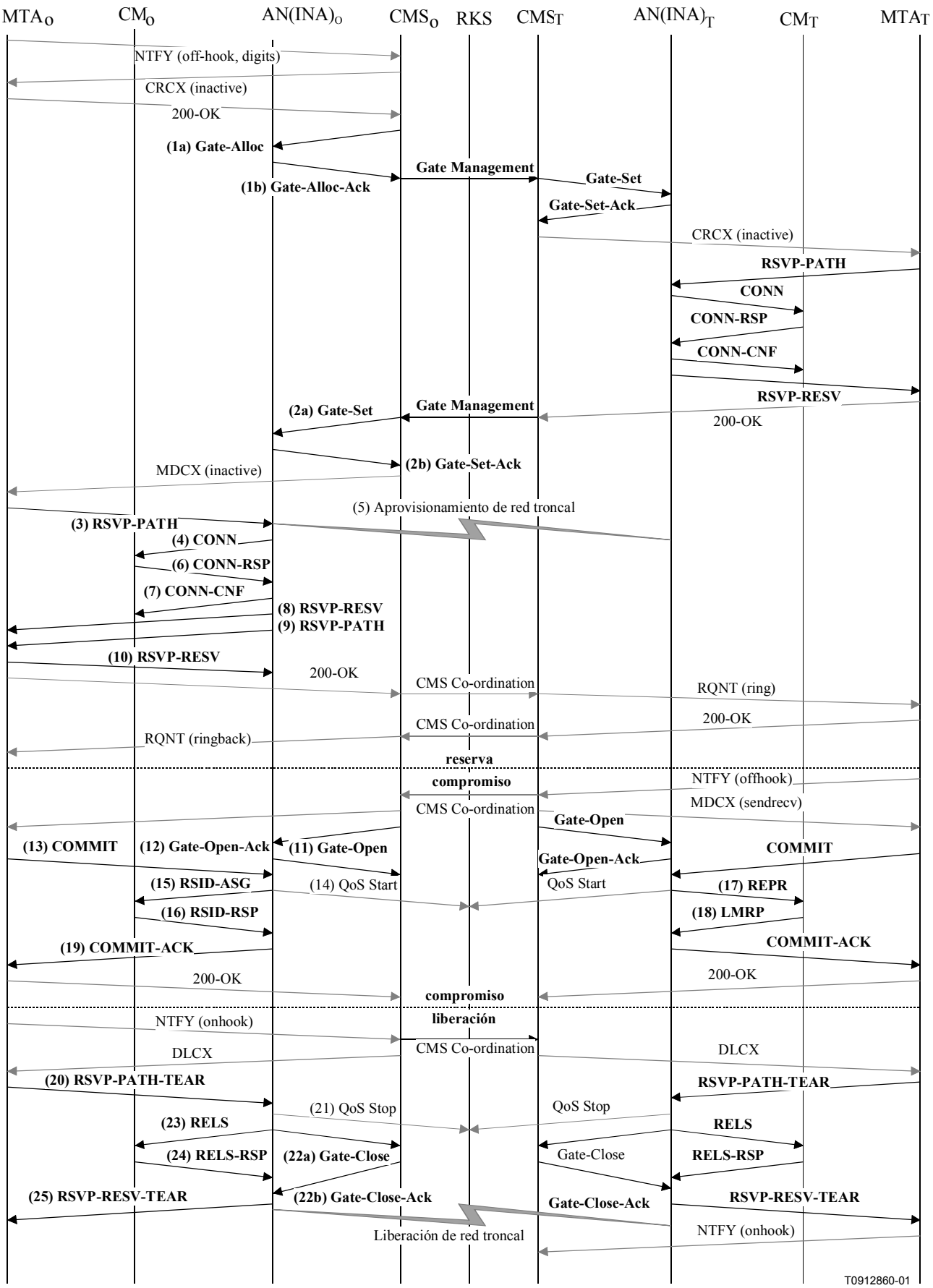


Figura III.1/J.163 – Flujo de llamada básico con mensajes de J.112 Anexo A – NCS

1) Cuando el GCo/CMSo recibe información de señalización del MTAo, verifica el consumo actual de recursos del MTAo consultando al ANo (1a).

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales que utiliza este punto extremo.
Cómputo de actividad		4	Número máximo de puertas permitidas para este abonado.

El ANo verifica la utilización actual de recursos por parte del MTAo, y responde indicando el número de puertas asignadas (1b).

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

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales que utiliza este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		3	Número máximo de puertas establecidas para este abonado.

2) Tras un intercambio adicional de señalización, el GCo/CMSo autoriza que el ANo inicie la fase de reserva del proceso de asignación de recursos para el nuevo flujo J.112 (2a).

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición para la especificación de la puerta anteriormente asignada.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección	CMSo	Información necesaria para realizar la coordinación de puerta. Nótese que el CMSo ha indicado que él es la entidad para el intercambio de mensajes de coordinación de puertas.
	Puerto	2052	
	ID de puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	No-apertura-puerta	El valor de la bandera indica que el AN no debería enviar un mensaje apertura de puerta cuando recibe un mensaje COMMIT del MTA, pero aún espera recibir un mensaje apertura de puerta del CMSo.
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 de facturación	<id>	Dados opacos que pasarán al RKS cuando los recursos estén comprometidos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Dirección	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 del tipo de paquete para los paquetes ascendentes.
	T1	180 000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Especificación de puerta	Dirección	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para los paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

El ANo responde a la instrucción establecimiento de puerta con un acuse de recibo (2b).

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

ID de transacción		3177	
Abonado		MTAo	Petición para la especificación de la puerta previamente asignada.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		4	Número total de puertas establecidas para este abonado.

3) Cuando el MTAo recibe una instrucción modificación de conexión, envía al MTAt un mensaje RSVP-PATH, pero con el bit alerta de encaminador fijado en la cabecera IP. Los encaminadores intermedios en la LAN originaria 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 asimismo se utilizan en los clasificadores de QoS.
	Dirección de fuente	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Tspec de emisor	b	120	Parámetros de tráfico negociados para esta llamada. El AN calcula los parámetros reales de QoS 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 AN. NOTA – El parámetro supresión de cabecera sólo se utiliza para identificar los flujos en los que se lleva a cabo la supresión de cabecera. El contexto de supresión de cabecera se establece utilizando mensajes MAC.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	no	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
Sesión inversa	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al AN 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 inversa	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Tspec de emisor inversa	b	120	Parámetros de tráfico negociados solicitados para esta llamada. El AN calcula los parámetros reales de QoS descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que será ignorado por los encaminadores intermedios. NOTA – El parámetro supresión de cabecera sólo se utiliza para identificar los flujos en los que se realiza la supresión de
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	no	
	VAD	Off	

RSVP-PATH (trayecto RSVP)

Rspec inversa	R	12 000	cabecera. El contexto de supresión de cabecera se establece utilizando mensajes MAC.
	S	0	
ID de puerta		37125	

4) El AN utiliza el mensaje RSVP-PATH y calcula los parámetros de QoS para el enlace J.112. El AN envía al CM el siguiente mensaje conexión. Este mensaje se utiliza para establecer los parámetros de los flujos ascendente y descendente. Suponiendo que se utiliza una velocidad ascendente de 3,088 Mbit/s y que los paquetes IP se encapsulan utilizando DirectIP, los recursos en sentido ascendente se calculan de la forma siguiente. En las primeras 3 células ATM se ubica un paquete IP de 120 bytes (de Tspec) incluyendo los 5 bytes AAL 5 posteriores. Por lo tanto, utilizando el modo de acceso de reserva el AN debe conceder 3 intervalos cada 10 ms. En el modo de acceso de velocidad constante, es necesaria una asignación cíclica de 3 intervalos cada vez con una distancia máxima de 60 intervalos. La anchura de banda solicitada es de 360 intervalos cada 1200 ms. Sin embargo, en el mensaje conexión no se asignan recursos. Ello indica al CM que los recursos para dicho flujo J.112 están reservados pero aún no comprometidos.

CONN

Connection_ID	37125 <Gate ID>
Session_number	<not used>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <yes>
IPv6_add	0 <no>
Priority_included	0 <no>
Flowspec_DS_included	0 <no>
Session_binding_US_included	1 <yes>
Session_binding_DS_included	1 <yes>
Encapsulation_included	1 <yes>
DS_multiprotocol_CBD_included	0 <no>
Resource_number	0x00
Connection_Control_Field	
DS_ATM_CBD_included	0 <no>
DS_MPEG_CBD_included	1 <yes>
US_ATM_CBD_included	1 <yes>
Upstream_Channel_Number	0x1
Slot_list_included	0 <no>
Cyclic_assignment	0 <no>
Frame_Length	0 <no>
Maximum_Contention_Access_Message_Length	1 <slots>
Maximum_Reservation_Access_Message_Length	50 <slots>

CONN

Downstream_MPEG_CBD	
Downstream_Frequency	472000000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20000000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Session_binding_US	
US_session_binding_control	0x1F
NIU_client_source_IP_add	MTAo
NIU_client_destination_IP_add	MTAt
NIU_client_source_port	0
NIU_client_destination_port	7000
Upstream_transport_protocol	UDP
Session_binding_DS	
DS_session_binding_control	0x1F
INA_client_source_IP_add	MTAt
INA_client_destination_IP_add	MTAo
INA_client_source_port	0
INA_client_destination_port	7120
Downstream_transport_protocol	UDP
Connection_control_field2	
Upstream_modulation_included	1 <yes>
Upstream_Modulation	QPSK (1)

5) Simultáneamente con el mensaje 4, el AN 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 AN 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, el contexto de supresión de cabecera, el ID de conexión, el contexto de clasificador) e instala los clasificadores. Si la operación se realiza con éxito devuelve el mensaje respuesta de conexión indicando dicha circunstancia.

CONN-RSP (respuesta de conexión)

Connection_ID	37125 <Gate ID>

7) Cuando el AN recibe el mensaje respuesta de conexión, acusa recibo con un mensaje confirmación de conexión.

CONN-CNF (confirmación de conexión)

Connection_ID	37125 <Gate ID>

8) Cuando se completa la reserva J.112, y la reserva de red troncal se ha realizado con éxito, el AN responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. El mensaje incluye el ID de recurso que el AN asigna a este flujo IP. El mensaje RSVP-RESV se envía con la dirección de fuente MTAt y la dirección de destino MTAo. Todos los encaminadores intermedios interceptan, procesan y reenvían esto como un mensaje RSVP-RESV normalizado.

RSVP-RESV (reserva RSVP)

Objeto sesión	Protocolo	UDP	Campos que identifican el flujo IP para el que se ha establecido la reserva.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Especificación de filtro	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Especificación de flujo	b	120	Campos que identifican los recursos reservados para este flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

9) Si la dirección del tramo previo en el mensaje RSVP-PATH difiere de la dirección de fuente, el AN debe generar un mensaje RSVP-PATH para reservar recursos en sentido descendente en todos los encaminadores intermedios. Esta condición sólo se cumple si el MTAo no es inmediatamente adyacente al CM.

En este ejemplo, se supone que existe un encaminador intermedio entre el MTAo y su CM, pero no entre el MTAt y su CM.

El AN construye un mensaje RSVP-PATH utilizando la información de trayecto inverso y envía el mensaje al MTAo 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 replican como si el mensaje RSVP procediese del extremo lejano.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Tspec de emisor	b	120	El Tspec procede de la Tspec de emisor inversa del mensaje RSVP-PATH procedente del MTAo. Identifica los recursos que serán necesarios en sentido descendente (del MTAt al MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	no	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva

10) En respuesta a RSVP-PATH, el MTAo envía a MTAt el mensaje RSVP-RESV. Este mensaje se envía con el bit "alerta de encaminador" fijado, de forma que todos los encaminadores intermedios interceptan, procesan y reenvían este mensaje hasta que alcanza el AN.

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	b	120	Estos parámetros también se copian del mensaje RSVP-PATH y especifican la cantidad de recursos que se reservan para el flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	no	
	VAD	Desact.	
	R	12 000	
	S	0	
ID de recurso		1	ID de recurso, copiado del RSVP-PATH.

11) El CMS envía al AN el mensaje de coordinación de puerta para informarle de que los recursos deberían comprometerse. Si el AN no recibe del MTA un mensaje COMMIT antes de que venza el temporizador T2, aborta la llamada.

GATE-OPEN (apertura de puerta)

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		37125	ID de puerta en el AN que recibe este mensaje.
HMAC			Suma de control de seguridad para este mensaje.

12) El AN responde a GATE-OPEN con un mensaje GATE-OPEN-ACK.

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

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

13) En respuesta a una instrucción modificación de conexión, que indica que se ha completado el establecimiento de llamada (es decir, que el otro lado ha descolgado), el MTAo envía al AN el mensaje COMMIT. Este mensaje se envía al AN a través de un puerto UDP incluido en el objeto entidad compromiso de RSVP-RESV. El objeto sesión y la plantilla de emisor proporcionan al AN información suficiente para identificar los recursos reservados que se han comprometido.

COMMIT (compromiso)

Objeto sesión	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, fuente y puerto de destino deben concordar con los del ID de puerta.
	Dirección de destino	MTAt	
	Puerto de destino	7000	

COMMIT (compromiso)

Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	

14) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que se ha concedido a esta llamada una QoS mejorada. En [UIT-T J.164] se describe el formato de este mensaje.

15) El AN puede comprometer los recursos reservados utilizando el modo de acceso de velocidad constante o el modo de acceso de reserva. Cuando recibe el mensaje COMMIT, el AN debe enviar los mensajes de capa MAC adecuados para completar el establecimiento de un flujo J.112.

En este ejemplo, se asume que el AN del MTAo decide utilizar el modo de acceso de reserva mientras que el AN del MTAt compromete recursos utilizando el modo de acceso de velocidad constante.

Se utiliza el porteo continuo para acomodar las características de tipo CBR de este tráfico. Para iniciar la transmisión el AN envía un mensaje asignación de ID de reserva (RSID-ASG, *reservation ID assignement*).

RSID-ASG (asignación de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <slots>
GFC_10_Slots	3 <slots>
GFC_01_Slots	1 <slots>

16) El CM envía un mensaje respuesta de ID de reserva (RSID-RSP) que informa que la operación ha tenido éxito.

RSID-RSP (respuesta de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

17) El AN del lado de terminación de la llamada decide proporcionar los recursos solicitados utilizando el modo de acceso de velocidad constante. Para comprometer los recursos e iniciar la transmisión, el AN envía al CM un mensaje reaprovisionamiento (REPR, *Reprovision*).

REPR (reaprovisionamiento)

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <no>
Delete_Reservation_IDs	0 <no>
New_Downstream_IB_Frequency_included	0 <no>
New_Downstream_OOB_Frequency_included	0 <no>
New_Upstream_Frequency_included	0 <no>

REPR (reaprovisionamiento)

New_Frame_Length_included	1 <yes>
New_Cyclical_Assignment_included	1 <yes>
New_Slot_List_included	0 <no>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	37125 <Gate ID>
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

18) El CM envía un mensaje respuesta de gestión de enlace (LMRP, *link management response*) que informa que la operación ha tenido éxito.

LMRP (respuesta de gestión de enlace)

Link_Management_Msg_Number	<Reprovision Message Type Value>

19) El AN acusa recibo de COMMIT con un mensaje COMMIT-ACK.

COMMIT-ACK (acuse de compromiso)

Objeto sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente, la fuente y el puerto de destino pueden ayudar a que el acuse de recibo concuerde 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	

20) Cuando la llamada finaliza en respuesta a una instrucción suprimir conexión, el MTA envía al AN un mensaje RSVP-PATH-TEAR. Para cada reserva RSVP, el MTA envía un mensaje RSVP-PATH-TEAR independiente.

RSVP-PATH-TEAR

Objeto sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente, la 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	

21) El AN envía al servidor de mantenimiento de registros la notificación de que la llamada ha finalizado. En [UIT-T J.164] se describe el formato de este mensaje de evento.

22) Cuando el AN recibe RSVP-PATH-TEAR, envía el mensaje de coordinación de puerta a la dirección anteriormente incluida en la instrucción GATE-SET, que en el caso de NCS es el agente de llamada (21b).

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		8095	ID de puerta en el elemento de red (aquí: CMS) que recibe este mensaje.
HMAC			Suma de control de seguridad para este mensaje.

El CMS responde con un mensaje GATE-CLOSE-ACK (22b).

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

23) Cuando el AN recibe RSVP-PATH-TEAR, envía al CM un mensaje liberación (RELS, *release*) indicando el flujo J.112 que debe eliminarse.

RELS (liberación)

Number_of_Connections	1
Connection_ID	37125 <Gate ID>

24) El CM libera el flujo J.112 y envía al AN el mensaje respuesta de liberación (RELS-RSP, *release response*).

RELS-RSP (respuesta de liberación)

Connection_ID	37125 <Gate ID>

25) El AN envía al MTA el mensaje RSVP-RESV-TEAR.

RSVP-RESV-TEAR (deshacer reserva RSVP)

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

III.2 Ejemplo de flujo de llamada con mensajes de J.112 Anexos B y C

Véase la figura III.2.

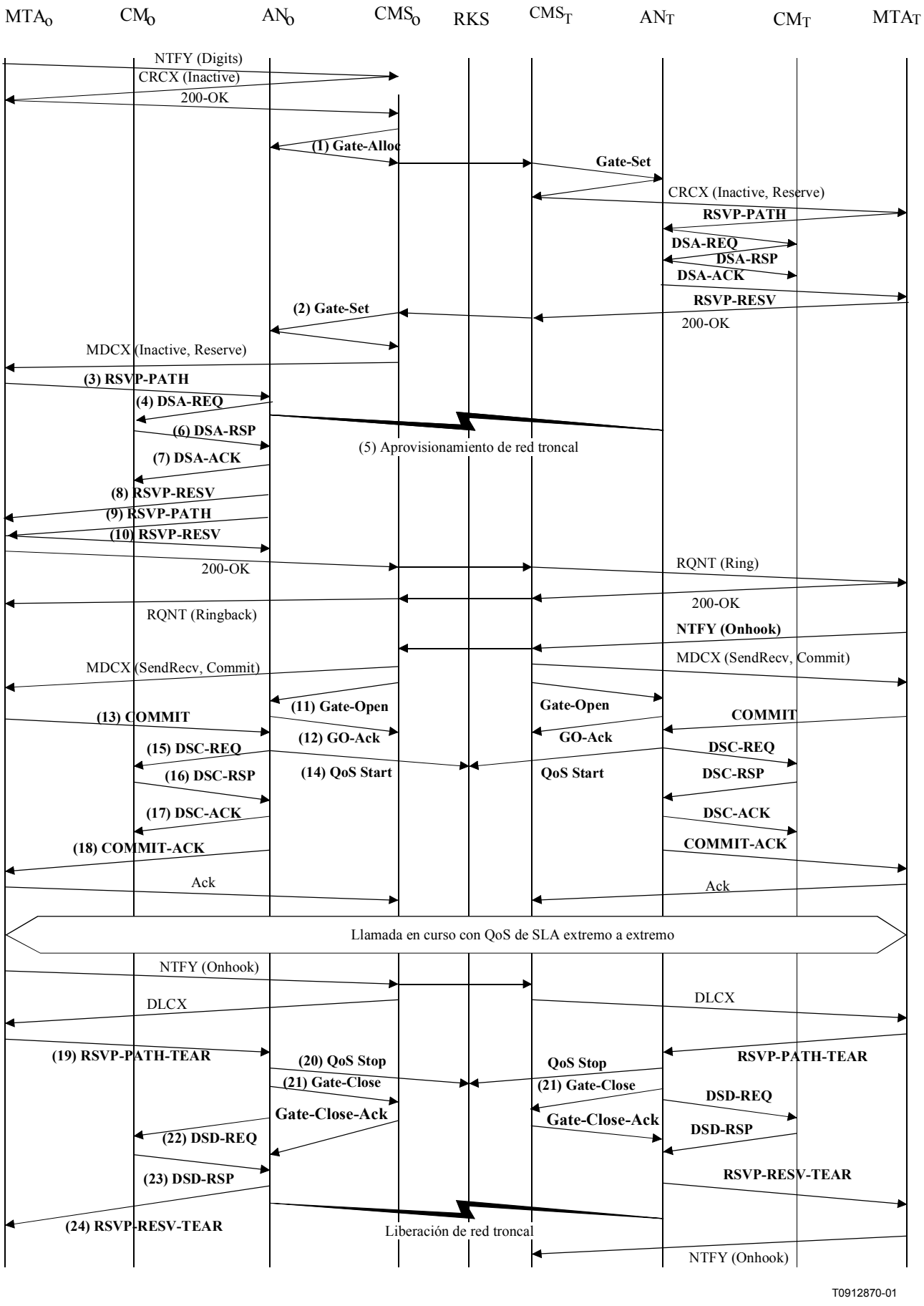


Figura III.2/J.163 – Flujo de llamada básico – NCS

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

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales utilizados por este punto extremo.
Cómputo de actividad		4	Número máximo de conexiones permitido por el cliente

El ANo verifica la utilización actual de recursos por parte del MTAo y responde informando del número de conexiones activas.

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

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales utilizados por este punto extremo.
ID de puerta		37125	Identificador de puerta asignada
Cómputo de actividad		3	Número total de conexiones establecidas por este cliente.

2) Tras un intercambio adicional de señalización, el GCo autoriza que el ANo 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 de los recursos totales utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección	CMSo	Información necesaria para realizar la coordinación de puerta. Nótese que el CMSo se ha identificado a sí mismo como la entidad que realiza el intercambio de mensajes de coordinación de puerta. El valor de la bandera indica que el AN no debería enviar un mensaje apertura de puerta cuando recibe un mensaje COMMIT del MTA, pero aún espera recibir un mensaje apertura de puerta del CMS_O.
	Puerto	2052	
	ID de puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	Sin puerta abierta	
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 de facturación	<id>	Datos opacos que se pasan al RKS cuando los recursos están comprometidos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Dirección	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para los paquetes ascendentes
	T1	180000	Tiempo máximo entre reserva y compromiso
	T2	2000	Tiempo máximo para completar la coordinación de puertas.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Especificación de puerta	Dirección	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para los paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

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

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

ID de transacción		3177	
Abonado		MTAo	Petición de los recursos totales utilizados por este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		4	Número máximo de conexiones que establece el cliente.

3) Cuando el MTAo recibe una instrucción modificar conexión, envía al MTAt un mensaje RSVP-PATH, pero con el bit alerta de encaminador fijado en la cabecera IP. Los encaminadores intermedios en la LAN originaria interceptan, procesan y reenvían este mensaje como un 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 de destino	MTAt	
	Puerto de destino	7000	
Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Tspec de emisor	b	120	Parámetros de tráfico negociados que han sido solicitados para esta llamada. El AN calcula los parámetros reales de QoS 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 AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
Sesión inversa	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al AN 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 inversa	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Tspec de emisor inversa	b	120	Parámetros de tráfico negociados solicitados para esta llamada. El AN calcula los parámetros reales de QoS en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que será ignorado por los encaminadores intermedios.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	0	
	VAD	Desact.	

RSVP-PATH (trayecto RSVP)

Rspec inversa	R	12 000	
	S	0	
ID de puerta		37125	

4) El AN utiliza el mensaje RSVP-PATH y calcula los parámetros de QoS para el enlace J.112. El AN envía al CM el siguiente mensaje DSA-REQ. Este mensaje se utiliza para establecer parámetros ascendentes y descendentes. El tamaño de concesión no solicitada ascendente se calcula como 120 (a partir de Tspec) más 18 (tara Ethernet) menos 40 (supresión de la cabecera) más 13 (tara J.112). La supresión de cabecera, especificada con una longitud de 40 en RSVP-PATH, hace referencia a los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se toma del paquete RSVP.

DSA-REQ (petición DSA)

ID de transacción		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSA-REQ (petición DSA)

DownstreamPacketClassification (clasificación de paquetes descendentes)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactivo(0)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7120
	IPProtocol	UDP (17)
PayloadHeaderSuppression (supresión de cabecera de carga útil)	ClassifierIdentifier	3001
	ServiceFlowIdentifier	1001
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42bytes>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Verificar (0)
HMAC		

5) Simultáneamente con el mensaje N.º 2, el AN inicia las reservas de red troncal que sean necesarias para la calidad de servicio requerida. El contenido de este mensaje es función de los algoritmos específicos empleados en la red troncal y queda fuera del campo de aplicación de esta Recomendación. El encaminador de la red troncal enviará al AN una notificación que indique que la reserva ha tenido éxito.

6) El CM verifica los recursos que debe asignar (por ejemplo, espacio del cuadro de supresión de cabecera, los ID de flujos de servicio, espacio del cuadro clasificador, anchura de banda de la red local) e instala los clasificadores. Si la operación tiene éxito, devuelve el mensaje DSA-RSP (respuesta DSA) indicando dicha circunstancia.

DSA-RSP (respuesta DSA)

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

7) Cuado el AN recibe el DSA-RSP, acusa recibo del mismo con un mensaje DSA-ACK.

DSA-ACK (acuse de recibo DSA).

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

8) Una vez que se completa la reserva J.112, y se ha realizado con éxito la reserva en la red troncal, el AN responde al mensaje RSVP-PATH con un mensaje RSVP-RESV. Éste incluye el ID de recurso que el AN asigna a esta conexión. El mensaje RSVP-RESV se envía con la dirección de fuente MTAt y la dirección de destino MTAo. Todos los encaminadores intermedios lo interceptarán, procesarán y reenviarán como un mensaje RSVP-RESV (reserva RSVP) 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	b	120	Estos campos identifican los recursos reservados para este flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

9) Si la dirección del tramo previo difiere de la dirección de fuente, el AN debe generar un mensaje RSVP-PATH para 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, se supone que existe un encaminador intermedio entre MTAo y su CM, pero no entre el MTAt y su CM.

El AN construye un mensaje RSVP-PATH utilizando la información de trayecto inverso recibida en el mensaje RSVP-PATH y envía el mensaje 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 replican como si el mensaje RSVP procediese del extremo lejano.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Tspec de emisor	b	120	El Tspec de emisor procede de Tspec de emisor inversa incluida en el mensaje RSVP-PATH del MTAo. Permite identificar los recursos que serán necesarios en el sentido descendente (del MTAt al MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
ID de recurso		1	Nuevo ID de recurso creado para esta reserva.

10) En respuesta a RSVP-PATH (7), el MTAo envía al MTAt el mensaje RSVP-RESV. Este mensaje se envía con el bit "alerta de encaminador" fijado de forma que todos los encaminadores intermedios interceptan, procesan y reenvían este mensaje hasta que alcanza el AN.

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	b	120	Estos valores también se copian del mensaje RSVP-PATH y especifican la cantidad de recursos reservados para el flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
	R	12 000	
	S	0	
ID de recurso		1	ID de recurso, copiado de RSP-PATH.

11) El CMS envía al AN el mensaje de coordinación de puertas para informarle que los recursos deberían comprometerse. Si el AN no recibe del MTA un mensaje COMMIT antes de que venza el temporizador T2, aborta la conexión.

GATE-OPEN (apertura de puerta)

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		37125	ID de puerta en el AN distante.
HMAC			Suma de control de seguridad para este mensaje.

12) El AN responde a GATE-OPEN con:

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

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

13) En respuesta a la instrucción modificación de conexión, que indica que la llamada se ha completado (es decir que el otro lado ha descolgado), el MTAo envía al AN el mensaje COMMIT. Este mensaje se envía al AN a través de un puerto UDP incluido en el objeto entidad compromiso de RSVP-RESV. El objeto sesión y la plantilla de emisor proporcionan al AN información suficiente para identificar la "puerta" y los recursos reservados que se han comprometido.

COMMIT (compromiso)

Objeto sesión	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente y puerto de destino deben concordar con los 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 ANo envía al servidor de mantenimiento de registros (RKS) el registro de evento que indica que se ha concedido a esta llamada una conexión de calidad de servicio mejorada.

QoS-START (inicio de QoS)

Cabecera	Indicación de tiempo	<time>	Instante en el que se registra el evento
	ID de correlación de facturación	<string>	ID de correlación en el establecimiento de puerta.
Descriptor de QoS	Tipo	UGS	Descripción de la QoS proporcionada a esta conexión.
	Intervalo de concesión	10 ms	
	Fluctuación de fase de la concesión	2 ms	
	Concesión/Intervalo	1	
	Tamaño de concesión	111	
Puerto MTA	Puerto	7120	

15) El AN determina la reserva que debe activarse y envía al CM un mensaje DSC-REQ (petición DSC) para activar el flujo.

DSC-REQ (petición DSC)

ID de transacción		2
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification (Clasificación de paquete ascendente)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Activar (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSC-REQ (petición DSC)

DownstreamPacketClassification (Clasificación de paquete descendente)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Activar (1)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

16) El CM envía un mensaje DSC-RSP (respuesta DSC) que indica que la operación ha tenido éxito.

DSC-RSP (respuesta DSC)

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

17) El AN envía un mensaje DSC-ACK para indicar que se ha recibido el mensaje DSC-RSP y que está de acuerdo con él.

DSC-ACK (acuse de recibo DSC)

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

18) El AN acusa recibo de COMMIT con:

COMMIT-ACK (acuse de COMMIT)

Objeto sesión	Protocolo	UDP	El protocolo, la dirección de destino, la dirección de fuente y el puerto de destino pueden ayudar en 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	

19) Cuando finaliza la llamada, el MTA envía al AN un mensaje RSVP-PATH-TEAR en respuesta a una instrucción supresión de conexión. Para cada reserva RSVP, el MTA envía un mensaje RSVP-PATH-TEAR independiente.

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	

20) El AN envía al servidor de mantenimiento de registros la notificación de que la llamada ha finalizado.

QoS-Stop (parada de QoS)

Indicación de tiempo		<time>	Hora a la que se registra el evento.
Cabecera	Indicación de tiempo	<time>	Hora a la que se registra el evento.
	ID de correlación de facturación	<string>	ID de correlación del mensaje establecimiento de puerta.
SF-ID	SF-ID	1001	Identificador de flujo de servicio.

21) Cuando el AN recibe RSVP-PATH-TEAR, envía el mensaje de coordinación de puerta a la dirección incluida en la instrucción GATE-SET, que en el caso de NCS es el agente de llamada.

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta
ID de puerta		8095	Identifica el ID de puerta en el AN distante.
HMAC			Suma de control de seguridad para este mensaje

El CMS responde con:

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta
HMAC			Suma de control de seguridad para este mensaje

22) Cuando el AN recibe RSVP-PATH-TEAR, envía al CM un DSD-REQ indicando el ID de flujo de servicio que debe eliminarse.

DSD-REQ (petición DSD)

ID de transacción		3
ID de flujo de servicio		1001
HMAC		

DSD-REQ

ID de transacción		4
ID de flujo de servicio		2001
HMAC		

23) El CM suprime el ID de flujo de servicio y envía al AN la respuesta.

DSD-RSP

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

DSD-RSP (respuesta DSD)

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

24) El AN envía al MTA el mensaje RSVP-RESV-TEAR.

RSVP-RESV-TEAR (deshacer trayecto RSVP)

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 a fin de determinar el nuevo códec que va a utilizarse. La nueva especificación de flujo para la llamada se describe en el mensaje RSVP-PATH y debe ajustarse a la envolvente autorizada especificado en el mensaje establecimiento de puerta que anteriormente se ha intercambiado entre los GC y los AN para esta puerta. El RSVP-PATH incluye el mismo ID de puerta que se había utilizado previamente para esta llamada. Debe notarse que el mensaje INVITE (invitación) inicial para establecer la llamada debería haber incluido en el SDP los códecs a fin de asegurar que la envolvente autorizada es suficientemente amplia como para incluir el cambio de módem. El mensaje RSVP-PATH incluye la especificación de flujo para ambos códecs tal como se explica a continuación.

IV.1 Ejemplo de flujo de llamada con mensajes de J.112 Anexo A

Queda en estudio.

IV.2 Ejemplo de flujo de llamada con mensajes del J.112 Anexos B y C

Véase la figura IV.1.

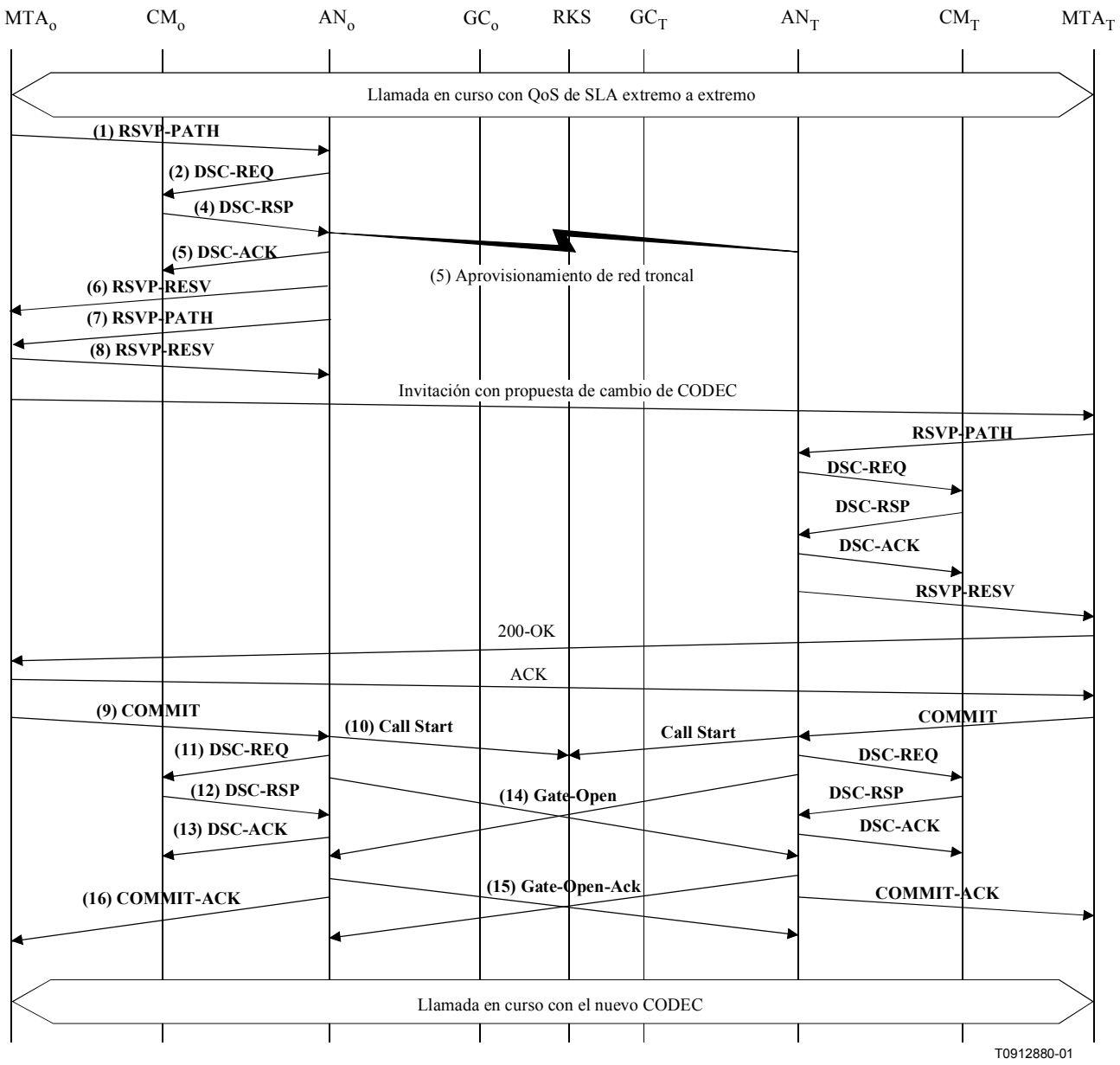


Figura IV.1/J.163 – Señalización de QoS para el cambio de códec

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 CODEC G.711 (paquetes de 10 ms, cada uno de 120 bytes). Después de un intercambio inicial de señalización que determina que el MTAt puede manejar el nuevo CODEC, el MTAo envía al MTAt un mensaje RSVP-PATH, pero con el bit alerta de encaminador fijado en la cabecera IP. Los encaminadores intermedios en la LAN originaria interceptan, procesan y reencaminan este mensaje como un mensaje RSVP-PATH normal, del que sólo pueden interpretar el conjunto de parámetros de tráfico del límite mínimo superior incluidos en el Tspec de emisor.

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	
Tspec de emisor	b	120	Estos parámetros constituyen el límite mínimo superior de todos los parámetros de tráfico individuales de 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 AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
ID de puerta		37125	Identidad de la puerta que autoriza esta petición.
Tspec componente	b	120	Parámetros de tráfico negociados para el nuevo CODEC solicitado para esta llamada. El AN calcula los parámetros reales de QoS en sentido ascendente utilizando estos parámetros Tspec y Rspec.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	12 000	Rspec que se corresponde con la Tspec componente inmediatamente precedente.
	S	0	
Sesión inversa	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al AN 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 inversa	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
Tspec de emisor inversa	b	120	Parámetros de tráfico negociados para el CODEC solicitado para esta llamada. El AN calcula los parámetros reales de QoS en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP, que es ignorado por los encaminadores intermedios.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	0	
	VAD	Desact.	
Rspec inversa	R	12 000	
	S	0	

RSVP-PATH (trayecto RSVP)

Tspec componente	b	80	Parámetros de tráfico negociados para el anterior CODEC utilizado en esta llamada. El AN calcula los parámetros reales de QoS en sentido ascendente utilizando estos parámetros Tspec y Rspec.
	r	4 000	
	p	4 000	
	m	80	
	M	80	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	4 000	Rspec que se corresponde con la Tspec componente inmediatamente precedente
	S	0	
Sesión inversa	Protocolo	UDP	Nuevos objetos RSVP que proporciona al AN información suficiente para calcular los parámetros de tráfico descendente y para generar un mensaje RSVP-PATH para el flujo descendente.
	Dirección de destino	MTAo	
	Puerto de destino	7120	
Plantilla de emisor inversa	Dirección de fuente	MTAt	
	Puerto de fuente	7000	
Tspec de emisor inversa	b	80	Parámetros de tráfico negociados para el anterior CODEC utilizado en esta llamada. El AN calcula los parámetros reales de QoS en sentido descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que será ignorado por los encaminadores intermedios.
	r	4 000	
	p	4 000	
	m	80	
	M	80	
	Supresión de cabecera	0	
	VAD	Desact.	
Rspec inversa	R	4 000	
	S	0	

2) El AN utiliza el mensaje RSVP-PATH y calcula los nuevos parámetros de QoS para el enlace J.112. Dado que el tren G.728 se ajusta plenamente a una asignación realizada para G.711, no es necesario disponer de un flujo de servicio separado; por lo tanto, los flujos de servicio existentes se modifican para incrementar la anchura de banda admisible. El AN envía al CM el siguiente mensaje DSC-REQ. Este mensaje se utiliza para establecer parámetros ascendentes y descendentes. El tamaño de concesión no solicitada ascendente se ha calculado como 120 (de Tspec) más 18 (tara Ethernet) menos 40 (supresión de cabecera) más 13 (tara J.112). La supresión de la cabecera, si bien se ha especificado con una longitud de 40 en el RSVP-PATH, hace referencia a los 42 bytes de la Ethernet/IP/UDP. El contenido de la cabecera suprimida se toma del paquete RSVP.

DSC-REQ (petición DSC)

ID de transacción		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Activo (4)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	20 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	71
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido (2)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Activo (4)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	4 000
HMAC		

3) Simultáneamente con el mensaje N.º 2, el AN 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 AN cualquier notificación precisa para indicar que la reserva ha tenido éxito.

4) El CM verifica los recursos adicionales que debe asignar (por ejemplo, anchura de banda de red local). Si la operación tiene éxito devuelve el mensaje DSC-RSP (respuesta DSC) indicando el éxito.

DSC-RSP (respuesta DSC)

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

5) Cuando el AN 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		Éxito (0)
HMAC		

6) Una vez que ha completado la reserva J.112 y se ha realizado con éxito la reserva en la red troncal, el AN responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. El mensaje incluye el límite mínimo superior de las dos Tspec de emisor, de forma que los encaminadores intermedios asignen recursos suficientes para cualquiera de los dos flujos. El mensaje RSVP-RESV se envía con la dirección de fuente MTAt y con la dirección de destino MTAo. Todos los encaminadores intermedios interceptan, procesan y reenvían este mensaje como un mensaje RSVP-RESV normalizado.

RSVP-RESV (reserva RSVP)

Objeto sesión	Protocolo	UDP	Campos que identifican el flujo IP para el que se ha establecido la reserva.
	Dirección de destino	MTAt	
	Puerto de destino	7000	
Especificación de filtro	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
Especificación de flujo	b	120	Campos que identifican los recursos reservados para este flujo. Dichos valores constituyen el límite mínimo superior de las dos Tspec incluidas en RSVP-PATH.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ID de recurso		1	ID de recurso previamente creado para esta reserva.

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

El AN construye un mensaje RSVP-PATH utilizando información del trayecto inverso que ha recibido en el mensaje RSVP-PATH y envía el mensaje 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 replican 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	

RSVP-PATH (trayecto RSVP)

Tspec de emisor	b	120	La Tspec de emisor procede de la Tspec de emisor inversa del mensaje RSVP-PATH procedente del MTAo. Identifica los recursos que serán necesarios en sentido descendente (del MTAt al MTAo). Esta Tspec es el límite mínimo superior de las dos Tspec individuales enviadas al AN, que hacen que todos los encaminadores intermedios asignen recursos suficientes para cualquiera de los flujos.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	12 000	
	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. Este mensaje se envía con el bit "alerta de encaminador" fijado, de forma que todos los encaminadores intermedios interceptan, procesan y reenvían este mensaje hasta que alcanza el AN.

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	b	120	Los valores e estos parámetros también se copian del mensaje RSVP-PATH y especifican la cantidad de recursos reservados para el flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
	R	12 000	
	S	0	
ID de recurso		1	ID de recurso copiado del RSP-PATH.

9) En respuesta a los mensajes de señalización extremo a extremo que indican que la reserva de recursos ha tenido éxito en ambos extremos, el MTAo envía al AN el mensaje COMMIT. Este mensaje se envía a un puerto UDP del AN que se determina mediante señalización de llamada.

El objeto sesión y la plantilla de emisor proporcionan al AN información necesaria para verificar la ID 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 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 ANo envía al servidor de mantenimiento de registros el registro de evento que informa que se ha recibido un mensaje compromiso (*Commit*) en esta llamada. Este mensaje sólo es una muestra de lo que podría incluirse en un mensaje inicio de QoS (*QoS-Start*).

QoS-START (inicio de QoS)

Cabecera	Indicación de tiempo	<time>	Hora a la que se registra el evento.
	ID de correlación de facturación	<string>	ID de correlación del mensaje establecimiento de puerta.
Descriptor de QoS	Tipo	UGS	Descripción de la QoS proporcionada para esta conexión.
	Intervalo de concesión	10ms	
	Fluctuación de fase de la concesión	2ms	
	Concesión/Intervalo	1	
	Tamaño de concesión	111	
Puerto MTA	Puerto	7120	

11) El AN decide qué reserva se debe de activar y envía al CM un mensaje DSC-REQ para activar el flujo.

DSC-REQ (petición DSC)

ID de transacción		2
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
HMAC		

12) El CM envía un mensaje DSC-RSP (respuesta DSC) que indica que la operación ha tenido éxito.

DSC-RSP (respuesta DSC)

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

13) El AN envía un mensaje DSC-ACK (acuse de recibo DSC) para indicar que se ha recibido el mensaje DSC-RSP y que está de acuerdo con él.

DSC-ACK (acuse de recibo DSC)

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

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

GATE-OPEN (apertura de puerta)

ID de transacción		74	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		1273	ID de puerta en el AN distante.
Tspec	b	120	Parámetros de tráfico comprometidos que están siendo utilizados en el sentido de MTAo a MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Tspec inversa	b	120	Parámetros de tráfico que están siendo utilizados en el sentido del MTAt al MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Suma de control de seguridad para este mensaje.

15) El AN distante responde al mensaje GATE-OPEN con:

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

ID de transacción		74	Identificador para hacer corresponder este mensaje con su respuesta
HMAC			Suma de control de seguridad para este mensaje

16) El AN acusa recibo del mensaje COMMIT con:

COMMIT-ACK (acuse de recibo de compromiso)

Objeto sesión	Protocolo	UDP	El protocolo, dirección de destino, dirección de fuente y 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 del protocolo para la retención de llamada

La retención de llamada en un MTA se realiza enviando a éste un mensaje INVITE con los parámetros SDP puestos a cero. Ello da lugar a que el MTA envíe un mensaje COMMIT cuya especificación de flujo es 0. Asimismo se incluye un ID de recurso. Ello permite al AN retener los recursos admitidos, pero no comprometer ningún recurso en el flujo. Ello se realiza mediante un intercambio de mensajes MAC al nivel de MAC J.112.

V.1 Ejemplo de flujo de llamada con mensajes de J.112 Anexo A

Véase la figura V.1.

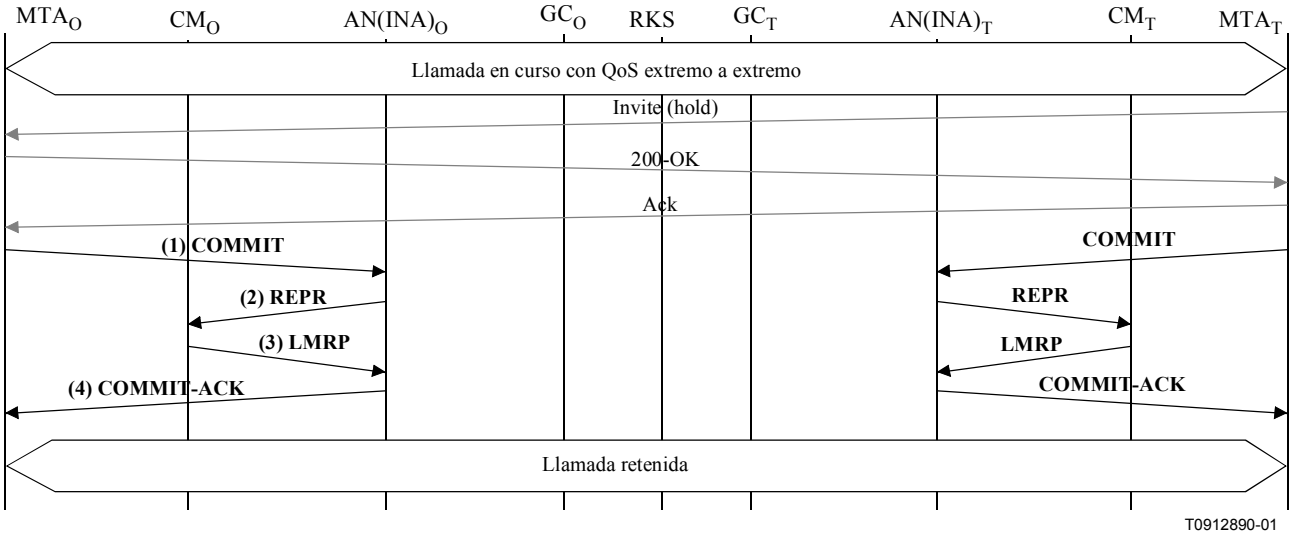


Figura V.1/J.163 – Señalización de QoS para retención de llamada

1) Cuando el MTAt decide que se debe retener la llamada en curso, envía al MTAo un mensaje INVITE. Después de un intercambio adicional de señalización de llamada, el MTAo envía un mensaje COMMIT con una especificación de flujo vacía.

COMMIT (compromiso)

Objeto sesión	Protocolo	UDP	El objeto sesión y la plantilla de emisor verifican la identidad de la puerta.
	Dirección de destino	MTAt	
	Puerto de destino	7000	

COMMIT (compromiso)

Plantilla de emisor	Dirección de fuente	MTAo	
	Puerto de fuente	7120	
ID de puerta		37125	
Especificación de flujo	b	0	Una especificación de flujo es un objeto opcional de un mensaje COMMIT e indica que la cantidad de recursos comprometidos difiere de los recursos reservados; en caso de retención de llamada, los recursos comprometidos en sentido ascendente pasan a ser cero.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	
Especificación de flujo inversa	b	0	Una especificación de flujo es un objeto opcional para un mensaje COMMIT e indica que la cantidad de recursos comprometidos difiere de los recursos reservados; en caso de retención de llamada, los recursos comprometidos en sentido descendente pasan a ser cero.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	

2) El ANo envía al CMt un mensaje reaprovisionamiento.

REPR (reaprovisionamiento)

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <no>
Delete_Reservation_Ids	1 <yes>
New_Downstream_IB_Frequency_included	0 <no>
New_Downstream_OOB_Frequency_included	0 <no>
New_Upstream_Frequency_included	0 <no>
New_Frame_Length_included	1 <yes>
New_Cyclical_Assignment_included	1 <yes>
New_Slot_List_included	0 <no>
New_Frame_Length	0
Number_of_Connections	1
Connection_ID	37125 <Gate ID>
Cyclic_Assignment	
Fixedrate_Start	0xFFFF
Fixedrate_Dist	0
Fixedrate_Stop	0xFFFF

3) El CMt envía un mensaje respuesta de gestión de enlace (LMRP que indica que la operación se ha realizado con éxito.

LMRP (respuesta de gestión de enlace)

Link_Management_Msg_Number	<Reprovision Message Type Value>

4) El ANo acusa recibo del mensaje COMMIT con un mensaje COMMIT-ACK.

COMMIT-ACK (acuse de recibo de compromiso)

Objeto sesión	Protocolo	UDP	El protocolo, dirección de destino, dirección de fuente y 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	

V.2 Ejemplo de flujo de llamada con mensajes de J.112 Anexos B y C

Véase la figura V.2.

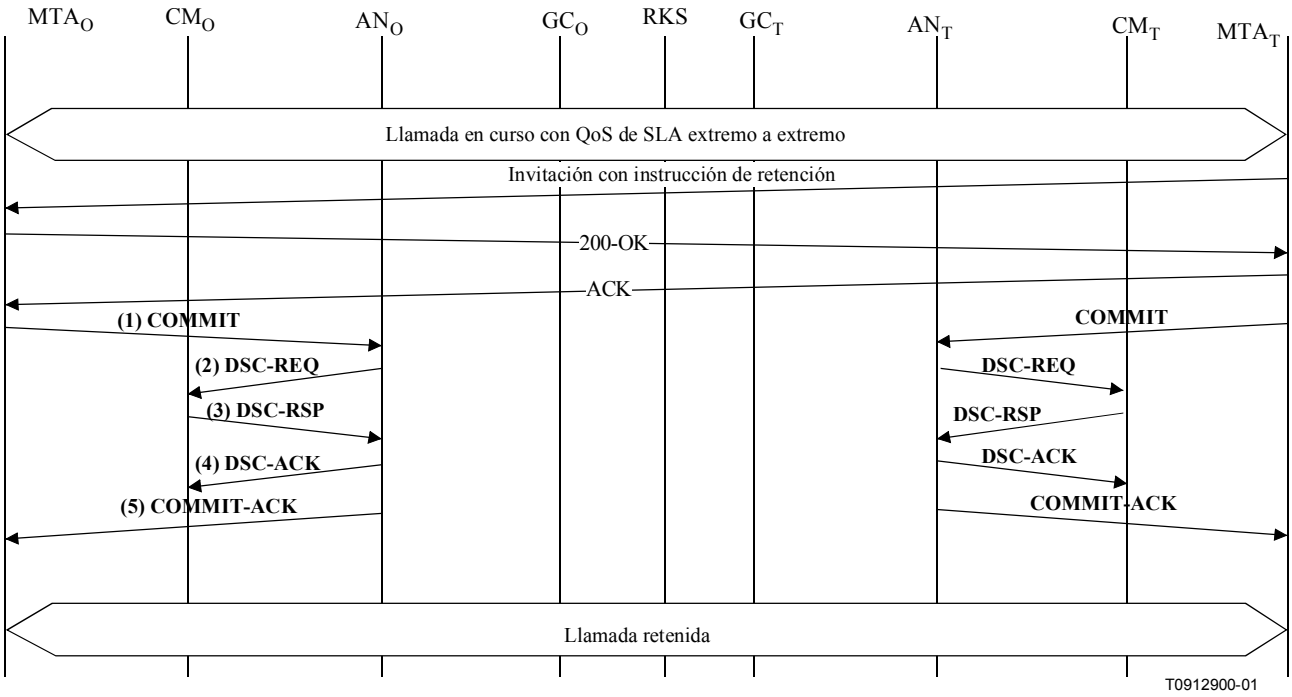


Figura V.2/J.163 – Señalización de QoS para la retención de llamada

1) Cuando el MTA decide que la llamada en curso debe quedar retenida, envía un mensaje de compromiso con una anchura de banda nula. El MTA no puede modificar el ID de sesión activa durante un mensaje de compromiso de retención de 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	b	0	Son opcionales en un mensaje COMMIT e indican que la cantidad de recursos activados difiere de los recursos que habían sido reservados; en este caso, la activación deseada en sentido ascendente es nula.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	
Especificación de flujo inversa	b	0	Son opcionales en un mensaje COMMIT e indican que la cantidad de recursos activados difiere de los recursos que habían sido reservados; en este caso, la activación deseada en sentido descendente es nula.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	

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

DSC-REQ (petición DSC)

ID de transacción		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSC-REQ (petición DSC)

DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

3) El CM envía un mensaje DSC-RSP que indica que la operación ha tenido éxito.

DSC-RSP

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

4) El AN envía un mensaje DSC-ACK para indicar que se ha recibido el mensaje DSC-RSP y que está de acuerdo con él.

DSC-ACK (acuse de recibo DSC)

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

5) El AN 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 con mensajes de J.112 Anexo A

Queda en estudio.

VI.2 Ejemplo de flujo de llamada con mensajes de J.112 Anexos B y C

Véase la figura VI.1.

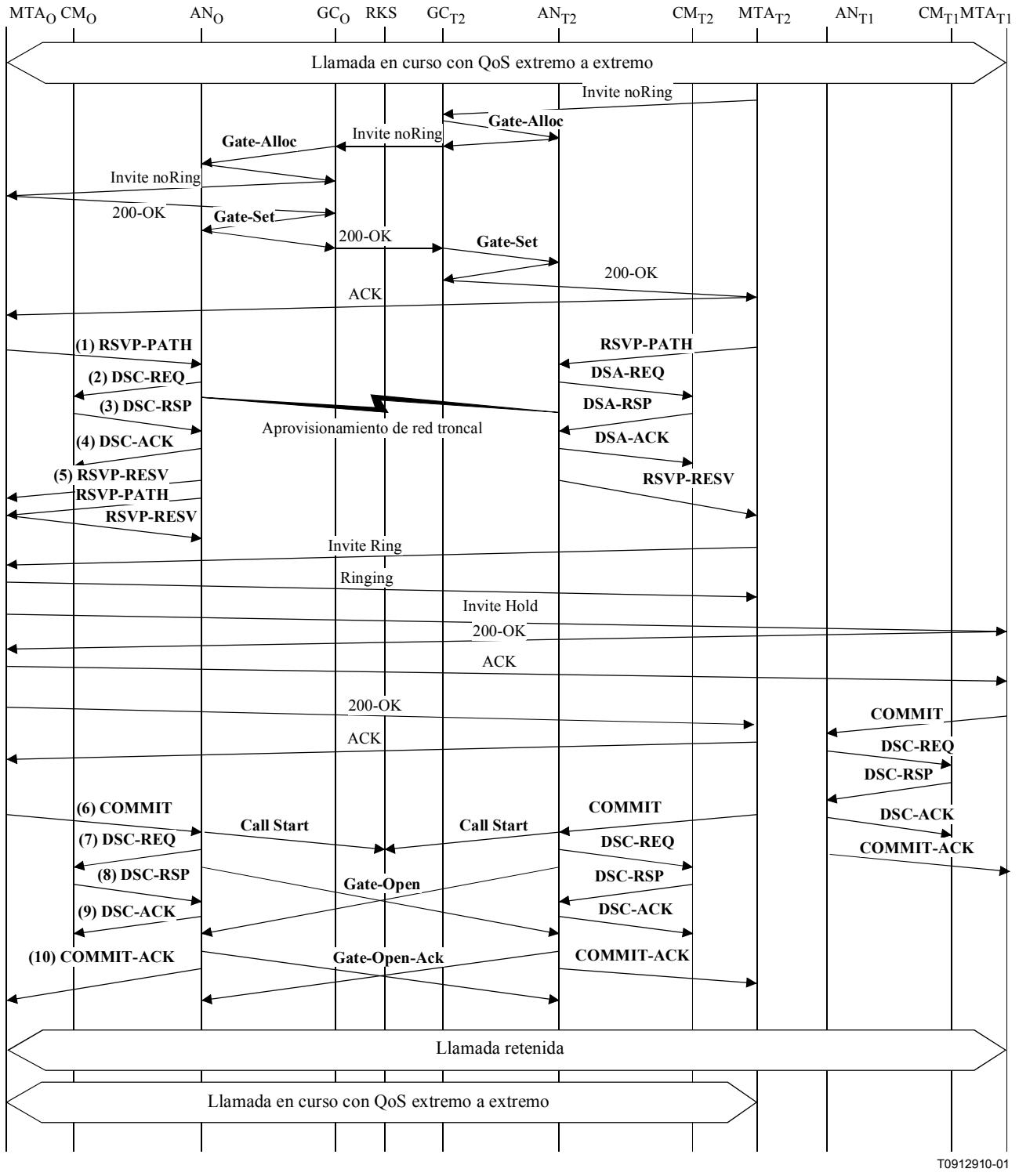


Figura VI.1/J.163 – Señalización de QoS para llamada en espera

1) El MTAo se conecta al MTAt1 y recibe una llamada entrante del MTAt2. En este ejemplo, se supone que la llamada procedente del MTAt1 ha utilizado el puerto 7120 y el ID de recurso asignado 472. Cuando se recibe información de señalización de llamada, el MTAo envía al MTAt2 un mensaje RSVP-PATH, pero con el bit de alerta de encaminador fijado en la cabecera IP. Los encaminadores intermedios en la LAN originaria interceptan, procesan y reenvían este mensaje como un mensaje RSVP-PATH normal, asumiendo que se trata de un flujo separado y asignando recursos independientes para el mismo.

RSVP-PATH

Objeto sesión	Protocolo	UDP	Parámetros que conforman el 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	
Tspec de emisor	b	120	Parámetros de tráfico negociados solicitados para esta llamada. El AN calcula los parámetros reales de QoS 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 AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	40	
	VAD	Desact.	
Rspec directa	R	12 000	
	S	0	
Sesión inversa	Protocolo	UDP	Nuevos objetos RSVP que proporcionan al AN 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 inversa	Dirección de fuente	MTAt	
	Puerto de fuente	0	
Tspec de emisor inversa	b	120	Parámetros de tráfico negociados solicitados para esta llamada. El AN calcula los parámetros reales de QoS descendente utilizando estos parámetros Tspec y Rspec. Es un nuevo objeto RSVP que será ignorado por los encaminadores intermedios.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Supresión de cabecera	0	
	VAD	Desact.	
Rspec inversa	R	12 000	
	S	0	
ID de recurso		472	ID de recurso asignado de llamada existente.
ID de puerta		37126	ID de puerta para esta nueva llamada que toma los recursos de la anterior.

2) El AN 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 y que, por lo tanto, los requisitos de anchura de banda son idénticos. Por consiguiente, el flujo de servicio existente puede ser utilizado por ambos trenes de paquetes. El AN envía al CM el siguiente mensaje DSC-REQ, que establece los nuevos clasificadores. La supresión de la cabecera, que en el mensaje RSVP-PATH se especifica con una longitud de 40 bytes, hace referencia a los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se toma del paquete RSVP.

DSC-REQ (petición DSC)

ID de transacción		1
UpstreamPacketClassification (Clasificación de paquete ascendente)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3003
	ClassifierChangeAction	Añadir (0)
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7122
	IPDestinationAddress	MTAt2
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification (Clasificación de paquete descendente)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3004
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAt2
	IPDestinationAddress	MTAo
	IPDestinationPort	7122
	IPProtocol	UDP (17)
PayloadHeaderSuppression (Supresión de cabecera de la carga útil)	ClassifierIdentifier	3003
	ServiceFlowIdentifier	1001
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42bytes>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Verificación (0)
HMAC		

3) El CM verifica los recursos que debe asignar (por ejemplo, espacio para el cuadro de supresión de cabecera, los ID de flujo de servicio, espacio del cuadro del clasificador, anchura de banda de la red local) e instala los clasificadores. Si la operación tiene éxito, devuelve el mensaje DSC-RSP (respuesta DSC) señalando el mismo.

DSC-RSP (respuesta DSC)

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

4) Cuando el AN recibe el mensaje DSC-RSP, acusa recibo de éste mediante un mensaje DSC-ACK.

DSC-ACK (acuse de recibo DSC)

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

5) Una vez que se ha completado la reserva J.112 y se ha realizado con éxito la reserva en la red troncal, el AN responde al mensaje RSVP-PATH enviando un mensaje RSVP-RESV. Éste incluye el ID de recurso que el AN asigna a esta conexión. El mensaje RSVP-RESV se envía con la dirección de fuente MTAt y la dirección de destino MTAo. Todos los encaminadores intermedios lo interceptarán, procesarán y reenviarán como a 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	MTAt2	
	Puerto de destino	7000	
Especificación de filtro	Dirección de fuente	MTAo	
	Puerto de fuente	7122	
Especificación de flujo	b	120	Campos que identifican los recursos reservados para este flujo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ID de recurso		472	ID de recurso para esta reserva.

6) En respuesta a un golpe de gancho o al accionamiento del correspondiente interruptor del aparato telefónico, y después de señalizar con las partes anteriormente existentes y con las nuevas, el MTAo envía al AN el mensaje COMMIT. Este mensaje se dirige al AN a través de un puerto UDP determinado mediante señalización de llamada.

7) El objeto sesión y la plantilla del emisor proporcionan al AN información suficiente para identificar la "puerta" y los recursos reservados que han sido comprometidos. 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.

COMMIT (compromiso)

Objeto sesión	Protocolo	UDP	Los valores de protocolo, dirección de destino, dirección de fuente y puerto de destino deben concordar con los del 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	

8) El AN 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
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
Upstream Classifier (Clasificador ascendente)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
Downstream Classifier (Clasificador descendente)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7120
	IPProtocol	UDP (17)

DSC-REQ (petición DSC)

UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3003
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Activo (1)
	IPSourceAddress	MTAo
	IPSourcePort	7122
	IPDestinationAddress	MTAt2
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3004
	ClassifierChangeAction	Sustituir (1)
	ClassifierPriority	150
	ClassifierActivationState	Activo (1)
	IPSourceAddress	MTAt2
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7122
	IPProtocol	UDP (17)
HMAC		

9) El CM envía un mensaje DSC-RSP que indica que la operación ha tenido éxito.

DSC-RSP (respuesta DSC)

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

10) El AN envía un mensaje DSC-ACK (acuse de recibo DSC) para indicar que se ha recibido el mensaje DSC-RSP y que está de acuerdo con él.

DSC-ACK (acuse de recibo DSC)

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

11) El AN 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

VII.1 Ejemplo de flujo de llamada con mensajes de J.112 Anexo A

Véase la figura VII.1.

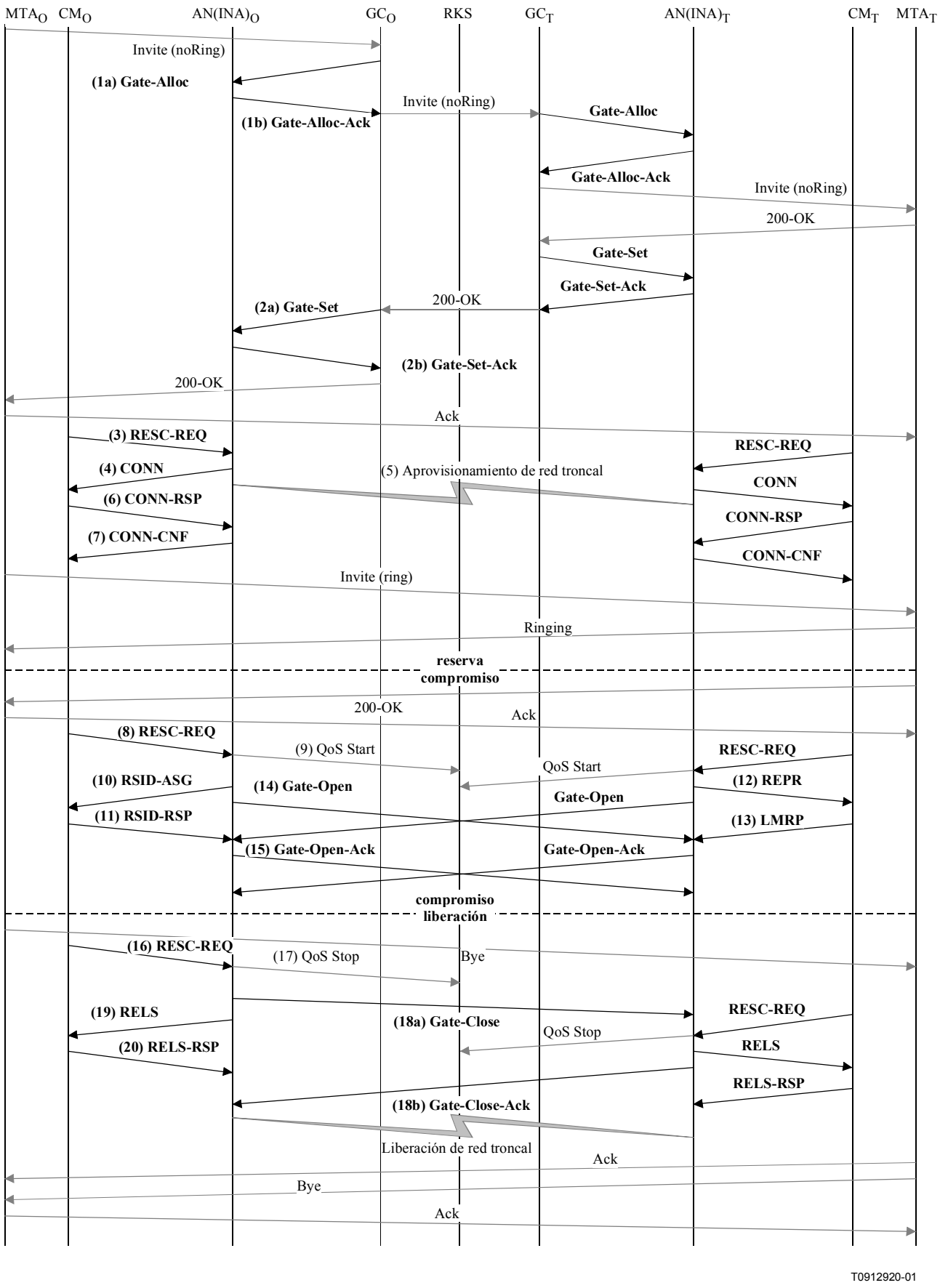


Figura VII.1/J.163 – Flujo de llamada básica con mensajes de J.112 Anexo A – DCS en MTA integrados

1) Cuando el GCo recibe información de señalización del MTAo, verifica el consumo actual de recursos del MTAo consultando al ANo (1a).

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales que utiliza este punto extremo.
Cómputo de actividad		4	Número máximo de puertas permitidas para este abonado.

El ANo verifica la utilización actual de recursos por parte del MTAo, y responde indicando el número de puertas asignadas (1b).

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

ID de transacción		3176	
Abonado		MTAo	Respuesta a la petición de los recursos totales que utiliza este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		3	Número total de puertas establecidas para este abonado.
Puerto de coordinación de puerta		4104	Puerto UDP en el cual el AN espera los mensajes de coordinación de puerta.

2) Tras un intercambio adicional de señalización, el GCo autoriza que el ANo inicie la fase de reserva del proceso de asignación de recursos para el nuevo flujo J.112 (2a).

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición para la especificación de la puerta previamente asignada.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección	ANt	Información necesaria para la coordinación de puerta.
	Puerto	2052	
	ID de puerta distante	1273	
	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 de facturación	<id>	Datos opacos que pasan al RKS cuando se comprometen los recursos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Dirección	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para paquetes ascendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Especificación de puerta	Dirección	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para paquetes descendentes
	T1	180000	Tiempo máximo entre reserva y compromiso
	T2	2000	Tiempo máximo para completar la coordinación de puerta
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

El ANo responde a la instrucción establecimiento de puerta con un acuse de recibo (2b).

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

ID de transacción		3177	
Abonado		MTAo	Respuesta a la petición de especificación de la puerta previamente asignada.
ID de puerta		37125	Identificador de puerta asignada
Cómputo de actividad		4	Número total de puertas establecidas para este abonado.

3) Cuando el MTAo recibe información de señalización de llamada, calcula los parámetros de QoS para el enlace J.112. Utiliza la interfaz de capa MAC para ordenar al CMo que envíe al ANo un mensaje petición de recurso. Suponiendo que se utiliza una velocidad ascendente de 3,088 Mbit/s y que los paquetes IP se encapsulan utilizando DirectIP, los recursos en sentido ascendente se calculan de la forma siguiente. Un paquete IP de un tamaño de 120 bytes (de Tspec) incluyendo los 5 bytes del indicador de fin AAL 5 encaja en 3 células ATM. Por lo tanto, utilizando el modo de acceso de reserva, el ANo tiene que conceder 3 intervalos cada 10 ms. En el modo de acceso de velocidad constante, es necesaria una asignación cíclica de 3 intervalos cada vez con una distancia máxima de 60 intervalos. La anchura de banda requerida es de 360 intervalos cada 1200 ms.

RESC-REQ (petición de recurso)

Resource_Request_ID	0x01
Connection_ID	37125 <Gate ID>
Field	
Aux_Control_Field_included	1 <yes>
Admit_Flag	1 <reservation requested>
Flowspec_DS_included	1 <yes>
Priority_included	0 <no>
Max_packet_size_included	1 <yes>
Session_binding_US_included	0 <no>
Release_requested	0 <no>
Reservation_ID_requested	0 <no>
Cyclic_Assignment_needed	1 <yes>
Requested_Bandwidth	360 <slots per 1 200 ms>
Maximum_Distance_Between_Slots	60 <slots>
Encapsulation	DirectIP (1)
Aux_Control_Field	
IPv6_Add	0 <no>
Flowspec_DS_included	1 <yes>
Session_binding_DS_included	0 <no>
Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

4) El ANo detecta la petición de recurso y no puede hacer concordar el ID de conexión incluido con un flujo J.112 existente. Por lo tanto, verifica la autorización buscando un ID de puerta que concuerde con el ID de conexión. Si la puerta ya había sido establecida, el ANo puede verificar que los recursos solicitados están incluidos en la envolvente autorizada. Si ese es el caso, el ANo envía al CMo el siguiente mensaje conexión. Este mensaje se utiliza para establecer los parámetros ascendentes y descendentes. Sin embargo, en el mensaje conexión no se asignan recursos. Ello indica al CMo que los recursos para el flujo J.112 están reservados pero aún no comprometidos.

CONN (conexión)

Connection_ID	37125 <Gate ID>
Session_number	<not used>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <yes>
IPv6_add	0 <no>
Priority_included	0 <no>
Flowspec_DS_included	0 <no>
Session_binding_US_included	0 <no>
Session_binding_DS_included	0 <no>
Encapsulation_included	1 <yes>
DS_multiprotocol_CBD_included	0 <no>
Resource_number	0x01
Connection_Control_Field	
DS_ATM_CBD_included	0 <no>
DS_MPEG_CBD_included	1 <yes>
US_ATM_CBD_included	1 <yes>
Upstream_Channel_Number	0x1
Slot_list_included	0 <no>
Cyclic_assignment	0 <no>
Frame_Length	0 <no>
Maximum_Contention_Access_Message_Length	1 <slots>
Maximum_Reservation_Access_Message_Length	50 <slots>
Downstream_MPEG_CBD	
Downstream_Frequency	472000000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20000000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)

CONN (conexión)

Connection_control_field2	
Upstream_modulation_included	1 <yes>
Upstream_Modulation	QPSK (1)

5) Simultáneamente con el mensaje N.º 4, el ANo 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 ANo cualquier notificación que sea necesaria para informar que la reserva ha tenido éxito.

6) El CMo verifica los recursos que debe asignar (por ejemplo, contexto de supresión de cabecera, ID de conexiones, contexto de clasificador) e instala los clasificadores. Si la operación se realiza con éxito devuelve el mensaje respuesta de conexión indicando dicha circunstancia.

CONN-RSP (respuesta de conexión)

Connection_ID	37125 <Gate ID>

7) Tras recibir el mensaje respuesta de conexión el ANo acusa recibo con un mensaje confirmación de conexión.

CONN-CNF (confirmación de conexión)

Connection_ID	37125 <Gate ID>

8) En respuesta a los mensajes de señalización que indican que se ha completado el establecimiento de la comunicación (es decir, que el otro lado ha descolgado), el MTAo utiliza la interfaz de capa MAC J.112 para iniciar el compromiso de los recursos reservados. Ello se realiza mediante el envío, por parte del CMo, de un mensaje petición de recurso (RESC-REQ, *resource request*).

RESC-REQ (petición de recurso)

Resource_Request_ID	0x02
Connection_ID	37125 <Gate ID>
Field	
Aux_Control_Field_included	1 <yes>
Admit_Flag	0 <commitment requested>
Flowspec_DS_included	1 <yes>
Priority_included	0 <no>
Max_packet_size_included	1 <yes>
Session_binding_US_included	0 <no>
Release_requested	0 <no>
Reservation_ID_requested	0 <no>
Cyclic_Assignment_needed	1 <yes>
Requested_Bandwidth	360 <slots per 1 200 ms>
Maximum_Distance_Between_Slots	60 <slots>
Encapsulation	DirectIP (1)
Aux_Control_Field	
IPv6_Add	0 <no>
Flowspec_DS_included	1 <yes>
Session_binding_DS_included	0 <no>

RESC-REQ (petición de recurso)

Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

9) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que se ha concedido a esta llamada una calidad de servicio mejorada. En [UIT-T J.164] se describe el formato de este mensaje.

10) El AN puede comprometer los recursos reservados utilizando el modo de acceso de velocidad constante o el modo de acceso de reserva. Cuando se recibe el mensaje petición de recurso, el AN debe enviar los mensajes de capa MAC adecuados para completar el establecimiento de un flujo J.112.

En este ejemplo se asume que el ANo decide utilizar el modo de acceso de reserva mientras que el ANt compromete recursos utilizando el modo de acceso de velocidad constante.

Se utiliza el porteo continuo para acomodar las características de tipo CBR de este tráfico. Para iniciar la transmisión, el ANo envía un mensaje asignación de ID de reserva (RSID-ASG)

RSID-ASG (asignación de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <slots>
GFC_10_Slots	3 <slots>
GFC_01_Slots	1 <slots>

11) El CMo envía un mensaje respuesta de ID de reserva que indica que la operación ha tenido éxito.

RSID-RSP (respuesta de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

12) El ANt en el lado de terminación de la llamada ha decidido proporcionar los recursos solicitados utilizando el modo de acceso de velocidad constante. Para comprometer los recursos e iniciar la transmisión, el ANt envía al CMt un mensaje de reaprovisionamiento.

REPR (reaprovisionamiento)

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <no>
Delete_Reservation_IDs	0 <no>
New_Downstream_IB_Frequency_included	0 <no>
New_Downstream_OOB_Frequency_included	0 <no>
New_Upstream_Frequency_included	0 <no>

REPR (reaprovisionamiento)

New_Frame_Length_included	1 <yes>
New_Cyclical_Assignment_included	1 <yes>
New_Slot_List_included	0 <no>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	1273 <Gate ID>
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

13) El CMt envía un mensaje respuesta de gestión de enlace (LMRP) que indica que la operación ha tenido éxito.

LMRP (respuesta de gestión de enlace)

Link_Management_Msg_Number	<Reprovision Message Type Value>

14) El ANo envía al ANt distante el mensaje de coordinación de puerta para informarle que en el extremo local se han comprometido los recursos.

GATE-OPEN (apertura de puerta)

ID de transacción		72	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		1273	ID de puerta en el AN que recibe este mensaje.
Tspec	b	120	Parámetros de tráfico realmente utilizados por los recursos comprometidos en el flujo del MTAo al MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Tspec inversa	b	120	Parámetros de tráfico esperados utilizados en el flujo del MTAt al MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Suma de control de seguridad para este mensaje.

15) Cuando se recibe el mensaje GATE-OPEN del ANt distante, el ANo responde con un mensaje GATE-OPEN-ACK.

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

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su petición.
HMAC			Suma de control de seguridad para este mensaje.

16) Cuando se termina la llamada, el MTAo utiliza la interfaz de capa MAC J.112 para liberar los recursos reservados. Esto se realiza mediante enviando el CMo un mensaje petición de recursos (RESC-REQ).

RESC-REQ (petición de recursos)

Resource_Request_ID	0x04
Connection_ID	37125 <Gate ID>
Field	
Aux_Control_Field_included	0 <no>
Admit_Flag	0
Flowspec_DS_included	0 <no>
Priority_included	0 <no>
Max_packet_size_included	0 <no>
Session_binding_US_included	0 <no>
Release_requested	1 <yes>
Reservation_ID_requested	0 <no>
Cyclic_Assignment_needed	0 <no>
Requested_Bandwidth	0
Maximum_Distance_Between_Slots	0
Encapsulation	DirectIP (1)

17) El ANo notifica al servidor de mantenimiento de registros (RKS) que la llamada ha terminado. En [UIT-T J.164] se describe el formato de este mensaje de evento.

18) Cuando el ANo recibe la petición para liberar los recursos, envía el mensaje de coordinación de puerta a la dirección incluida en la anterior instrucción GATE-SET, que en el caso de DCS es el ANt que sirve al MTAt (18a).

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		1273	ID de puerta en el elemento de red que recibe este mensaje.
HMAC			Suma de control de seguridad para este mensaje.

El ANt responde con un mensaje GATE-CLOSE-ACK (18b).

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su petición.
HMAC			Suma de control de seguridad para este mensaje.

19) El ANo responde al mensaje petición de recursos enviando al CMo un mensaje liberación que indica el flujo J.112 que debe ser eliminado.

RELS (liberación)

Number_of_Connections	1
Connection_ID	37125 <Gate ID>

20) El CMo libera el flujo J.112 y envía al ANo el mensaje respuesta de liberación.

RELS-RSP (respuesta de liberación)

Connection_ID	37125 <Gate ID>

VII.2 Ejemplo de flujo de llamada con mensajes de J.112 Anexos B y C

Véase la figura VII.2.

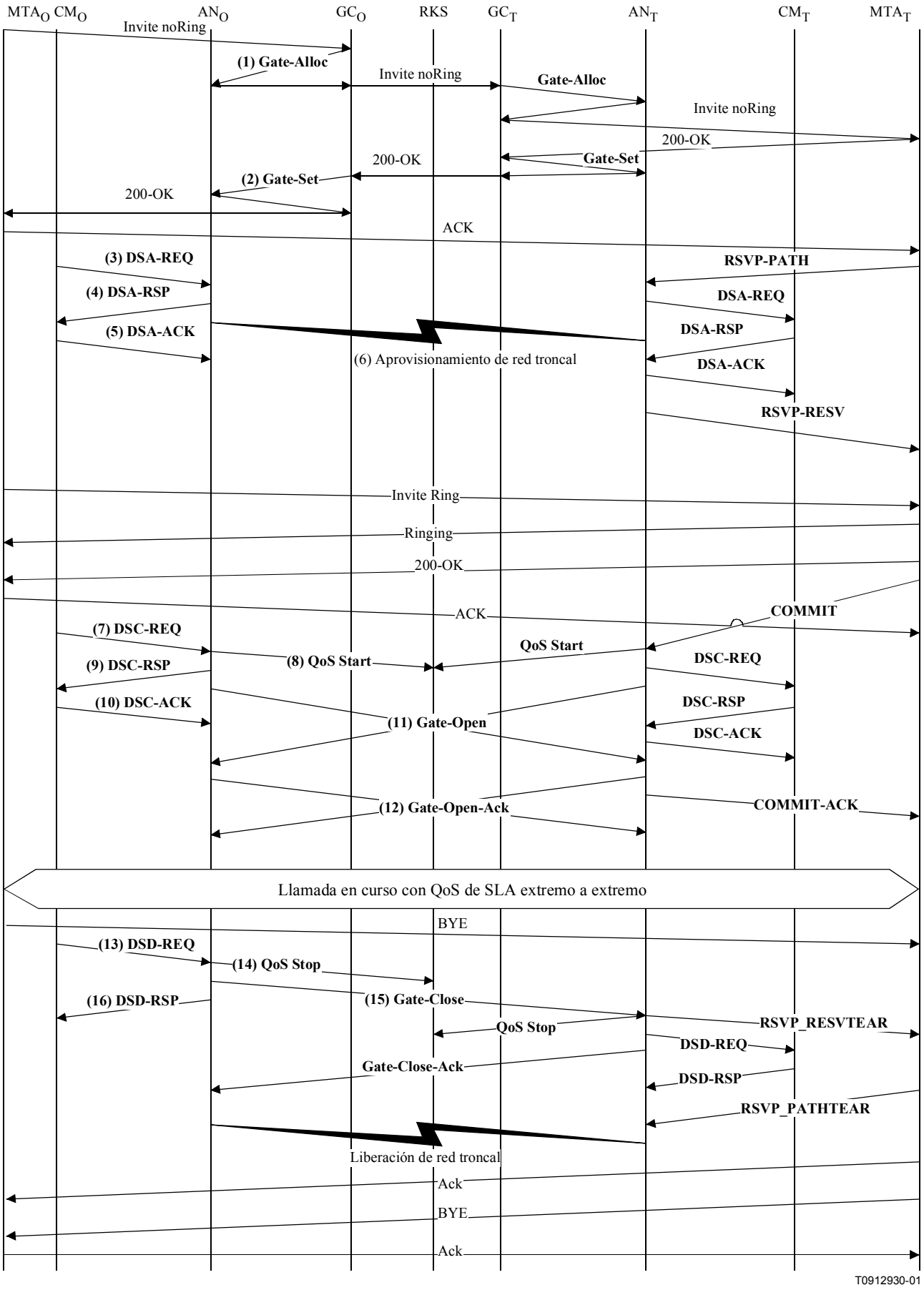


Figura VII.2/J.163 – Flujo de llamada básica – MTA integrado

1) Cuando se recibe información de señalización del MTAo, el GCo verifica el consumo actual de recursos del MTAo consultado al ANo.

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales que utiliza este cliente.
Cómputo de actividad		4	Número máximo de conexiones permitidas por cliente.

El ANo 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 de los recursos totales que utiliza este cliente.
ID de puerta		37125	Identificador de puerta asignada
Cómputo de actividad		3	Número total de conexiones establecidas por este cliente.

2) Tras un intercambio de señalización adicional, el GCo autoriza que el ANo 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 para todos los recursos utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección de AN	ANt	Información necesaria para la coordinación de puerta.
	Puerto de AN	2052	
	ID de puerta distante	1273	
	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 de facturación	<id>	Datos opacos que se pasan el RKS cuando se comprometen los recursos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Protocolo	Ascend.	
	Dirección de fuente	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, fuente y puerto de destino se utiliza en los clasificadores de QoS.
	Dirección de destino	MTAo	
	Puerto de fuente	MTAt	
	Puerto de destino	0	
	Protocolo	7000	
	DSCP	6	Valor de tipo de paquete para paquetes ascendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Especificación de puerta	Dirección	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

3) El ANo 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 de los recursos totales utilizados por este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		4	Número máximo de conexiones que establece el cliente.

4) Cuando el MTAo recibe información de señalización de llamada, calcula los parámetros de QoS para el enlace J.112. Utiliza la interfaz del anexo E al anexo B/J.112 con el CM para enviar al AN el siguiente mensaje DSA-REQ. Este mensaje se utiliza para establecer parámetros en sentido ascendente y descendente. El tamaño de la concesión no solicitada ascendente se calcula como 120 (del SDP) más 18 (tara Ethernet) menos 40 (supresión de cabecera) más 13 (tara J.112). La supresión de cabecera hace referencia a los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se incluye en el mensaje petición DSA (DSA-REQ, *DSA-request*).

DSA-REQ (petición DSA)

ID de transacción		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowReference	1
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37125
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowReference	2
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37125
UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowReference	1
	PacketClassifierReference	1
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSA-REQ (petición DSA)

DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowReference	2
	PacketClassifierReference	2
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
PayloadHeaderSuppression (Supresión de cabecera de carga útil)	ClassifierReference	1
	ServiceFlowReference	1
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42bytes>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Verificación (0)
AuthorizationBlock (Bloque de autorización)		37125
HMAC		

5) El AN verifica la autorización buscando una puerta cuyo ID de puerta concuerde con el valor incluido en AuthBlock, y verifica cuales son los recursos que debe asignar (por ejemplo, espacio del cuadro de supresión de cabecera, los ID de flujos de servicio, espacio del cuadro clasificador) e instala los clasificadores. Si la operación tiene éxito, devuelve el mensaje DSA-RSP (respuesta DSA) indicando dicha circunstancia.

DSA-RSP (respuesta DSA)

ID de transacción		1
Código de confirmación		Éxito (0)
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowReference	1
	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37125

DSA-RSP (respuesta DSA)

DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowReference	2
	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37125
UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowReference	1
	PacketClassifierReference	1
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowReference	2
	PacketClassifierReference	2
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

6) Cuando se recibe el DSA-RSP, el CM acusa recibo de la recepción mediante un mensaje DSA-ACK.

DSA-ACK (acuse de recibo DSA)

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

7) Simultáneamente con el mensaje N.º 4, el AN inicia cualquier reserva de red troncal necesaria 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 red troncal envía al AN la notificación que sea precisa para indicar que la reserva ha tenido éxito.

8) En respuesta a los mensajes de señalización que indican que la llamada se ha completado (es decir, que el otro lado ha descolgado), el MTAo utiliza la interfaz del anexo E al anexo B/J.112 para activar los recursos admitidos. Para ello se utiliza una instrucción DSC-REQ (petición DSC) dirigida al AN.

DSC-REQ (petición DSC)

ID de transacción		2
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Sustitución (1)
	ClassifierPriority	150
	ClassifierActivationState	Activo (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Sustitución (1)
	ClassifierPriority	150
	ClassifierActivationState	Active (1)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

9) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que se ha recibido un compromiso relativo a esta llamada. Este mensaje sólo es una muestra de lo que podría incluirse en el mensaje inicio de QoS.

QoS-START (inicio de QoS)

Cabecera	Indicación de tiempo	<time>	Hora a la que se registra el evento
	ID de correlación de tiempo	<string>	ID de correlación incluido en el mensaje establecimiento de puerta.
Descriptor de QoS	Tipo	UGS	Descripción de la QoS de esta conexión
	Intervalo de concesión	10 ms	
	Fluctuación de fase de la concesión	2 ms	
	Concesión/Intervalo	1	
	Tamaño de concesión	111	
Puerto MTA	Puerto	7120	

10) El AN envía un mensaje DSC-RSP (respuesta DSC) que indica que la operación ha tenido éxito.

DSC-RSP (respuesta DSC)

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

11) El CM envía un mensaje DSC-ACK para indicar que se ha recibido el mensaje DSC-RSP y que está de acuerdo con él.

DSC-ACK (acuse de recibo DSC)

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

12) El AN envía al AN distante el mensaje de coordinación de puerta para informarle que los recursos de este extremo han sido comprometidos.

GATE-OPEN (apertura de puerta)

ID de transacción		72	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		1273	ID de puerta en el AN distante.
Tspec	b	120	Parámetros de tráfico comprometidos utilizados en el sentido del MTAo al MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Tspec inversa	b	120	Parámetros de tráfico esperados utilizados para el flujo en el sentido del MTAt al MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Suma de control de seguridad para este mensaje.

13) El AN distante responde al mensaje GATE-OPEN con:

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

ID de transacción		72	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

14) Cuando finaliza la llamada, el MTA utiliza el anexo E al anexo B/J.112 para eliminar los flujos de servicio enviando al AN un mensaje DSD-REQ (petición DSD).

DSD-REQ (petición DSD)

ID de transacción		3
ID de flujo de servicio		1001
HMAC		

DSD-REQ (petición DSD)

ID de transacción		4
ID de flujo de servicio		2001
HMAC		

15) El AN envía al servidor de mantenimiento de registros una notificación que indica que la llamada ha finalizado. Este mensaje es solo una muestra de lo que se podría incluir en el mensaje parada de QoS; véase UIT-T J.164.

QoS-Stop (parada de QoS)

Indicación de tiempo		<time>	Hora a la que se registra el evento.
Cabecera	Indicación de tiempo	<time>	Hora del evento que debe registrarse.
	ID de correlación de facturación	<string>	ID de correlación del mensaje establecimiento de puerta.
SF-ID	SF-ID	1001	Identificador de flujo de servicio.

16) Cuando el AN recibe el mensaje RSVP-PATH-TEAR, envía el mensaje de coordinación de puerta al correspondiente AN del MTAt.

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		1273	ID de puerta en el AN distante.
HMAC			Suma de control de seguridad para este mensaje.

El AN distante responde con:

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

17) El AN elimina los ID de flujo de servicio y envía al CM la respuesta.

DSD-RSP (respuesta DSD)

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

DSD-RSP (respuesta DSD)

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

APÉNDICE VIII

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

VIII.1 Ejemplo de flujo de llamada con mensajes de J.112 Anexo A

Véase la figura VIII.1.

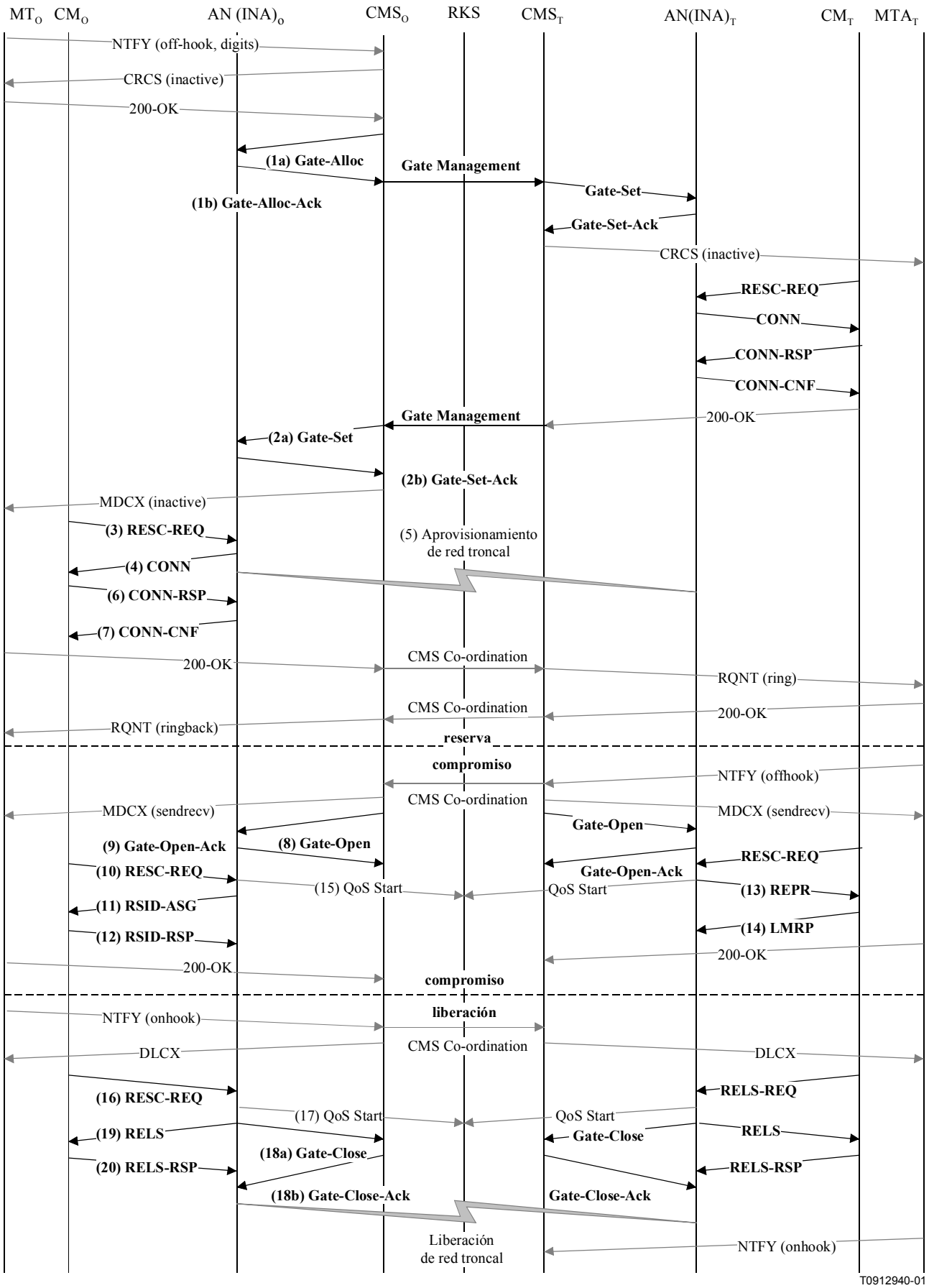


Figura VIII.1/J.163 – Flujo de llamada básica con mensajes de J.112 Anexo A – NCS en MTA integrado

1) Cuando el GCo/CMSo recibe información de señalización del MTAo, verifica el consumo actual de recursos del MTAo consultando al ANo (1a).

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales que utiliza este punto extremo.
Cómputo de actividad		4	Número máximo de puertas permitidas para este abonado.

El ANo verifica la utilización actual de recursos por parte del MTAo, y responde indicando el número de puertas asignadas (1b).

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

ID de transacción		3176	
Abonado		MTAo	Respuesta a la petición de recursos totales que utiliza este punto extremo.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		3	Número máximo de puertas establecidas para este abonado.

2) Tras un intercambio de señalización adicional, el GCo/CMSo autoriza que el ANo inicie la fase de reserva del proceso de asignación de recursos para el nuevo flujo J.112 (2a).

GATE-SET (establecimiento de puerta)

ID de transacción		3177	ID de transacción único para este intercambio de mensajes.
Abonado		MTAo	Petición para la especificación de la puerta previamente asignada.
ID de puerta		37125	Identificador de puerta asignada.
Información de puerta distante	Dirección	CMSo	Información necesaria para realizar la coordinación de puerta. Nótese que el CMSo ha indicado que él es la entidad para intercambiar mensajes de coordinación de puertas. El valor de la bandera indica que el AN no debería enviar un mensaje apertura de puerta cuando recibe un COMMIT del MTA, pero aún espera recibir un mensaje apertura de puerta del CMSo.
	Puerto	2052	
	ID de puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	Sin-apertura-puerta	
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 de facturación	<id>	Dados opacos que pasarán al RKS cuando los recursos estén comprometidos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Dirección	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para los paquetes ascendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puertas.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Especificación de puerta	Dirección	Descend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para los paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puertas.
	b	120	Parámetros de anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

El ANo responde a la instrucción establecimiento de puerta con un acuse de recibo (2b).

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

ID de transacción		3177	
Abonado		MTAo	Petición de la especificación de la puerta previamente asignada.
ID de puerta		37125	Identificador de puerta asignada
Cómputo de actividad		4	Número total de puertas establecidas para este abonado.

3) Cuando el MTAo recibe una instrucción modificación de conexión, calcula los parámetros de QoS para el enlace J.112. Utiliza la interfaz de capa MAC para ordenar al CMo que envíe al ANo un mensaje petición de recurso. Suponiendo una velocidad ascendente de 3,088 Mbit/s y que los paquetes IP se encapsulan utilizando DirectIP, los recursos en sentido ascendente se calculan de la forma siguiente. Un paquete IP de un tamaño de 120 bytes (de Tspec) incluyendo los 5 bytes del indicador de fin AAL 5 encaja en 3 células ATM. Por lo tanto, utilizando el modo de acceso de reserva, el AN tiene que conceder 3 intervalos cada 10 ms. En el modo de acceso de velocidad constante, es necesaria una asignación cíclica de 3 intervalos cada vez con una distancia máxima de 60 intervalos. La anchura de banda requerida es de 360 intervalos por cada 1200 ms.

RESC-REQ (petición de recurso)

Resource_Request_ID	0x01
Connection_ID	37125 <Gate ID>
Field	
Aux_Control_Field_included	1 <yes>
Admit_Flag	1 <reservation requested>
Flowspec_DS_included	1 <yes>
Priority_included	0 <no>
Max_packet_size_included	1 <yes>
Session_binding_US_included	0 <no>
Release_requested	0 <no>
Reservation_ID_requested	0 <no>
Cyclic_Assignment_needed	1 <yes>
Requested_Bandwidth	360 <slots per 1 200 ms>
Maximum_Distance_Between_Slots	60 <slots>
Encapsulation	DirectIP (1)
Aux_Control_Field	
IPv6_Add	0 <no>
Flowspec_DS_included	1 <yes>
Session_binding_DS_included	0 <no>
Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

4) El ANo detecta la petición de recurso y no puede hacer concordar el ID de conexión incluido en el mismo con un flujo J.112 existente. Por lo tanto, verifica la autorización buscando un ID de puerta que concuerde con el ID de conexión. Si la puerta ya había sido establecida, el ANo puede verificar que los recursos solicitados se encuentran en la envolvente autorizada. Si ese es el caso, el ANo envía al CMo el siguiente mensaje conexión. Este mensaje se utiliza para determinar los parámetros ascendentes y descendentes. Sin embargo, en el mensaje conexión no se asignan recursos. Ello indica al CMo que los recursos para dicho flujo J.112 están reservados pero aún no comprometidos.

CONN (conexión)

Connection_ID	37125 <Gate ID>
Session_number	<not used>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <yes>
IPv6_add	0 <no>
Priority_included	0 <no>
Flowspec_DS_included	0 <no>
Session_binding_US_included	0 <no>
Session_binding_DS_included	0 <no>
Encapsulation_included	1 <yes>
DS_multiprotocol_CBD_included	0 <no>
Resource_number	0x01
Connection_Control_Field	
DS_ATM_CBD_included	0 <no>
DS_MPEG_CBD_included	1 <yes>
US_ATM_CBD_included	1 <yes>
Upstream_Channel_Number	0x1
Slot_list_included	0 <no>
Cyclic_assignment	0 <no>
Frame_Length	0 <no>
Maximum_Contention_Access_Message_Length	1 <slots>
Maximum_Reservation_Access_Message_Length	50 <slots>
Downstream_MPEG_CBD	
Downstream_Frequency	472000000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20000000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Connection_control_field2	
Upstream_modulation_included	1 <yes>
Upstream_Modulation	QPSK (1)

5) Simultáneamente con el mensaje N.º 4, el ANo 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 ANo cualquier notificación que sea necesaria para indicar que la reserva se ha realizado con éxito.

6) El CMo verifica los recursos que debe asignar (por ejemplo, contexto de supresión de cabecera, los ID de conexión, contexto de clasificador) e instala los clasificadores. Si la operación se realiza con éxito devuelve el mensaje respuesta de conexión indicando dicha circunstancia.

CONN-RSP (respuesta de conexión)

Connection_ID	37125 <Gate ID>

7) Cuando el ANo recibe el mensaje respuesta de conexión, acusa recibo con un mensaje confirmación de conexión.

CONN-CNF (confirmación de conexión)

Connection_ID	37125 <Gate ID>

8) El CMSo envía al ANo el mensaje de coordinación de puerta para informarle que los recursos se deberían comprometer. Si transcurrido un tiempo razonable el ANo no recibe del CMo un mensaje petición de recurso, revoca la autorización de la puerta.

GATE-OPEN (apertura de puerta)

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		37125	ID de puerta en el AN que recibe este mensaje.
HMAC			Suma de control de seguridad para este mensaje.

9) El ANo responde a GATE-OPEN con un mensaje GATE-OPEN-ACK.

GATE-OPEN-ACK (acuse de apertura de puerta

ID de transacción		8096	Identificador para hacer corresponder este mensaje con su petición.
HMAC			Suma de control de seguridad para este mensaje.

10) En respuesta a una instrucción modificación de conexión que indica que se ha completado el establecimiento de la comunicación (es decir, que el otro lado ha descolgado), el MTAo utiliza la interfaz de capa MAC J.112 para iniciar el compromiso de los recursos reservados. Para ello, el CMo envía un mensaje petición de recurso.

RESC-REQ (petición de recurso)

Resource_Request_ID	0x02
Connection_ID	37125 <Gate ID>
Field	
Aux_Control_Field_included	1 <yes>
Admit_Flag	0 <commitment requested>
Flowspec_DS_included	1 <yes>
Priority_included	0 <no>
Max_packet_size_included	1 <yes>
Session_binding_US_included	0 <no>
Release_requested	0 <no>

RESC-REQ (petición de recurso)

Reservation_ID_requested	0 <no>
Cyclic_Assignment_needed	1 <yes>
Requested_Bandwidth	360 <slots per 1 200 ms>
Maximum_Distance_Between_Slots	60 <slots>
Encapsulation	DirectIP (1)
Aux_Control_Field	
IPv6_Add	0 <no>
Flowspec_DS_included	1 <yes>
Session_binding_DS_included	0 <no>
Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

11) El AN puede comprometer los recursos reservados utilizando el modo de acceso de velocidad constante o el modo de acceso de reserva. Cuando recibe el mensaje COMMIT, debe enviar los mensajes de capa MAC adecuados para completar el establecimiento de un flujo J.112.

En este ejemplo se supone que el ANo decide utilizar el modo de acceso de reserva mientras que el ANt compromete recursos utilizando el modo de acceso de velocidad constante.

Se utiliza el porteo continuo para acomodar las características de tipo CBR de este tráfico. Para iniciar la transmisión, el ANo envía un mensaje asignación de ID de reserva.

RSID-ASG (asignación de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <slots>
GFC_10_Slots	3 <slots>
GFC_01_Slots	1 <slots>

12) El CMo envía un mensaje respuesta de ID de reserva que informa que la operación ha tenido éxito.

RSID-RSP (respuesta de ID de reserva)

Connection_ID	37125 <Gate ID>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

13) El ANt en el lado de terminación de la llamada ha decidido proporcionar los recursos solicitados utilizando el modo de acceso de velocidad constante. Para comprometer los recursos e iniciar la transmisión, el ANt envía al CMt un mensaje de reaprovisionamiento.

REPR (reaprovisionamiento)

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <no>
Delete_Reservation_IDs	0 <no>
New_Downstream_IB_Frequency_included	0 <no>
New_Downstream_OOB_Frequency_included	0 <no>
New_Upstream_Frequency_included	0 <no>
New_Frame_Length_included	1 <yes>
New_Cyclical_Assignment_included	1 <yes>
New_Slot_List_included	0 <no>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	8095 <Gate ID>
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

14) El CMt envía un mensaje respuesta de gestión de enlace (LMRP) que indica que la operación ha tenido éxito.

LMRP (respuesta de gestión de enlace)

Link_Management_Msg_Number	<Reprovision Message Type Value>

15) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que se ha concedido a esta llamada una calidad de servicio mejorada. En [UIT-T J.164] se describe el formato de este mensaje.

16) Cuando la llamada finaliza, en respuesta a la instrucción eliminación de conexión, el MTAo utiliza la interfaz de capa MAC J.112 para liberar los recursos reservados. Para ello, el CMo envía un mensaje petición de recurso.

RESC-REQ (petición de recurso)

Resource_Request_ID	0x04
Connection_ID	37125 <Gate ID>
Field	
Aux_Control_Field_included	0 <no>
Admit_Flag	0
Flowspec_DS_included	0 <no>
Priority_included	0 <no>
Max_packet_size_included	0 <no>
Session_binding_US_included	0 <no>
Release_requested	1 <yes>
Reservation_ID_requested	0 <no>
Cyclic_Assignment_needed	0 <no>

RESC-REQ (petición de recurso)

Requested_Bandwidth	0
Maximum_Distance_Between_Slots	0
Encapsulation	DirectIP (1)

17) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que la llamada ha finalizado. En [UIT-T J.164] se describe el formato de este mensaje.

18) Cuando el ANo recibe un mensaje petición de recurso, envía el mensaje de coordinación de puerta a la dirección incluida en la instrucción GATE-SET anterior, que en el caso de NCS es el agente de llamada (18a).

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		8095	ID de puerta del elemento de red (aquí el CMS) que recibe este mensaje.
HMAC			Suma de control de seguridad para este mensaje.

El CMSo responde con un mensaje GATE-CLOSE-ACK (18b).

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su petición.
HMAC			Suma de control de seguridad para este mensaje.

19) El ANo responde al mensaje petición de recurso enviando al CMo un mensaje liberación que indica el flujo J.112 que debe ser eliminado.

RELS (liberación)

Number_of_Connections	1
Connection_ID	37125 <Gate ID>

20) El CMo libera el flujo J.112 y envía al ANo la respuesta de liberación.

RELS-RSP (respuesta de liberación)

Connection_ID	37125 <Gate ID>

VIII.2 Ejemplo de flujo de llamada con mensajes de J.112 Anexos B y C

Véase la figura VIII.2.

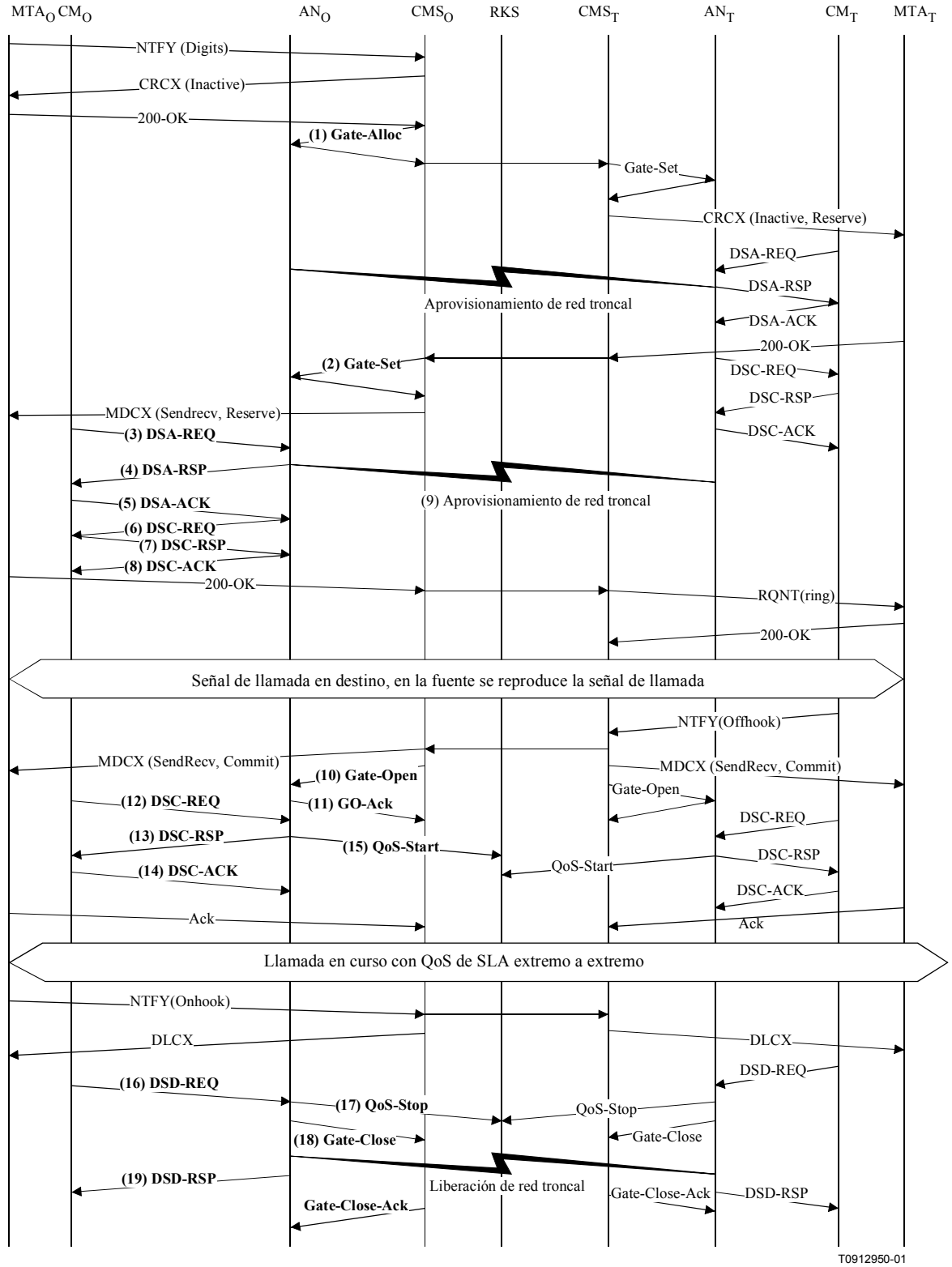


Figura VIII.2/J.163 – Llamada NCS integrada entre elementos de la red

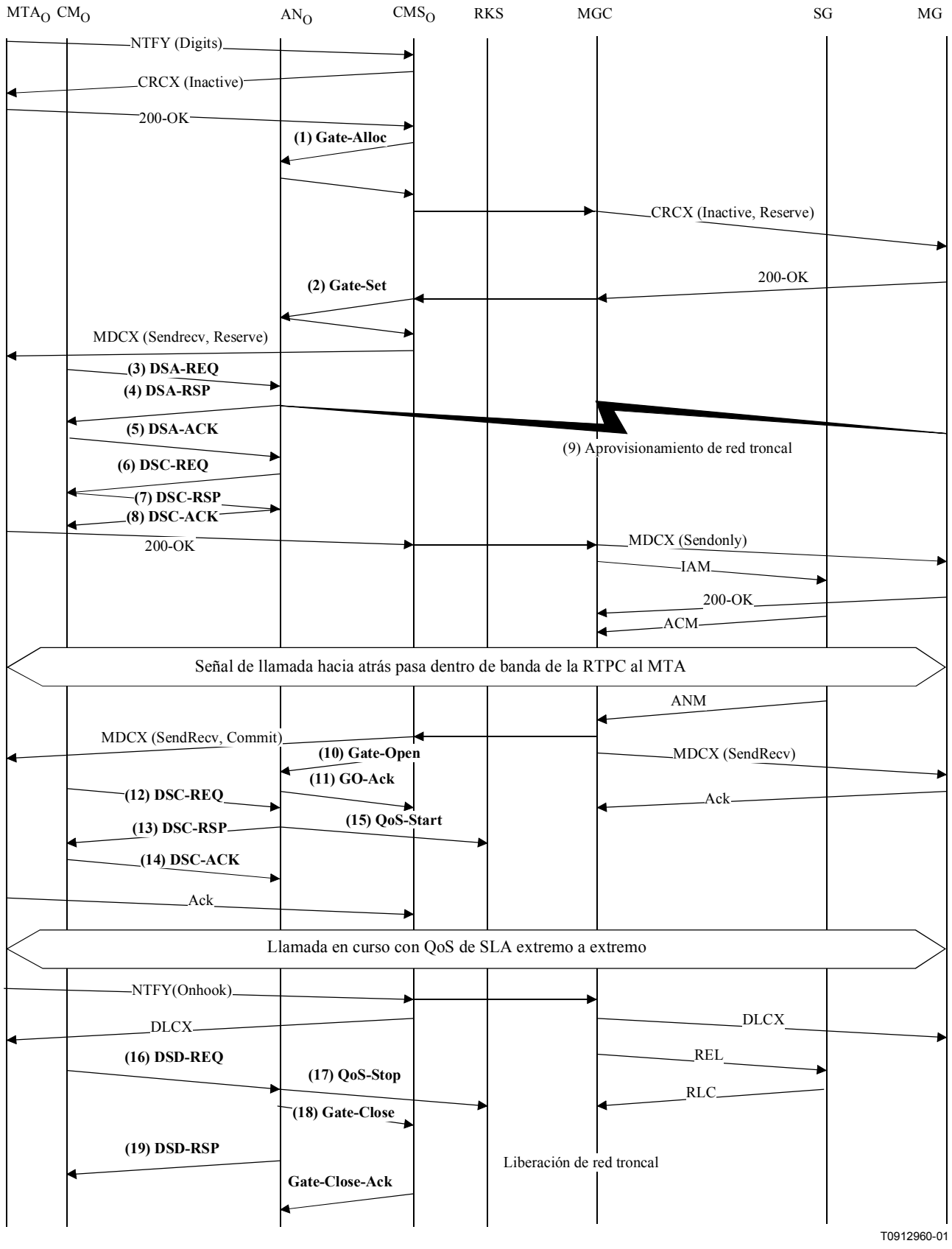


Figura VIII.3/J.163 – NCS integrada entre elementos de la red y elementos externos a la red

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

GATE-ALLOC (asignación de puerta)

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales utilizados por este cliente.
Cómputo de actividad		4	Número máximo de conexiones permitidas por cliente.

El ANo verifica la utilización actual de recursos por parte del MTAo, y responde informando del número de conexiones activas.

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

ID de transacción		3176	
Abonado		MTAo	Petición de los recursos totales utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada.
Cómputo de actividad		3	Número total de conexiones establecidas por este cliente.

2) Tras un intercambio de señalización adicional, el CMSo autoriza que el ANo 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 de los recursos totales utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada
Información de puerta distante	Dirección AN	CMSo	Información necesaria para realizar la coordinación de puerta. Nótese que el CMS ha establecido que él es la entidad para intercambiar mensajes de coordinación de puertas.
	Puerto AN	2052	
	ID de puerta distante	8095	
	Clave de seguridad	<key>	
	Bandera	Sin apertura de puerta	
Información de generación de eventos	Dirección RKS	RKS	Dirección del servidor de mantenimiento de registros (RKS).
	Puerto RKS	3288	Puerto de servidor de mantenimiento de registros.
	ID de correlación de facturación	<id>	Datos opacos que pasarán al RKS cuando los recursos estén comprometidos.

GATE-SET (establecimiento de puerta)

Especificación de puerta	Dirección	Ascend.	
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para paquetes ascendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puertas.
	b	120	Parámetros de anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Especificación de puerta	Dirección	Descend.	
	Bandera	Auto-compromiso	Bandera para activar recursos en la operación de reserva.
	Protocolo	UDP	La cuádrupla protocolo, dirección de destino, dirección de fuente, 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 para paquetes descendentes.
	T1	180000	Tiempo máximo entre reserva y compromiso.
	T2	2000	Tiempo máximo para completar la coordinación de puerta.
	b	120	Parámetros de la anchura de banda máxima que el MTAo está autorizado a solicitar para esta conversación.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

El ANo 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 de los recursos totales utilizados por este cliente.
ID de puerta		37125	Identificador de puerta asignada
Cómputo 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 del anexo E al anexo B/J.112 con el CM para enviar al AN el siguiente mensaje DSA-REQ. Este mensaje se utiliza para establecer los parámetros en los sentidos ascendente y descendente. El tamaño de la concesión no solicitada ascendente se calcula como 120 (del SDP) más 18 (tara Ethernet) menos 40 (por la supresión de cabecera) más 13 (tara J.112). La supresión de cabecera hace referencia a los 42 bytes de la cabecera Ethernet/IP/UDP. El contenido de la cabecera suprimida se incluye en el mensaje DSA-REQ (petición DSA).

DSA-REQ (petición DSA)

ID de transacción		1
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowReference	1
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37125
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowReference	2
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37125
UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowReference	1
	PacketClassifierReference	1
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSA-REQ (petición DSA)

DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowReference	2
	PacketClassifierReference	2
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
PayloadHeaderSuppression (Supresión de cabecera de carga útil)	ClassifierReference	1
	ServiceFlowReference	1
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42bytes>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Verificación (0)
AuthorizationBlock (Bloque de autorización)		37125
HMAC		

4) El AN verifica la autorización buscando una puerta cuyo ID de puerta concuerde con el valor incluido en AuthBlock, y verifica los recursos que debe asignar (por ejemplo, espacio del cuadro de supresión de cabecera, los ID de flujos de servicio, espacio del cuadro clasificador) e instala los clasificadores. Si la operación tiene éxito, devuelve el mensaje DSA-RSP (respuesta DSA) indicando dicha circunstancia.

DSA-RSP (respuesta DSA)

ID de transacción		1
Código de confirmación		Éxito (0)
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowReference	1
	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37125

DSA-RSP (respuesta DSA)

DownstreamServiceFlow (flujo de servicio descendente)	ServiceFlowReference	2
	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37125
UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowReference	1
	PacketClassifierReference	1
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowReference	2
	PacketClassifierReference	2
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Activo (1)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

5) Cuando el CM recibe el DSA-RSP, acusa recibo de la recepción con un mensaje DSA-ACK.

DSA-ACK (acuse de recibo DSA)

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

6) Cuando recibe el mensaje DSA-ACK del CM, el AN envía al CM un mensaje DSC-REQ para activar los recursos del flujo de servicio descendente. El AN lo hace porque la bandera de compromiso automático está habilitada en el mensaje GATE-SET enviado desde el CMS para la puerta descendente.

DSC-REQ (petición DSC)

ID de transacción		2
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido (2)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
Upstream Classifier (Clasificador ascendente)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Sustitución (1)
	ClassifierPriority	150
	ClassifierActivationState	Inactivo (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
Downstream Classifier (Clasificador descendente)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Sustitución (1)
	ClassifierPriority	150
	ClassifierActivationState	Active (1)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

7) Cuando se recibe el DSC-REQ del AN, el CM envía al AN un mensaje DSC-RSP.

DSC-RSP (respuesta DSC)

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

8) Cuando se recibe el DSC-RSP del CM, el AN envía al CM un mensaje DSC-ACK.

DSC-ACK (acuse de recibo DSC)

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

9) Simultáneamente con el mensaje N.º 4, el AN 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 AN la notificación precisa para indicar que la reserva ha tenido éxito.

10) El CMS envía al AN el mensaje de apertura de puerta para informarle que los recursos deberían comprometerse. Si el AN no recibiese del MTAo el mensaje DSC-REQ en un plazo breve de tiempo, debería revocar la autorización de puerta.

GATE-OPEN (apertura de puerta)

ID de transacción		72	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		37125	ID de puerta en el AN
HMAC			Suma de control de seguridad para este mensaje.

11) El AN responde al mensaje GATE-OPEN con:

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

ID de transacción		72	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje.

12) En respuesta a los mensajes de señalización que indican que la llamada se ha completado (es decir, el otro lado ha descolgado), el MTAo utiliza la interfaz del anexo E al anexo B/J.112 para activar los recursos admitidos. Esto se realiza enviando al AN una instrucción DSC-REQ.

DSC-REQ (petición DSC)

TransactionID		2
UpstreamServiceFlow (Flujo de servicio ascendente)	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow (Flujo de servicio descendente)	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitido + Activado (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000

DSC-REQ (petición DSC)

UpstreamPacketClassification (Clasificación de paquetes ascendentes)	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Sustitución (1)
	ClassifierPriority	150
	ClassifierActivationState	Activo (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification (Clasificación de paquetes descendentes)	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Sustitución (1)
	ClassifierPriority	150
	ClassifierActivationState	Activo (1)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

13) El AN envía un mensaje DSC-RSP que informa que la operación ha tenido éxito.

DSC-RSP (respuesta DSC)

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

14) El CM envía un mensaje DSC-ACK para indicar que se ha recibo el DSC-RSP y que está de acuerdo con él.

DSC-ACK (acuse de recibo DSC)

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

15) El ANo envía al servidor de mantenimiento de registros el registro de evento que indica que se ha recibido un compromiso en esta llamada. Este mensaje sólo es una muestra de lo que podría incluirse en el mensaje inicio de QoS.

QoS-START (inicio de QoS)

Cabecera	Indicación de tiempo	<time>	Hora a la que se registra el evento.
	ID de correlación de tiempo	<string>	ID de correlación incluido en el establecimiento de puerta.

QoS-START (inicio de QoS)

Descriptor de QoS	Tipo	UGS	Descripción de la QoS de la conexión.
	Intervalo de la concesión	10 ms	
	Fluctuación de fase de la concesión	2 ms	
	Concesión/Intervalo	1	
	Tamaño de la concesión	111	
Puerto MTA	Puerto	7120	

16) Cuando finaliza la llamada, el MTA utiliza la interfaz del anexo E al anexo B/J.112 para eliminar los flujos de servicio, enviando al AN un mensaje DSD-REQ.

DSD-REQ (petición DSD)

ID de transacción		3
ID de flujo de servicio		1001
HMAC		

DSD-REQ (petición DSD)

ID de transacción		4
ID de flujo de servicio		2001
HMAC		

17) El AN envía al servidor de mantenimiento de registros la notificación que indica que la llamada ha finalizado. Este mensaje es solo una muestra de lo que podría incluirse en el mensaje parada de QoS.

QoS-Stop (parada de QoS)

Indicación de tiempo		<time>	Hora a la que se ha registrado el evento.
Cabecera	Indicación de tiempo	<time>	Hora a la que se ha registrado el evento.
	ID de correlación de facturación	<string>	ID de correlación del mensaje establecimiento de puerta.
SF-ID	SF-ID	1001	Identificador de flujo de servicio.

18) Cuando el AN recibe el mensaje RSVP-PATH-TEAR, envía el mensaje de coordinación de puerta al CMS (identificado en el mensaje establecimiento de puerta).

GATE-CLOSE (cierre de puerta)

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
ID de puerta		8095	Identifica el ID de puerta en el CMS.
HMAC			Suma de control de seguridad para este mensaje.

El CMS responde con:

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

ID de transacción		73	Identificador para hacer corresponder este mensaje con su respuesta.
HMAC			Suma de control de seguridad para este mensaje

19) El AN suprime los ID de flujo de servicio y envía la respuesta al CM.

DSD-RSP (respuesta DSD)

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

DSD-RSP (respuesta DSD)

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

APÉNDICE IX

Escenarios de hurto de servicio

Se presentan a continuación algunos escenarios de hurto de servicio para destacar la necesidad de disponer de autorización dinámica, la necesidad de que el protocolo de reserva de recursos se componga de 2 fases, la necesidad de puertas y de la coordinación entre puertas. El diseño del sistema sitúa una gran parte de la inteligencia de control de la sesión en los clientes, donde es posible aplicar la tecnología para conseguir la escalabilidad necesaria 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 una amplia gama de posibilidades de fraude. En este apéndice se analizan algunas de dichas posibilidades y cómo la arquitectura de señalización de QoS ayuda a evitarlas.

El supuesto básico es que el MTA no es inmune a los intentos de intervención del cliente, y que el atractivo incentivo que supone poder disponer de un servicio gratuito hace que se produzcan intentos muy sofisticados para burlar los controles de red sobre el MTA. Las posibles formas de intervención sobre el cliente incluyen, aunque no se limita a, la apertura de la caja y la sustitución de memorias ROM, la sustitución de circuitos integrados, el sondeo y la ingeniería inversa del diseño del MTA e incluso, la sustitución total del MTA por una versión ilegal del mercado negro. Si bien existen soluciones técnicas para la seguridad física de la MTA (por ejemplo, instalar una trampa en la caja con gas letal), éstas no se consideran aceptables.

Debido a que el MTA sólo puede distinguirse en función de su comunicación sobre la red J.112, es posible, y bastante probable, que se escriba soporte lógico para PC que emule el comportamiento de un MTA. Dicho tipo de PC puede resultar indistinguible de un MTA real. En este caso, el comportamiento del soporte lógico se encuentra bajo el control total del cliente.

Además, se pretende que los nuevos servicios se implementen en el MTA y que el control del soporte lógico de tales nuevos servicios pueda ser proporcionado por varios vendedores. Dicho soporte lógico actualizado se descargará en el MTA, estando abierta la posibilidad de que los

clientes puedan descargar versiones especiales ilegales que proporcionen un acceso fraudulento. No son objeto de análisis los "caballos de Troya" que puede acarrear la utilización de soporte lógico descargable, ya que se trata de un problema idéntico al que actualmente existe cuando los clientes dan a conocer su número de tarjeta de crédito y/o su número PIN. Este documento se centra en el caso en que el cliente descarga soporte lógico intencionadamente en aras de conseguir un beneficio ilícito.

IX.1 Escenario 1: Clientes que establecen por sí mismos conexiones de elevada QoS

Un MTA que disponga de inteligencia suficiente puede recordar destinos anteriormente marcados y la dirección de los mismos, o utilizar otros mecanismos para determinar la dirección IP de un destino. Puede entonces ser él mismo quien intercambie señalización con el destino (con una cierta colaboración por parte del otro cliente) y negociar una conexión de calidad de servicio elevada mediante el mecanismo RSVP o la interfaz del anexo E al anexo B/J.112 para un cliente integrado. Dado que no se utiliza un agente de red para iniciar la sesión, no se genera un registro de facturación. Este escenario se previene requiriendo una autorización dinámica en el AN; sin dicha autorización, fracasará cualquier intento de disponer de una calidad de servicio elevada.

El escenario anterior requiere la cooperación de dos MTA que hayan sido modificados. Puede producirse un hurto de servicio similar modificando únicamente el originador. Si el MTA originario utiliza el agente de red para establecer la sesión, informando al destino en la forma normalizada de una sesión de entrada, pero negociando una calidad de servicio elevada, no se generaría un registro de facturación y el originador podría obtener así una sesión gratis. De nuevo, la solución consiste en exigir el uso de puertas en los AN.

IX.2 Escenario 2: Clientes que utilizan la QoS aprovisionada para aplicaciones distintas a la voz

Una QoS aprovisionada de forma estadística sólo identifica a un cliente como alguien que está autorizado para disponer de una elevada calidad de servicio. No existen restricciones en 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 a través de la red J.112, puede utilizar esta capacidad para navegación en la web o para otras aplicaciones basadas en PC. Este escenario se previene exigiendo la autorización dinámica en el AN; sin dicha autorización fracasará cualquier intento de disponer de una calidad de servicio elevada.

IX.3 Escenario 3: No cooperación del MTA para la facturación

Puede imaginarse fácilmente qué ocurriría si existiera un mensaje del MTA en el establecimiento de la sesión que dijera "De acuerdo, el llamado ha respondido, comience a facturarme a partir de ahora", o un mensaje que cuando se produjera el colgado dijera "la sesión ha terminado, detenga la facturación en este momento". No obstante, existen formas más sutiles que puede utilizar un usuario y que tendrían el mismo efecto que la manipulación de dichos mensajes en caso de que existieran.

En el aprovisionamiento de un servicio de comunicaciones vocales con una calidad de servicio comercial utilizando IPCablecom es esencial asegurar que exista capacidad de red antes de iniciar la señalización con el CPE receptor. Esta función se realiza mediante el mensaje RESERVE (reserva). Si el mensaje RESERVE hiciera efectivamente la asignación 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. El mensaje COMMIT se convertiría, de hecho, en el mensaje de inicio de facturación antes

mencionado. Por lo tanto, es esencial que RESERVE no realice realmente la asignación de anchura de banda, sino que verifique 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 4: El MTA modifica la dirección de destino de los paquetes vocales

Otro caso significativo se produce cuando dos MTA, distantes entre sí, establecen 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 facturación continua facturando a cada uno por sus sesiones locales, mientras que en realidad los clientes están en una sesión de larga distancia. Ello exige disponer en los AN de mecanismos que proporcionen acceso a una QoS superior sólo en base a filtros de paquetes previamente autorizados. Por lo tanto, además de la gestión de los recursos en dos fases, de este escenario se desprende la necesidad de disponer de filtros de paquetes en las puertas.

IX.5 Escenario 5: Utilización de medias conexiones

Este es un ejemplo de hurto de servicio que podría ocurrir en ausencia de la coordinación de puerta. 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 que fracasa en el envío del mensaje de señalización adecuado, de forma que el origen no llega a enviar nunca un mensaje COMMIT. En este caso, sólo se abre una puerta y tanto los usuarios como la red quedan con media conexión. Debido a que el originador no envió un mensaje COMMIT, la red no puede legítimamente facturar al usuario por la media conexión. Sin embargo, es posible que dos clientes se pongan de acuerdo de modo que cada uno establezca una media conexión dando lugar a una conexión completa entre las dos partes. Ello genera una sesión gratis para ambos. Los fraudes de este tipo sólo pueden evitarse mediante la sincronización del funcionamiento de ambas puertas.

IX.6 Escenario 6: Terminación prematura manteniendo media conexión

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

IX.7 Escenario 7: Mensajes de coordinación de puertas falsificados

Cada MTA conoce la identidad de su AN, y conoce la quíntupla que éste utiliza para identificar el ID de puerta. Los MTA pueden realizar varios tipos de negociación extremo a extremo antes de solicitar recursos; en particular, pueden intercambiar fácilmente la información acerca de sus ID de puerta. El MTA puede entonces imitar fraudulentamente el mensaje GATE-OPEN enviado al extremo que no paga y obtener una conexión unidireccional no facturada. Realizar esto mismo dos veces permite disponer de una conexión completa no facturada. Una solución a este problema consiste en que el controlador de puerta entregue al AN una clave para ser empleada en los mensajes AN-AN o para cada sesión (o para cada puerta).

IX.8 Escenario 8: Fraude contra llamantes indeseados

Debido al detalle de la secuencia de establecimiento de la comunicación, es posible que la autorización de la anchura de banda en el destino sea más generosa que en la fuente. En esta circunstancia, es posible que una parte llamada reserve y asigne una anchura de banda muy superior

a la cantidad finalmente negociada, dando lugar a que la parte llamante reciba una factura superior a lo esperado. Si fuera posible, se podría utilizar contra llamadas realizadas por las empresas de telemarketing, por ejemplo, para evitar llamadas indeseadas durante la hora de la cena.

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

APÉNDICE X

Servicio de política común abierta (COPS)

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

En este apéndice se presenta una breve descripción de los procedimientos y principios del servicio de política común abierta (COPS) y sobre cómo COPS se relaciona con otros protocolos tales como LDAP. Puede encontrarse una definición de COPS en el documento Internet Draft-IETF-RAP-COPS-07.

El protocolo del servicio de política común 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 bien conocido, el 3288. Las entidades COPS residen en un dispositivo situado en el límite de la red y en un servidor de política. En el marco de RAP se definen tres entidades funcionales:

- Punto de decisión de política (PDP) – Es la entidad servidora COPS que toma la decisión final sobre la admisión o rechazo de la sesión, en base a la información sobre la política a la que tiene acceso. 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 u obtener información sobre la política que puede ser de utilidad para la toma de decisiones de control de admisión; el PEP puede recibir peticiones de servicio y realizar una pregunta al PDP que resultará en una respuesta que indique proseguir o no proseguir; 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 incluida en un elemento de almacenamiento intermedio relativa a decisiones previamente tomadas. Una decisión PDP siempre tiene prioridad respecto a una decisión LDP.

En la figura X.1 se muestra una secuencia COPS, tal como se utiliza en un entorno RSVP/IntServ.

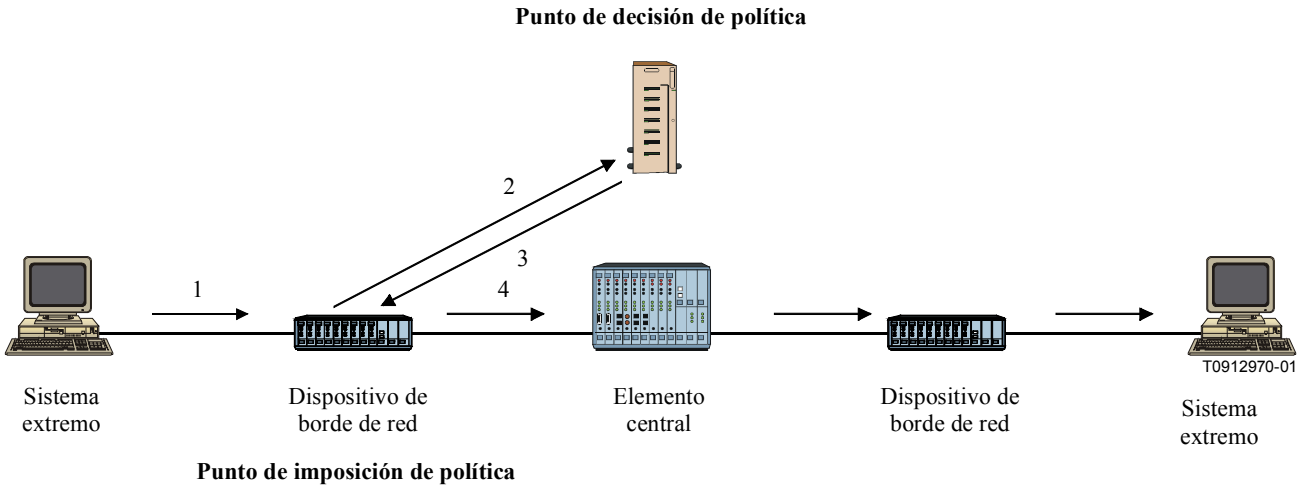


Figura X.1/J.163 – Protocolo COPS

En la secuencia COPS, el cliente PEP es inicialmente responsable del establecimiento de una sesión con el PDP utilizando información que está configurada en el PEP o que se determinada por algún otro medio. Una vez que la sesión esté establecida, el dispositivo del borde de la red recibe un mensaje RSVP (1), genera una petición al PDP (2) que describe el contexto de la petición y transporta la información sobre la 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 vivo que verifica que la sesión está activa en caso de que no se haya recibido recientemente ningún mensaje. Cada petición RSVP, o de cualquier otro tipo, se identifica mediante un asa que puede utilizarse para asociar la respuesta, respuestas ulteriores no solicitadas y la cancelación.

Los mensajes del protocolo pueden utilizarse también para otras tareas. Constan de un código opcional que identifica si el mensaje es una petición, una respuesta o de otro tipo, 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 define lo que es el objeto, por ejemplo, un objeto temporizador o un objeto de decisión, más 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

Aunque tanto COPS como LDAP se han asociado a la gestión basada en la política, ambos proporcionan funciones muy distintas.

COPS está diseñado para que el cliente solicite al punto de decisión de política (PDP) que tome una decisión y para interactuar con el PDP a fin de participar activamente en la gestión de la política y en asuntos relacionados con la misma. El PEP que realiza la petición puede no tener conocimiento de las políticas, y se apoya en el PDP para tomar decisiones en función del conocimiento que éste tiene de las políticas. El protocolo permite que el PEP pase al PDP información sobre la petición, y que éste devuelva una decisión para aceptar o rechazar la petición.

El LDAP está diseñado para que el cliente solicite 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 un 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 en base a la información sobre política que se ha recuperado y utilizaría el COPS para devolver esa decisión al PEP. Véase la figura X.2.

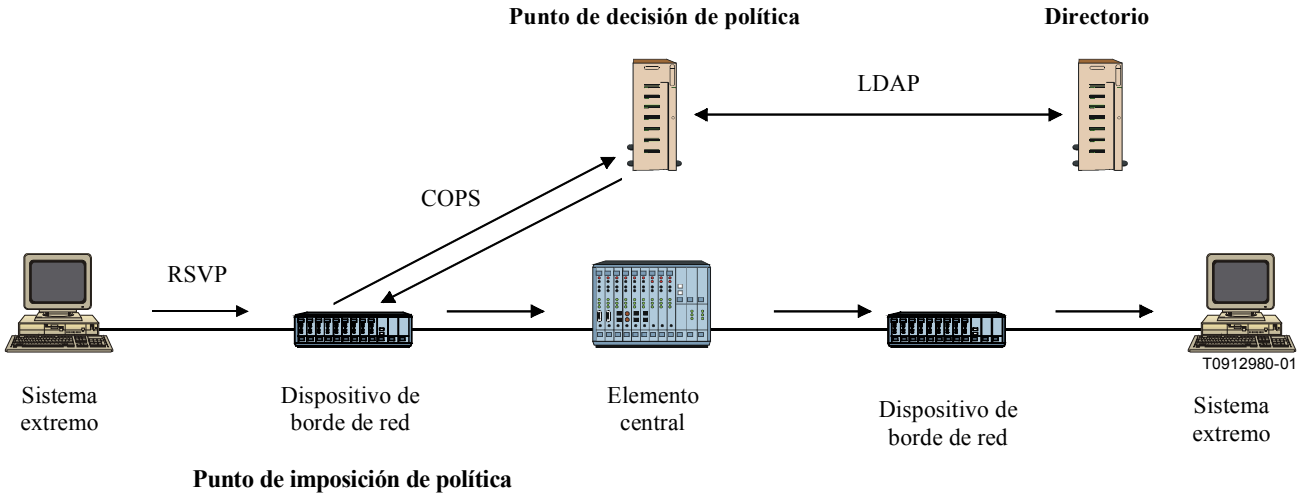


Figura X.2/J.163 – Modelo con COPS y LDAP

APÉNDICE XI

Protocolo de reserva de recursos (RSVP)

XI.1 Procedimientos y principios del RSVP

En este apéndice se proporciona una breve descripción de los procedimientos y principios del protocolo de reserva de recursos (RSVP). El protocolo RSVP se encuentra actualmente definido en la RFC 2205 del IETF.

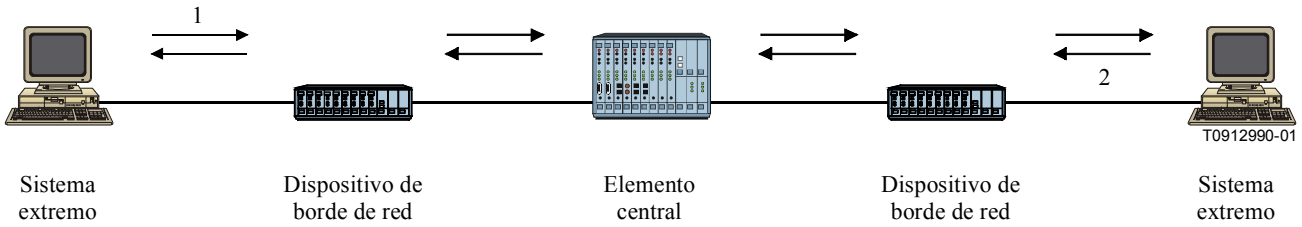


Figura XI.1/J.163 – RSVP

El RSVP se desarrolló en el IETF para la reserva de recursos destinada a soportar flujos de información a través de Internet. Algunas de las principales características del RSVP son las siguientes:

- 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 blando – la reserva debe refrescarse periódicamente o se cancela automáticamente;
- está gobernado por las peticiones – un mensaje PATH inicial establece un estado del encaminador. El mensaje RESV que envía el receptor sirve para reservar 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 la dirección de destino, por lo que replica la ruta que siguen los paquetes de datos. Conforme progresa el paquete, 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. No obstante, garantiza que se asignan recursos 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" y de una "especificación de filtro"; dicha pareja de elementos se denomina "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 recibe la QoS que define 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 flujo de dicha sesión, se tratan como tráfico que se encamina sobre la base del criterio del 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 "Rspec" (R de "reserva") que define la QoS deseada, y
2) una "Tspec" (T de "tráfico") 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 la RFC 2210 del IETF 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 nodo de acceso (AN) que se utiliza para la autorización de puerta y que, fundamentalmente, soporta un protocolo basado en transacciones independientes entre sí. Para este intercambio de mensajes puede utilizarse TCP como mecanismo de transporte. Sin embargo, se han identificado algunos aspectos preocupantes de las implicaciones de la utilización de TCP en relación con la calidad de funcionamiento. En este apéndice se examinan algunos de dichos aspectos preocupantes, y se proponen soluciones que permiten un transporte aceptable mediante optimizaciones de la implementación y un ajuste dela implementación del TCP.

El diseño de la red debe soportar el grado deseado de fiabilidad y el funcionamiento en tiempo real.

XII.1 Requisitos

Se recogen a continuación los requisitos que se imponen al protocolo de transporte para la interacción entre el GC y el AN.

1) Es necesario que la entrega de los mensajes intercambiados entre el GC y el AN sea fiable.
2) El intercambio de mensajes debe tener, normalmente (es decir en una situación sin pérdida de paquetes) un retardo bajo (del orden de milisegundos). También es necesario que el retardo sea razonablemente bajo incluso en una situación de pérdida de paquetes (del orden de decenas de milisegundos).
3) Existirán en curso simultáneamente numerosas peticiones. Ello se debe a que es probable que se produzcan a la vez numerosos establecimientos de llamada.
4) Si existe la posibilidad de que se produzca el bloqueo de cabeza de línea (HOL, *head-of-the-line*), éste debe evitarse.
5) Es probable que se produzca una asociación perdurable (de al menos varios minutos) entre el GC y el AN. Sin embargo, cuando se produce el fallo de un GC, el proceso de establecimiento de una nueva conexión con el AN no debe requerir un tiempo excesivo. Esto es especialmente cierto si durante el establecimiento de una comunicaicón se produce una nueva conexión.

XII.2 Cambios recomendados

De forma resumida, los cambios que se recomienda realizar para una implementación sencilla del protocolo TCP son las siguientes:

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-AN para evitar potenciales problemas de HOL (por ejemplo, utilizarlas en forma cíclica rotativa).
4) Utilizar una granularidad de la temporización inferior a 500 ms.
5) Deshabilitar el algoritmo de Nagle en el extremo transmisor al objeto de reducir el retardo.
6) Disponer de una interfaz sin bloqueo entre la aplicación y la pila TCP.

En el resto de este apéndice se presenta información detallada sobre cómo pueden implementarse estas modificaciones.

XII.3 Impacto del establecimiento de la conexión TCP en el retardo de postmarcación

El establecimiento de la conexión TCP utiliza tres señales de toma de contacto, tal como se indica a continuación (véase la figura XII.1).

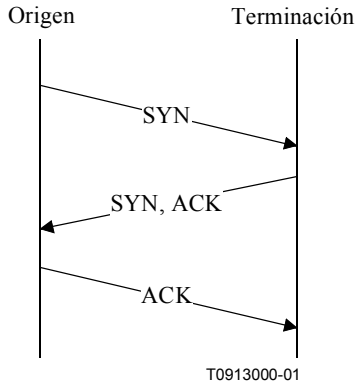


Figura XII.1/J.163 – Establecimiento de una conexión TCP

El protocolo TCP retransmite los segmentos que se suponen perdidos en base a una estimación del tiempo de ida y vuelta, A, y una desviación típica respecto al valor de A, es decir, D. El valor de la temporización de retransmisión (RTO, *retransmission timeout value*) se calcula generalmente utilizando la fórmula siguiente:

$$RTO = A + 4D$$

pero el 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, al valor vigente de RTO se le aplica una variación exponencial con un multiplicador de 2. 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 se calcula de la forma siguiente:

$$RTO = 0 + 4 \times 3 = 12$$

aplicando una variación de una potencia de 2, se obtiene un nuevo valor de temporización de la retransmisión de 24 segundos. 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 con la que falle el establecimiento de la conexión entre el GN → AN durante el periodo retardo de postmarcación. En los escenarios actualmente previsibles, esta circunstancia es mucho más una excepción que la regla. El retardo de establecimiento de la conexión, que incluye el retardo de postmarcación, constituye un motivo lo suficientemente importante como para evitar el establecimiento de la conexión durante el periodo de retardo de postmarcación. Puede utilizarse la marcación de los paquetes que realiza Diffserv al objeto de reducir el retardo y la probabilidad de pérdidas, de igual modo que actualmente se hace para el encaminamiento de tráfico con el fin de reducir retardos de establecimiento de conexión debido a la pérdida de paquetes.

XII.4 Necesidad de un retardo reducido de los paquetes entre el GC y el AN, incluso en situaciones de pérdidas

El requisito (2), que se refiere a la recuperación de la pérdida de paquetes debe utilizar determinadas soluciones para que TCP se recupere rápidamente de una situación de pérdidas. Cuando sólo se han transmitido unos pocos paquetes y el receptor no puede generar un número suficiente de acuses de recibo duplicados, la recuperación de la pérdida de paquetes se produce gracias a la temporización de la retransmisión. El algoritmo de retransmisión TCP se basa en una media suavizada del tiempo de ida y vuelta (RTT, *round-trip time*), A, y una media suavizada de la desviación típica de RTT. Tal como se ha descrito anteriormente, el valor del temporizador de retransmisión se fija en:

$$RTO = A + 4D$$

si el temporizador expira, el segmento en cuestión se retransmite y el RTO varía exponencialmente utilizando un multiplicador de 2[3] hasta que el RTO alcanza un límite superior de 64 segundos. Una vez que un segmento se ha pasado al TCP, se transmite con éxito al destino o bien, se cierra la conexión después de transcurrido un determinado periodo de tiempo (generalmente un periodo grande, por ejemplo, de 2 a 9 minutos).

Si bien la estrategia de retransmisión anterior se puede ser deseable, se considera que presenta dos problemas (conexos) para la interfaz considerada:

1) Si no se entrega con éxito del segmento en un periodo de tiempo pequeño, la llamada que se encuentra en fase de establecimiento es muy probable que sea abandonada y que se aborte la transacción.

2) El límite máximo de 64 segundos del temporizador de retransmisión no es adecuado para las comunicaciones en tiempo real, para las cuales debiera ser mucho menor.

Un aspecto distinto pero relacionado es la granularidad del RTO. Si bien la especificación de TCP no especifica la granularidad del RTO, es habitual que ésta sea de 500 ms en sistemas operativos 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 recuperar rápidamente los paquetes perdidos en una secuencia de paquetes (sin que se dependa de múltiples acuses de recibo duplicados para que se produzca la retransmisión rápida o tener que esperar a que venza el 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 que la implementación TCP utilice una granularidad de temporizador menor (si es posible inferior a 500 milisegundos).

XII.5 Bloqueo de cabeza de línea

El bloqueo de cabeza de línea hace referencia al hecho de que el TCP proporciona un servicio de distribución de datos en el que un segmento perdido puede bloquear la entrega a la aplicación de segmentos posteriores. Por lo tanto, 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 con éxito.

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 AN, utilizando el conjunto de conexiones TCP para realizar las transacciones, por ejemplo, utilizándolas de forma cíclica repetitiva. Por tanto, si en una conexión se pierde un segmento, ello no afectará a otros segmentos pues las transacciones se envían por conexiones diferentes.

---

[3] TCP utiliza mensajes ACK duplicados para que se produzca la retransmisión de segmentos que puedan estar perdidos; no obstante, en esta parte del análisis se ignorará este hecho.

El inconveniente de este enfoque es que no es probable que los segmentos perdidos sean retransmitidos hasta que venza su temporizador de retransmisión (en contraposición a la recepción de un ACK duplicado), ya que hasta entonces no habría ningún segmento adicional que transmitir.

XII.6 Arranque lento de TCP

La capacidad de TCP para iniciar la transmisión de un tren de paquetes de datos está a veces limitada por el mecanismo de arranque lento de TCP, especialmente cuando el tren consta de un número pequeño (mayor que 1) de paquetes de datos. Es conveniente elegir una ventana de tamaño superior a uno 1 (tanto al principio de la vida de 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 MSS. No obstante, es conveniente asegurarse que esta ventana inicial no es superior a 4 MSS por el potencial riesgo de congestión que ello conlleva.

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).

Debido a la naturaleza en tiempo real de este tráfico, es recomendable deshabilitar el algoritmo de Nagle para la comunicación entre GC y AN. En la mayoría de las plataformas basadas en Unix, el algoritmo Nagle puede deshabilitarse 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 restantes lenguajes y plataformas tienen una facilidad similar que permite deshabilitar el algoritmo de Nagle, y que normalmente se conoce como la opción TCP_NODELAY.

XII.8 Interfaz sin bloqueo

Por defecto, la mayoría de los sistemas operativos proporcionan una interfaz con bloqueo para los conectores TCP/IP. Aunque ello puede permitir disponer de un esquema de recuperación de errores mejorado, influye sobre la calidad de funcionamiento del canal de comunicación.

En esencia, una llamada del sistema tal como enviar() que disponga de interfaz con bloqueo 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.

Puede ser deseable emplear una interfaz sin bloqueo para mejorar la calidad de funcionamiento y soportar eventos asíncronos utilizando la llamada a la función seleccionar() de una arquitectura basada en UNIX. Puede establecerse una interfaz de conector sin bloqueo utilizando para la llamada siguiente 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 mayor parte de los restantes lenguajes y plataformas tienen una facilidad similar.

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	**Transmisiones de señales radiofónicas, de televisión 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 y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2001