UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.174

(02/2002)

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

IPCablecom

Calidad de servicio interdominio IPCablecom

Recomendación UIT-T J.174

RECOMENDACIONES UIT-T DE LA SERIE J

REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, 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**
Varios	J.180–J.199
Aplicación para televisión digital interactiva	J.200–J.209

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

Recomendación UIT-T J.174

Calidad de servicio interdominio IPCablecom

Resumen

En esta Recomendación se describe un conjunto de mecanismos de calidad de servicio (QoS) de extremo a extremo aplicables a entornos interdominio e intradominio IPCablecom.

Orígenes

La Recomendación UIT-T J.174, 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 13 de febrero de 2002.

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.

© UIT 2002

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

ÍNDICE

		Página
1	Alcance	1
2	Referencias	1
2.1	Referencias normativas	1
2.2	Referencias informativas	1
3	Términos y definiciones	2
4	Abreviaturas, acrónimos y convenios	2
4.1	Abreviaturas y acrónimos	2
4.2	Convenios	3
5	Introducción	4
5.1	Requisitos y soluciones	4
5.2	Solución gradual de los requisitos	4
5.3	Objetivos generales	5
6	Modelo de red	5
7	Utilización de servicios diferenciados (Diffserv) en redes dorsales	7
7.1	Tráfico de medios	7
7.2	Tráfico de señalización	7
7.3	Selección del PHB y fijación del DSCP	8
7.4	Soporte de PHB por el AN	9
7.5	Asignación de recursos	9
7.6	Control de admisión	9
8	Control de admisión para un solo dominio	10
8.1	Plano de control RSVP por flujo	10
8.1.1	Comportamiento del AN	11
8.1.2	Ubicación del contorno Diffserv	14
8.1.3	Comportamiento del encaminador de contorno	14
8.1.4	Otros dispositivos terminadores (pasarelas de medios, anonimizadores, servidores de anuncios, puentes de conferencia)	15
8.1.5	Comportamiento del encaminador medular	15
8.1.6	Latencia de señalización	15
8.1.7	Preapropiación	15
8.2	RSVP compuesto	16
8.2.1	Provisión de reservas compuestas	16
8.2.2	Reserva compuesta dinámica	17
8.2.3	Agregación jerárquica	17
8.2.4	Ubicación de los puntos de agregación y del contorno DiffServ	17

Página

8.3 Intermediario de ancho de banda 18

9 Control de admisión para múltiples dominios 19

10 Utilización de MPLS 20

11 Puesta en cola y filtrado 21

11.1 Puesta en cola 21

11.2 Filtrado 21

Apéndice I – Ejemplos de flujo de llamada 22

Apéndice II – Bibliografía 23

Recomendación UIT-T J.174

Calidad de servicio interdominio IPCablecom

1 Alcance

En esta Recomendación se describe un conjunto de mecanismos de calidad de servicio (QoS, *quality of service*) para el proyecto IPCablecom. El objetivo de esta Recomendación es definir un modelo de arquitectura aplicable a la calidad de servicio de extremo a extremo para entornos interdominio e intradominio IPCablecom. Se describen mecanismos para integrar los protocolos de señalización de la calidad de servicio dinámica (DQoS, *dynamic quality of service*) IPCablecom con modelos QoS de redes medulares IP actuales. En esta Recomendación no se tratan las redes sin control de QoS. Se supone que el lector está familiarizado con la arquitectura IPCablecom, concretamente con la DQoS y la señalización de llamada.

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.

2.1 Referencias normativas

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

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

[3] IETF RFC 2475 (1998), *An Architecture for Differentiated Service*.

[4] IETF RFC 2998 (2000), *A Framework for Integrated Services Operation over Diffserv Networks*.

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

[6] IETF RFC 3181 (2001), *Signalled Preemption Priority Policy Element*.

[7] Recomendación UIT-T J.163 (2001), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable*.

2.2 Referencias informativas

[8] IETF RFC 2638 (1999), *A Two-bit Differentiated Services Architecture for the Internet*.

[9] IETF RFC 2597 (1999), *Assured Forwarding PHB Group*.

[10] IETF RFC 2598 (1999), *An Expedited Forwarding PHB*.

[11] IETF RFC 2702 (1999), *Requirements for Traffic Engineering Over MPLS*.

[12] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

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

[14] Recomendación UIT-T J.171 (2002), *Protocolo de control de pasarela de circuitos troncales IPCablecom*.

[15] MAKAM [S.] et. al.: Framework for MPLS-based Recovery, *draft-ietf-mpls-recovery-frmwrk-03.txt*, julio de 2001.

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 nodo de acceso: En la acepción en que este término se utiliza en esta Recomendación, dispositivo de terminación de la capa 2 en el que termina el extremo de red de una conexión J.112. Es específico de la tecnología. En el anexo A de J.112 se denomina adaptador de red interactivo (INA, *interactive network adapter*) mientras que en los anexos B y C se denomina sistema de terminación de módem de cable (CMTS, *cable-modem termination system*).

3.2 punto extremo: Un terminal, una pasarela o una MCU.

3.3 flujo [flujo IP]: Secuencia unidireccional de paquetes identificados mediante información de encabezamiento correspondiente a las capas 3 y 4 ISO. Esta información incluye direcciones IP de fuente/destino, números de puerto fuente/destino e ID de protocolo. Un solo flujo IP puede transportar múltiples trenes multimedios.

3.4 flujo [flujo J.112]: Flujo unidireccional o bidireccional de paquetes de datos que está sujeto a señalización de capa MAC y a la asignación de QoS conforme con la Rec. UIT-T J.112. Un solo flujo J.112 puede transportar múltiples trenes multimedios.

3.5 pasarela (gateway): Dispositivos que sirven de puente entre el mundo de las comunicaciones de voz por IP IPCablecom y la RTPC. Ejemplos son la pasarela de medios, que proporciona las interfaces de circuito portador a la RTPC y transcodifica el tren de medios, y la pasarela de señalización, que envía y recibe señalización de las redes con conmutación de circuitos hasta el contorno de la red IPCablecom.

3.6 latencia: Tiempo, expresado en cantidad de símbolo, que requiere un elemento de señal para pasar a través de un dispositivo.

3.7 apoderado: Un dispositivo que presta indirectamente algún servicio o actúa como representante en el suministro de información descargando al anfitrión de la obligación de dar soporte a los servicios él mismo.

3.8 circuito troncal: Conexión analógica o digital desde un conmutador de circuitos, que transporta información de medios de usuario y puede transportar señalización de voz (MF, R2, etc.).

4 Abreviaturas, acrónimos y convenios

4.1 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas.

AF Reenvío asegurado (*assured forwarding*)

AN Nodo de acceso (*access node*)

ATM Modo de transferencia asíncrono (*asynchronous transfer mode*)

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

COPS Protocolo de servicio de política común abierta (*common open policy service protocol*)

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

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

DSCP Punto de código de servicio diferenciado (*differentiated services codepoint*)

EF Reenvío expeditado (*expedited forwarding*)

ER	Encaminador de contorno (*edge router*)
IETF	Grupo de tareas especiales de ingeniería en Internet (*Internet Engineering Task Force*)
IntServ	Servicios integrados (*integrated services*)
IP	Protocolo Internet (*Internet protocol*)
MPLS	Conmutación por etiquetas multiprotocolo (*multiprotocol label switching*)
MTA	Adaptador de terminal de medios (*media terminal adapter*)
PHB	Comportamiento por salto (*per-hop behaviour*)
PHS	Supresión de cabecera de la carga útil (*payload header suppression*)
QoS	Calidad de servicio (*quality of service*)
RSVP	Protocolo de reserva de recursos (*resource reservation protocol*)
RTPC	Red telefónica pública conmutada
UDP	Protocolo datagrama de usuario (*user datagram protocol*)
VoIP	Voz sobre el protocolo Internet (*voice over Internet protocol*)

4.2 Convenios

Al implementar esta Recomendación, se tendrá en cuenta que la obligatoriedad de la especificación se expresa mediante el verbo modal "DEBER" (modal inglés *MUST*) o un verbo en tiempo futuro con valor imperativo, por ejemplo "EXPIRARÁ" (modal inglés *SHALL*) o el adjetivo "OBLIGATORIO" (*REQUIRED*).

A continuación, se indican otras expresiones que se aplican a determinados requisitos con significado de obligación o posibilidad.

"DEBER" (*MUST*)	Este verbo (u otros con significado de obligación, como "tener que", "haber que/de" o un verbo en tiempo futuro con valor imperativo o el adjetivo OBLIGATORIO (*REQUIRED, MANDATORY*) indican que se tiene la obligación de hacer lo que expresa la especificación.
"NO DEBER" (*MUST NOT*)	La negación indica que se prohíbe hacer lo que expresa la especificación.
"DEBERÍA" (*SHOULD*)	El modo condicional de estos verbos, u otros verbos con significado de conveniencia (aconsejar, recomendar, ser conveniente) o el adjetivo RECOMENDADO (*RECOMMENDED*) indica que puede haber motivos fundados para que en determinadas circunstancias no se haga cierta cosa, pero que antes de hacer algo diferente, es preciso entender todas las consecuencias y sopesar el caso.
"NO DEBERÍA" (*SHOULD NOT*)	La negación indica la posibilidad de que haya motivos fundados para que en determinadas circunstancias la acción sea aceptable e incluso útil, pero que antes de realizarla es preciso entender todas las consecuencias y sopesar el caso.

"PODER" (*MAY*)	Éste u otros verbos que indican posibilidad o probabilidad (deber de) o el adjetivo FACULTATIVO u OPCIONAL (*OPTIONAL*) se refieren a la libertad de elegir. Un proveedor puede incluir un elemento porque el mercado lo exige o porque mejora el producto, mientras que otro puede optar por no hacerlo.

5 Introducción

5.1 Requisitos y soluciones

Hay tres requisitos básicos para proporcionar QoS de extremo a extremo en sesiones IPCablecom:

1) Proporcionar tiempos aceptables de establecimiento de comunicación, comparables a los de la RTPC.
2) Proporcionar una calidad de voz aceptable mediante mecanismos que garanticen valores suficientemente bajos de retardo, fluctuación de fase y pérdida de paquetes.
3) Garantizar que se mantiene una alta calidad durante toda la sesión (por ejemplo bloquear los intentos de nuevas llamadas que pudieran comprometer la calidad de las llamadas existentes).

En una red de paquetes el segundo requisito se traduce en: proporcionar mecanismos que reconozcan el tráfico IPCablecom y gestionen la calendarización del tráfico y la asignación de memoria intermedia en cada conmutador y encaminador de manera que el retardo y la pérdida de paquetes estén acotados.

El tercer requisito pone de manifiesto la necesidad de un control de admisión. En función del mecanismo de QoS elegido, el problema consiste en definir un método satisfactorio de bloquear o admitir llamadas o sesiones según la disponibilidad de recursos en la red dorsal.

A continuación se enumeran criterios generales para evaluar las posibles soluciones aplicables a la QoS de extremo a extremo en IPCablecom.

- La solución debería satisfacer los tres requisitos anteriores.
- La solución ha de ser gestionable e implementable.
- La solución ha de ser escalable. Los mecanismos QoS para los servicios de comunicación de voz deben ser capaces de crecer para dar cabida a muchas sesiones IPCablecom concurrentes sin introducir costos de implementación o complejidad indebidos.
- La solución debería ser capaz de recuperarse paulatinamente cuando se produce un fallo en la red. Por ejemplo, probablemente es inevitable que algunas llamadas se corten cuando se produce un fallo en la red, pero esto no debería repercutir sobre las demás llamadas en la red.

Estos requisitos, en particular el requisito de escalabilidad, convergen a una arquitectura de red dorsal basada en el método [2], [3] de servicios diferenciados (Diffserv, *differentiated services*) del IETF. Diffserv se diseñó específicamente como un método escalable para suministrar QoS en redes dorsales grandes. En las cláusulas siguientes se describe su aplicación en el entorno IPCablecom.

5.2 Solución gradual de los requisitos

En esta Recomendación se presentan varios métodos para proporcionar QoS a través de una red dorsal IPCablecom gestionada. Varias de estas soluciones son complementarias, y con vista de las necesidades de gestión de recursos del operador de red, estos distintos mecanismos se pueden combinar para obtener el control y gestión deseados de los recursos y sesiones IPCablecom.

En el siguiente cuadro se muestran las combinaciones factibles de los métodos descritos en las cláusulas 7 a 10.

Método	Cláusulas necesarias
Diffserv	Cláusula 7 (Diffserv)
RSVP por flujo	Cláusulas 7, 8.1
RSVP compuesto	Cláusulas 7, 8.1, 8.2
Intermediario de ancho de banda	Cláusulas 7, 8.3

El soporte de Diffserv es OBLIGATORIO para todas las redes dorsales IPCablecom. Los dispositivos IPCablecom DEBEN como mínimo soportar los requisitos Diffserv definidos en la cláusula 7.

Los requisitos RSVP por flujo, según se definen en las cláusulas 8 y 8.1, son FACULTATIVOS. Sin embargo, si se da soporte al RSVP por flujo estos requisitos son OBLIGATORIOS.

En la cláusula 8.2 se describe un método de agregación RSVP. Si se soporta la agregación de RSVP, toda la cláusula 8.2 es OBLIGATORIA. Además, también serán OBLIGATORIOS todos los requisitos de RSVP por flujo definidos en las cláusulas 8 y 8.1.

Las optimizaciones de MPLS, según se describen en la cláusula 9, son FACULTATIVAS y se pueden utilizar con cualquiera de los métodos descritos.

5.3 Objetivos generales

Los objetivos generales de esta Recomendación son los siguientes:

- Definir mecanismos de señalización para el establecimiento de recursos QoS entre nodos de acceso que estén separados mediante una red dorsal IP gestionada.
- Definir mecanismos de señalización para el establecimiento de recursos QoS entre nodos de acceso y otros elementos IPCablecom en el trayecto de medios, como por ejemplo encaminadores de contorno, encaminadores de frontera, pasarelas de medios y servidores de medios.
- Dar soporte a sesiones QoS dinámicas de extremo a extremo a través de redes dorsales IP gestionadas.
- Definir las interfaces para el control y el suministro de QoS entre dominios IPCablecom.
- Dar soporte a modelos de señalización de llamada basada en la red (NCS, *network-based call signalling*) y señalización de llamada distribuida (DCS).
- Dar soporte a las señalizaciones QoS de capa 2 (J.112) y de capa 3 (RSVP) en la red de acceso.
- Dar soporte a múltiples redes dorsales con implementaciones QoS normalizadas para gestionar la calendarización de tráfico y la asignación de memoria intermedia en conmutadores y encaminadores (por ejemplo, MPLS, DiffServ, ATM, RSVP, etc.).

6 Modelo de red

En la figura 1 se muestra la arquitectura de red IPCablecom. Una red dorsal IPCablecom consiste en una topología general de red IP gestionada que puede estar formada por múltiples dominios administrativos.

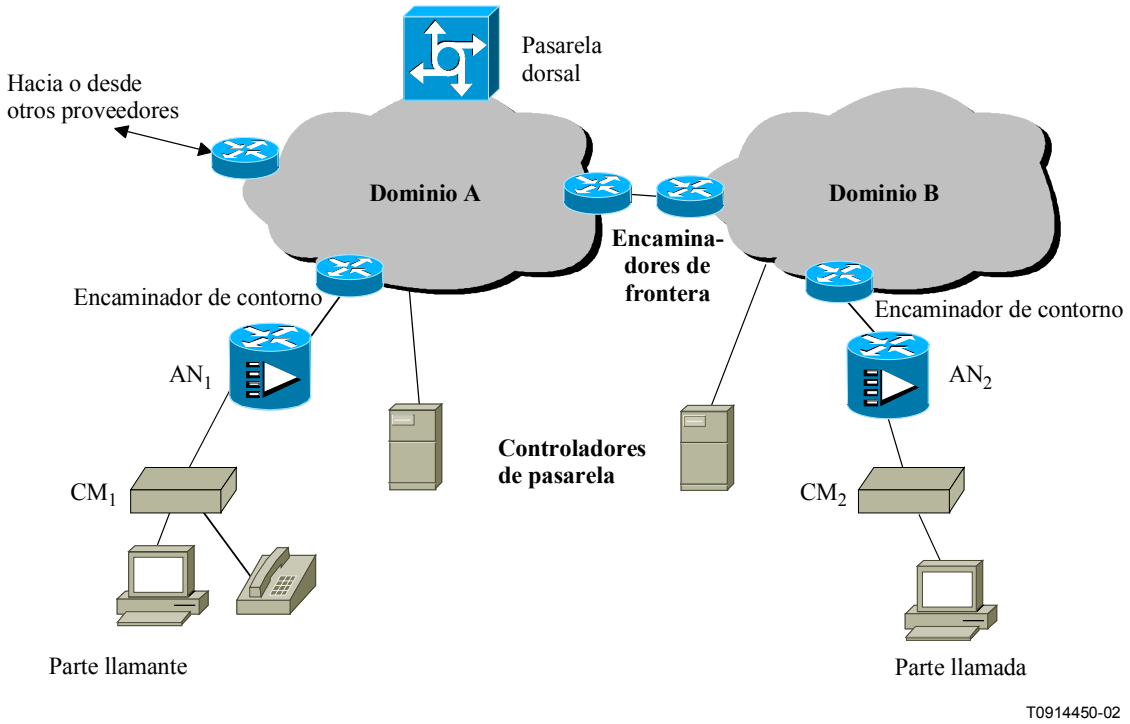


Figura 1/J.174 – Arquitectura QoS interdominio

En esta arquitectura se supone que existe un acuerdo de servicio entre proveedores de servicio en el que se define el nivel de confianza entre dominios IPCablecom así como los requisitos para QoS, señalización de llamada, requisitos de transporte y de interconexión, y otra información de este tipo.

La arquitectura también soporta el transporte de medios y señalización entre dominios y puede atravesar una o más redes IP intermedias o de tránsito. En IPCablecom se da por supuesto que los operadores tendrán acuerdos de transporte con todas las redes de tránsito a que están directamente conectados.

En esta arquitectura se supone que en la red de acceso se utiliza señalización DQoS. La porción de acceso de la red se define como la que está entre el adaptador de terminal de medios (MTA, *media terminal adapter*) y el nodo de acceso (AN, *access node*), e incluye la red híbrida de fibra/cable coaxial J.112.

Como mínimo, se espera que las redes IP dorsal y de tránsito sean conformes con la arquitectura Diffserv. La porción dorsal de la red se define como todos los elementos de red IP entre dos AN. Esto incluye los encaminadores de contorno, de frontera y medulares. En las sesiones que terminan en la RTPC, la red dorsal se puede definir además de modo que incluya todos los recursos entre el AN y la pasarela de medios.

En las cláusulas siguientes se describe una serie de posibles soluciones, las cuales ofrecen diferentes grados de garantía y niveles de complejidad.

Obsérvese que el AN puede o no estar en el contorno de la red dorsal Diffserv, lo que depende de diversos factores que se describen a continuación. Obsérvese asimismo que puede haber dispositivos intermedios (que no aparecen en la figura 1) entre el AN y el contorno de la red dorsal Diffserv.

Los encaminadores de frontera son aquellos que están situados en las fronteras entre proveedores. Estos encaminadores tienen funciones concretas en un entorno Diffserv (tales como la aplicación de políticas y el remarcado) que se describen más detalladamente en las cláusulas que siguen.

7 Utilización de servicios diferenciados (Diffserv) en redes dorsales

En esta cláusula se supone una red dorsal Diffserv [2], [3] sencilla sin otros requisitos de señalización de recursos que los especificados en DQoS. En este caso el AN funciona como el dispositivo de contorno Diffserv. En otras cláusulas se tratará el fundamento de una red dorsal Diffserv añadiendo capacidades de señalización para controlar el acceso a recursos de la red dorsal. Se supone que existe una red dorsal común para datos y voz; otra posibilidad sería utilizar una red física o lógicamente separada para la voz.

7.1 Tráfico de medios

El tráfico de medios IPCablecom se define como los paquetes que se originan o terminan en un punto extremo IPCablecom para el cual se ha solicitado QoS utilizando DQoS. (Obsérvese que esto excluye explícitamente paquetes de señalización de llamada y de QoS tales como mensajes de coordinación de puerta DQoS, mensajes Invite DCS/SIP, etc., los cuales se tratan en 7.2.) En la red dorsal DEBERÍA dedicarse como mínimo un comportamiento por salto (PHB, *per-hop behaviour*) para el tráfico de medios IPCablecom. Este PHB PUEDE ser un EF [10], uno de los PHB AF [9], uno de los PHB selector de clase (CS, *class selector*) o un PHB "privado". Las únicas restricciones son:

- NO DEBE ser el PHB por defecto (de "mejor esfuerzo");
- los únicos paquetes que tenga asignado este PHB DEBERÍAN ser aquellos para los cuales se ha solicitado la QoS utilizando DQoS;
- si se utiliza un PHB AF, DEBERÍA ser Afx1, es decir, debería ofrecer la probabilidad de supresión más baja.

No es obligatorio que todos los dominios utilicen el mismo PHB para los paquetes de medios IPCablecom. Por otra parte, es posible utilizar más de un PHB en un mismo dominio para paquetes de medios IPCablecom, en cuyo caso es necesario proporcionar alguna política en el AN para determinar cuál de los posibles PHB se ha de utilizar para un paquete dado. Se volverá sobre esta cuestión más adelante.

7.2 Tráfico de señalización

El tráfico de señalización incluye, por definición, todos los mensajes de señalización de llamada entre elementos de control de llamada IPCablecom (por ejemplo, mensajes DCS o NCS, mensajes de coordinación de puerta DQoS, mensajes RSVP, etc.). Para controlar la latencia y la pérdida que experimenta el tráfico de señalización, se PUEDEN dedicar uno o más PHB para el tráfico de señalización IPCablecom. Por ejemplo, el PHB CS6 se ha venido utilizando tradicionalmente para el tráfico de encaminamiento. Si se dedica un PHB a los mensajes de señalización, se aplicarán las siguientes directrices:

- el PHB para los mensajes de señalización DEBERÍA ser distinto del PHB de mejor esfuerzo por defecto;
- los únicos paquetes a los que se asignara este PHB DEBERÍAN ser los paquetes de mensajes de señalización;
- el PHB para los mensajes de señalización DEBE ser distinto del PHB que se utiliza para los mensajes de encaminamiento;
- el PHB para los mensajes de señalización DEBERÍA ser distinto del PHB que se utiliza para los mensajes de medios;
- el volumen de tráfico generado con el PHB DEBERÍA estar limitado.

Esta última directriz puede ser difícil de aplicar. Una posible solución es limitar el volumen de tráfico que puede generar cada usuario, límite que marca el código de punto de servicios diferenciados (DSCP) para este PHB a un valor configurado. Este valor ha de ser, justamente, lo

suficientemente grande para aceptar la carga de señalización prevista procedente del usuario. Este límite se puede hacer respetar mediante paquetes de aplicación de política que transportan el DSCP designado en el AN, de manera que los paquetes en exceso marquen ahora como "mejor esfuerzo". Los paquetes en exceso NO DEBERÍAN suprimirse. Al volver a marcar estos paquetes se impide que los usuarios envíen volúmenes considerables de tráfico de datos con el DSCP que está reservado para señalización. Al mismo tiempo, si el volumen de tráfico de señalización ofrecida sobrepasa temporalmente el nivel previsto, el tráfico en exceso se sigue transmitiendo a la red con una probabilidad razonable de entrega a tiempo, con lo que se evita una grave degradación de la calidad de funcionamiento de la señalización.

Obsérvese que la utilización de PHB diferentes para el tráfico de medios y de señalización no implica necesariamente que se dé prioridad relativa a los medios con respecto a la señalización o viceversa. Se trata sencillamente de permitir la asignación independiente de recursos para medios y señalización a fin de satisfacer los objetivos deseados de pérdida y latencia para cada tipo de tráfico.

7.3 Selección del PHB y fijación del DSCP

El AN debe fijar o vigilar el DSCP para los paquetes de medios y de señalización IPCablecom. En la Recomendación [7] sobre la DQoS IPCablecom se proporciona un medio por el cual un controlador de puerta puede decirle al AN, llamada por llamada, mediante el mensaje GATE-SET, qué DSCP habrá de utilizar. El AN DEBE garantizar que el DSCP de todos los paquetes y medios para una llamada dada se fije al valor contenido en el GATE-SPEC para dicha llamada. El AN DEBE garantizar que el volumen de tráfico de medios generado para una llamada dada, y que se marca con el DSCP deseado, no sobrepasa la recomendación relativa al colector de testigos que fue proporcionada por la señalización DQoS.

Cada dominio PUEDE utilizar su propio o sus propios DSCP para cualquiera o cualesquiera PHB que utilice, independientemente de los demás dominios, siempre que la elección sea coherente en un mismo dominio. Si se utiliza un PHB estándar DEBERÍA utilizarse el punto de código recomendado IETF según está definido en [9] y [10]. Si se utilizan DSCP diferentes para paquetes de medios y señalización IPCablecom en dominios vecinos, el remarcado DSCP DEBE realizarse mediante un encaminador de frontera sobre los paquetes que salen de un dominio y entran en otro. A continuación se describen las capacidades obligatorias de los encaminadores de frontera.

Los encaminadores en las fronteras de dominio DEBEN también poder fijar o vigilar el DSCP para paquetes que están destinados a un punto extremo IPCablecom y para los cuales se ha solicitado QoS utilizando DQoS. Si no hay señalización explícita en las fronteras de dominio no es posible identificar con autoridad los paquetes de medios IPCablecom que llegan a un encaminador de frontera en cada flujo. Por consiguiente, los encaminadores de frontera deben basarse en el DSCP para identificar dichos paquetes. Por esta razón, el encaminador de frontera DEBERÍA proporcionar las capacidades siguientes:

- DEBERÍA ser posible configurar el encaminador de frontera para imponer un límite al volumen total de tráfico que entra en el dominio y que está marcado con un determinado DSCP.
- DEBERÍA ser posible configurar el encaminador de frontera para modificar el DSCP del tráfico que entra en el dominio. Esta capacidad se utiliza cuando se sabe que se está utilizando un DSCP distinto para paquetes de medios IPCablecom en un dominio desde el cual se reciben paquetes. Es decir, un encaminador puede configurarse para reconocer paquetes que llegan a una interfaz con DSCP = x como paquetes de medios IPCablecom y posteriormente transmitirlos a otra interfaz con DSCP = y (donde x ! = y). Esta correspondencia de un DSCP a otro DEBERÍA negociarse entre los operadores de las redes pares.

Las pasarelas troncales DEBERÍAN también fijar el DSCP adecuado en los paquetes que generan y que están destinados a un punto extremo DQoS. Por ejemplo, esto puede lograrse señalizando el DSCP deseado en TGCP [14] (obsérvese que en la Recomendación sobre TGCP se utiliza el término obsoleto tipo de servicio). También puede ser aceptable que una pasarela fije el mismo valor DSCP en todos los paquetes que genere. Si la pasarela troncal no puede marcar correctamente los paquetes que genera, DEBERÍA configurarse otro dispositivo situado entre la pasarela y la red dorsal (por ejemplo, un encaminador) que fijara el DSCP para los paquetes de medios IPCablecom que entran en la red dorsal, procedentes de la pasarela.

Se RECOMIENDA que haya otros elementos IPCablecom en el trayecto de medios (por ejemplo servidores de audio/anuncios, anonimizadores, puentes de conferencias, etc.) capaces de marcar los paquetes por ellos generados y que están destinados a puntos extremos QoS.

Todos los dispositivos dentro de un mismo dominio que fijen o vigilen el DSCP para los paquetes de medios IPCablecom, o proporcionen QoS a los paquetes examinando su DSCP DEBERÍAN tener una configuración compatible. Esto puede lograrse utilizando COPS con configuración [13] o por otros medios.

Es posible utilizar múltiples PHB para diferentes tipos de servicio. Por ejemplo puede resultar apropiado utilizar diferentes PHB para vídeo y para voz, o pudiera ser conveniente utilizar PHB diferentes para llamadas con requisitos de retardo más estrictos debido a la distancia entre los puntos extremos o a otros factores. Los mecanismos para señalar la selección adecuada de PHB en este caso se han descrito antes.

7.4 Soporte de PHB por el AN

A partir de los criterios anteriores se selecciona uno o más PHB para utilizarlos en la red dorsal. El AN DEBERÍA implementar todos estos PHB en sus enlaces hacia el origen (es decir los enlaces que lo conectan a la red dorsal) para suministrar una QoS adecuada a los paquetes que entran en la red dorsal. Otra posibilidad es sobreconfigurar los enlaces hacia el origen en el AN en lugar de confiar en que Diffserv estará soportado en estos enlaces. Es importante observar que las soluciones basadas en la sobreconfiguración, aunque son viables en cuanto a la QoS, no son siempre las más económicas o eficaces en cuanto a los recursos.

7.5 Asignación de recursos

Es necesario garantizar la asignación de recursos suficientes para los PHB seleccionados en todos los elementos de red de la red dorsal. Si no hay señalización en la red dorsal, esto es fundamentalmente un problema de configuración. Se puede utilizar COPS [13] u otros medios para distribuir la información de configuración a los elementos de red.

7.6 Control de admisión

Incluso en una red dorsal de servicios diferenciados (Diffserv) configurada estáticamente es posible realizar control de admisión en ciertos puntos de la red. Una posibilidad es realizar el control de admisión en el AN; otra, es realizarlo en el CMS. Una, ambas o ninguna de estas opciones pueden ser adecuadas. Por ejemplo si el ancho de banda hacia el origen, desde el AN hacia la red dorsal, es grande en comparación con la capacidad de los enlaces J.112 servidos por ella, puede que no sea necesario realizar el control de admisión en los enlaces del AN en el sentido hacia el origen.

Si se va a realizar el control de admisión en el AN, cada AN DEBE configurarse con un ancho de banda máximo para cada PHB que se va a utilizar para tráfico de medios IPCablecom en cada una de sus interfaces hacia el origen (no especificadas en J.112). Además cada AN DEBE llevar la cuenta de la cantidad de ancho de banda que se ha admitido para cada PHB en cada interfaz. Cuando un AN recibe una petición DqoS para la admisión de una llamada, determinará qué PHD habrá de ser utilizado por la llamada, consultando para ello la correspondencia DSCP-PHB con la que está configurada, y utilizando el DSCP proporcionado en el GATE-SET. El AN DEBE

comprobar que el ancho de banda disponible en ese PHB, en la interfaz de salida que será utilizado por esta llamada, será suficiente para dar cabida a los recursos requeridos por la llamada. De esta manera el volumen total de tráfico de un PHB dado que será introducido en la red por cualquier AN está acotado.

En ciertas circunstancias también puede ser posible realizar el control de admisión basado en CMS. Si se puede proporcionar información suficiente sobre los recursos y topología de red a un CMS, éste podrá realizar el control de admisión en función del destino de las llamadas. Por ejemplo, el CMS X puede saber que las llamadas cuyo destino está gestionado por el CMS Y deben pasar a través de un enlace de capacidad conocida, y puede por tanto rechazar las llamadas hacia ese destino cuando la capacidad se haya agotado.

Los métodos de control de admisión descritos en esta cláusula pueden tener ciertas limitaciones. En particular, puede que no tengan en cuenta el trayecto completo que seguirán los paquetes a través de la red dorsal para una determinada llamada. Tampoco tienen necesariamente en cuenta la posibilidad de fallos del enlace que afecten a la capacidad disponible. Por consiguiente, existe el riesgo de que algunos enlaces lleguen a tener demasiados abonados. A continuación se examinan soluciones a estos problemas.

8 Control de admisión para un solo dominio

8.1 Plano de control RSVP por flujo

Es posible utilizar RSVP por flujo como el protocolo de admisión para un grupo de servicios diferenciados (nube Diffserv). En la referencia [4] se presenta una visión general de este método. En esta cláusula se describe la aplicación de la señalización RSVP por flujo a una red dorsal Diffserv en un entorno IPCablecom. La solución que se describe es más escalable que el RSVP por flujo tradicional porque toda clasificación y calendarización (es decir todas las operaciones en el plano de reenvío) se realizan en agregados de comportamientos Diffserv.

Para soportar las capacidades descritas en esta cláusula, la funcionalidad básica Diffserv descrita en la cláusula 7 DEBE proporcionarse en el AN y en la red dorsal. En los siguientes párrafos se presentan requisitos adicionales.

Para soportar un plano de control RSVP por flujo, los AN que participan en la señalización DQoS DEBEN soportar los dos modos de operación siguientes:

- Modo RSVP de extremo a extremo. En este modo, el MTA señaliza con mensajes RSVP según lo descrito en la cláusula 6/J.163 [7] y el AN DEBE reenviar dichos mensajes RSVP hacia el MTA del extremo distante de la llamada.
- Modo señalización incorporada. En este modo el MTA incorporado utiliza señalización J.112, y el AN DEBE originar mensajes RSVP y enviarlos al MTA del extremo distante.

En ambos modos el resultado es que se utiliza RSVP por flujo entre los dos AN que intervienen en una llamada. Puede tratarse de un verdadero RSVP de extremo a extremo (MTA-MTA) o solamente entre los AN que actúan como apoderados para los MTA; esto no tiene efecto alguno sobre el mecanismo QoS de la red dorsal.

En el caso del RSVP por flujo que funciona entre dos AN, el operador de red dispone de bastante flexibilidad a la hora de situar el contorno de la región Diffserv. Según se muestra en la figura 1, el contorno de la red Diffserv no tiene necesariamente que ser el AN, aunque puede serlo. Es decir, el RSVP por flujo con clasificación y calendarización por flujo puede utilizarse desde el AN hasta el contorno de la región Diffserv; otra posibilidad es que el AN esté en el contorno de la región Diffserv, en cuyo caso se utiliza la planificación y clasificación compuestas en todo el tráfico del AN en el sentido hacia el origen.

Para una mayor generalidad en la exposición se utiliza el concepto de encaminador de contorno (ER, *edge router*) definido en [4]. Este dispositivo es capaz de realizar RSVP por flujo y control de admisión sobre el tráfico que entrará en la red de servicios diferenciados (Diffserv). El AN PUEDE realizar la función ER o bien esta función se puede asignar a un encaminador en el sentido hacia el origen del AN, es decir un encaminador que esté más cerca de la red dorsal.

En las cláusulas siguientes se describe el comportamiento de los AN, los encaminadores de contorno y los encaminadores medulares (es decir los encaminadores Diffserv en la red dorsal que no son encaminadores de contorno).

8.1.1 Comportamiento del AN

Un AN puede funcionar en uno de dos modos, lo que dependerá de que el MTA por él servido utilice señalización incorporada o señalización RSVP. Ambos modos DEBEN estar soportados. Cada modo se trata por separado más adelante. En cada caso el AN utiliza RSVP por flujo en sus interfaces hacia el origen (no especificadas en J.112) y utiliza procedimientos RSVP/Intserv normalizados para el control de admisión, clasificación y calendarización para los paquetes transmitidos por dichas interfaces.

Obsérvese que cualquiera que sea el modo de funcionamiento, el AN se encarga de reenviar (u originar) los mensajes PATH y RESV hacia el extremo lejano. Se establece una reserva bidireccional entre los dos AN cuando se ha intercambiado entre ellos un par de mensajes RESV.

8.1.1.1 Señalización incorporada

Cuando utiliza la señalización incorporada, definida en los anexos A y B de la Rec. UIT-T J.163 [7], un AN detecta la necesidad de realizar una reserva en la red dorsal cuando llega un mensaje de señalización de la capa MAC que indica la petición de establecimiento de un nuevo flujo J.112 y cuando se ha establecido una puerta para la correspondiente llamada. En este caso, el AN DEBE enviar un mensaje PATH al MTA en el extremo distante utilizando los parámetros derivados del mensaje MAC para crear el PATH según se describe más adelante. Seguidamente, espera hasta que reciba un mensaje RESV del AN o del MTA del extremo distante. Una vez recibido dicho mensaje del extremo distante, sabe que la reserva se ha realizado con éxito y DEBE responder al MTA con un mensaje de señalización de la capa MAC por el que indique que la reserva se ha realizado correctamente.

Cuando un AN recibe un mensaje PATH procedente de una AN o un MTA en el extremo lejano, y el PATH está destinado a un MTA que no soporta RSVP, el AN DEBE verificar en primer lugar que dispone de una puerta establecida para la correspondiente llamada. Si es así, DEBE responder con un mensaje RESV transmitido en retorno al salto precedente (PHOP, *previous hop*) contenida en ese mensaje PATH. Los parámetros del RESV se determinan a partir del mensaje PATH recibido.

El tipo y formato de los mensajes de señalización de la capa MAC que se utilicen para establecer los flujos J.112 dependen del protocolo de capa 2 implementado en la red de televisión por cable. En los anexos A, B y C a la Recomendación J.112 se puede encontrar más información sobre la señalización MAC.

8.1.1.1.1 Determinación de los parámetros de PATH en el protocolo RSVP

Para generar un mensaje PATH en el protocolo RSVP (una vez recibido un mensaje de capa MAC que indica la necesidad de realizar una reserva en la red dorsal) el AN necesita construir el objeto sesión, el objeto plantilla de emisor y el objeto Tspec de emisor. El objeto sesión consiste en el protocolo, la dirección de destino y el número de puerto de destino. El objeto plantilla de emisor consiste en la dirección del emisor y el número de puerto del emisor. En el siguiente cuadro se presenta la correspondencia de los parámetros RSVP a los parámetros contenidos en el mensaje MAC.

Parámetro RSVP	Parámetro RESC-REQ Anexo A de J.112	Parámetro DSA-REQ Anexos B y C de J.112
Objeto de sesión		
Id de protocolo	Session_Binding_US. Upstream_internet_protocol	Clasificador de paquete hacia el origen. Protocolo IP.
Dirección de destino	Session_Binding_US. NIU_client_destination_IP_add	Clasificador de paquete hacia el origen. Dirección de destino IP.
Puerto de destino	Session_Binding_US. NIU_client_destination_port	Clasificador de paquete hacia el origen. Comienzo del puerto de destino TCP/UDP
Objeto plantilla de emisor		
Dirección de origen	Session_Binding_US. NIU_client_source_IP_add	Clasificador de paquete hacia el origen. Dirección de origen IP
Puerto de origen	Session_Binding_US. NIU_client_source_IP_port	Clasificador de paquete hacia el origen. Comienzo de puerto de origen TCP/UDP

Los parámetros Tspec de emisor se obtienen de las codificaciones de parámetros QoS hacia el origen J.112 contenidas en el mensaje de señalización de la capa MAC que solicita el establecimiento del nuevo flujo. A continuación se presenta un ejemplo de correspondencia de los parámetros QoS MAC al objeto Tspec para construir el mensaje PATH del RSVP. Para más información consúltese los anexos A, B o C de la Rec. UIT-T J.112.

El mensaje PATH también debería contener el objeto Adspec actualizado, el cual transporta el retardo adicional introducido por el AN en los encaminadores RSVP hacia el destino. Debido a los estrictos requisitos del límite de latencia, se prevé que los anfitriones que generen tráfico VoIP indicarán sus necesidades de recursos utilizando los parámetros de QoS del servicio garantizado según lo definido por la arquitectura IntServ. Por lo tanto, el bloque servicio garantizado del objeto Adspec debería contener los términos C (componente dependiente de la velocidad) y D (componente independiente de la velocidad) adecuados. En el valor de D se ha de tener en cuenta el retardo fijo (por ejemplo el retardo de procesamiento del mensaje, el retardo introducido por la codificación/decodificación, etc.).

8.1.1.1.1.1 Construcción del objeto Tspec a partir de los parámetros QoS en el anexo A de J.112

Para satisfacer las características de velocidad binaria constante (CBR) que presentan normalmente las fuentes de voz puede utilizarse el modo de acceso a velocidad fija o por reserva.

Este asunto queda en estudio.

8.1.1.1.1.2 Construcción del objeto Tspec a partir de los parámetros QoS en los anexos B y C de J.112

Puesto que las fuentes de voz presentan normalmente características de CBR, se prevé que los MTA pedirán un servicio de concesión no solicitada (UGS, *unsolicited grant service*) en el enlace J.112. Si el "tipo de calendarización de flujo de servicio" en el mensaje DSA-REQ se fija a UGS, el Tspec de emisor se determina de la manera siguiente. Sea:

G = tamaño de concesión (octetos);

I = intervalo de concesión (segundos).

Para flujos VoIP el parámetro "concesiones por intervalo" se fijaría normalmente a 1 (si es mayor que 1, G se ha de calcular en consecuencia). Dado lo anterior, los parámetros IntServ para el colector de testigos son:

M (tamaño máximo de datagrama) = G – tara Ethernet – tara ES 201 488;

r (velocidad de colector) = M/I.

La tara de encabezamiento Ethernet es de 18 octetos y la tara de encabezamiento correspondiente al anexo B/C de J.112 podría ser de hasta 13 octetos. Puesto que las fuentes VoIP presentan características de CBR,

p (velocidad de cresta) = r;

b (profundidad del colector) = M y;

m = M.

La tara correspondiente al anexo B/C de J.112 sólo incluye la tara de la capa MAC (encabezamiento MAC estándar, encabezamiento BPI extendido, etc.). No incluye la tara de la capa física.

Si se utiliza la supresión del encabezamiento de cabida útil en el sentido hacia el origen, M (según se ha calculado anteriormente) DEBE modificarse de nuevo para que refleje los octetos suprimidos. El parámetro "tamaño PHS" del DSA-REQ DEBE utilizarse para modificar M de la manera siguiente:

M' = M – 2 + tamaño PHS,

donde dos octetos constituyen encabezamiento extendido correspondiente al anexo B/C de J.112, que contiene el valor para el índice PHS. Puesto que el tamaño de la concesión también incluye esta tara, DEBE restarse para calcular M'.

Los demás parámetros Tspec se modifican en consecuencia:

r = M'/I;

p = r;

b = M';

m = M'.

En lo que respecta al objeto Adspec actualizado, el valor anunciado de C para el servicio UGS sería M (o M').

8.1.1.1.2 Determinación de los parámetros RESV del RSVP

Cuando un AN recibe un mensaje PATH del AN distantes, DEBE enviar el mensaje RESV para reservar los recursos adecuados en la red dorsal. El mensaje RESV DEBE incluir el objeto sesión, flowspec y filterspec. El objeto sesión y filterspec se obtienen del mensaje PATH. El tráfico VoIP debería utilizar las especificaciones de flujo del servicio garantizado, que consisten en una Tspec y una Rspec. Los parámetros Tspec se obtienen del objeto Tspec del emisor en el mensaje PATH. Los parámetros Rspec se obtienen a partir de los parámetros QoS hacia el destino especificado en J.112. En un entorno del anexo B/C de J.112, los parámetros Rspec se calculan del modo siguiente:

R = "Velocidad máxima del tráfico sostenido hacia el destino".

S = 0.

El valor recomendado para S (huelgo) es cero cuando no se especifica ninguno.

8.1.1.2 Señalización RSVP

Cuando el MTA utiliza señalización RSVP según se define en la cláusula 6/J.163 [7], y en la red dorsal se ha de soportar la señalización RSVP por flujo, el AN DEBE poder reenviar mensajes RSVP a la red dorsal en lugar de limitarse a interceptarlos cuando los recibe del MTA. El AN DEBE soportar un parámetro configurable en cada una de sus interfaces de red no especificadas en J.112 que define si el reenvío de mensajes RSVP está habilitado para la interfaz. Cuando dicho parámetro tiene el valor "habilitado" en una determinada interfaz, y el AN recibe un mensaje PATH procedente de un MTA que DEBERÍA enviarse a través de dicha interfaz de acuerdo con el cuadro de reenvíos del AN, el AN DEBE reenviar el mensaje PATH por dicha interfaz. Al reenviar dicho mensaje PATH que había recibido del MTA, el AN DEBE suprimir todos los objetos específicos de DQoS (por ejemplo Tspec inverso, etc.) antes de reenviar el mensaje hacia su destino. En esta

configuración, el AN, actuando como apoderado, NO DEBERÍA enviar mensajes RESV de vuelta hacia el MTA, sino que, en lugar de esto, DEBERÍA esperar la recepción de un mensaje RESV procedente de la red dorsal y seguidamente procesarlo y reenviarlo de conformidad con las reglas de procesamiento RSVP normalizadas. De manera similar, actuando como apoderado, NO DEBERÍA enviar mensajes PATH hacia el MTA, sino que, en lugar de esto, DEBERÍA esperar la recepción de un mensaje PATH del extremo lejano de la llamada, el cual DEBE procesar de conformidad con las reglas RSVP normalizadas.

Obsérvese que la decisión de reenviar los mensajes PATH a la red dorsal en lugar de actuar como un apoderado según lo descrito en la cláusula 6/J.163 [7] depende de la configuración de cada interfaz. Por consiguiente todos los flujos de paquetes de medios IPCablecom que atraviesen una interfaz configurada según lo descrito anteriormente estarán sometidos a control de admisión. Este comportamiento es deseable ya que garantiza que todos los flujos que entran en la red a través de una interfaz dada estarán sometidos a control de admisión, lo que permite tomar decisiones de control de admisión inteligentes[1].

8.1.2 Ubicación del contorno Diffserv

Cuando se utiliza un plano de control RSVP por flujo en la red dorsal, no es necesario que el AN esté en el contorno de la nube Diffserv. En cambio, la función de contorno Diffserv puede residir en un encaminador de contorno situado hacia el origen con respecto al AN. En este caso, entre el AN y el encaminador de contorno hay una red, que puede ser tan sencilla como un enlace punto a punto (véase la figura 1) o una red IP de topología general. La QoS requerida se puede proporcionar entre el AN y el encaminador de contorno mediante la utilización de servicios integrados o mediante el suministro de ancho de banda. Puede elegirse uno u otro método para cada enlace.

8.1.3 Comportamiento del encaminador de contorno

Si el encaminador de contorno es el AN o algún otro encaminador situado hacia el origen con respecto al AN, DEBE participar en el RSVP por flujo. Además, el encaminador de contorno (ER) dispone de un conjunto de interfaces algunas de las cuales son "interiores" a la nube Diffserv y otras son "exteriores". El ER está encargado de marcar los paquetes que pasan de una interfaz exterior a una interfaz interior con un DSCP elegido adecuadamente, a no ser que pueda confiar en que el DSCP se había fijado correctamente en el AN. El ER DEBE realizar el control de admisión en todas sus interfaces. Para hacer esto en las interfaces interiores, cada una de éstas debe configurarse con un conjunto de recursos disponibles para cada PHB que se va a utilizar en el tráfico de medios IPCablecom. El ER realiza el control de admisión sobre este conjunto de recursos para cada petición RSVP que recibe. El ER debe también poder determinar qué PHB y DSCP ha de utilizar para una petición RSVP dada. Esto se puede determinar mediante configuración local o como una cuestión de política proporcionada a partir de alguna fuente exterior, por ejemplo un servidor de políticas.

Un ER PUEDE realizar operaciones de clasificación, aplicación de políticas y calendarización de microflujo en sus interfaces exteriores pero DEBE realizar operaciones de clasificación, aplicación de políticas y calendarización compuestas en sus interfaces interiores. Si el ER no realiza operaciones de clasificación y aplicación de políticas de microflujo en los flujos que lo atraviesan para pasar a la red dorsal, esas funciones las DEBEN realizar los AN que envían tráfico al ER. La aplicación de políticas de microflujo en el AN puede proporcionar una mayor escalabilidad que si se aplican en el ER, puesto que el número de flujos es probablemente mayor en el ER.

---

[1] Otra posible solución sería decidir para cada flujo si se reenvían o no los mensajes PATH. Esto podría plantear la cuestión de cómo tomar tal decisión, pero, lo que es más importante, existiría el riesgo de que algún subconjunto de flujos introdujera en la red dorsal tráfico que no estuviera sometido a control de admisión, lo cual comprometería la excactitud global del control de admisión.

8.1.4 Otros dispositivos terminadores (pasarelas de medios, anonimizadores, servidores de anuncios, puentes de conferencia)

Para que la señalización RSVP por flujo funcione eficazmente a través de la red dorsal, todos los dispositivos que pueden terminar un tren de medios DEBERÍAN poder soportar la señalización RSVP por flujo. Entre estos dispositivos están las pasarelas de medios, anonimizadores, servidores de anuncios, puentes de conferencia, etc. Todo dispositivo que termine un tren de medios IPCablecom DEBERÍA:

- Enviar mensajes PATH hacia el(los) extremo(s) lejano(s) de la llamada.
- Recibir mensajes PATH y RESV procedentes del(los) extremo(s) lejano(s) de la llamada.
- Enviar mensajes RESV hacia el(los) extremo(s) lejano(s) de la llamada en respuesta a los mensajes PATH recibidos.

Estos dispositivos obtienen el contenido de los mensajes PATH a partir de la señalización de llamada de la misma manera que lo obtienen un MTA en operación DQoS normal. El contenido de los mensajes RESV se puede obtener a partir de los mensajes PATH de igual forma que la descrita en 8.1.1.

Obsérvese que, al igual que un AN, los dispositivos mencionados en esta cláusula pueden o no funcionar como encaminadores de contorno, según estén o no en el contorno de la nube Diffserv.

8.1.5 Comportamiento del encaminador medular

Un encaminador se comporta como un encaminador medular cuando recibe paquetes en una interfaz interior y los reenvía en una interfaz interior. Obsérvese que un mismo encaminador puede comportarse como un ER con respecto a ciertos flujos y como un encaminador medular con respecto a otros.

Un encaminador medular no realiza el remarcado del DSCP en los paquetes que reenvía. Realiza el control de admisión de los recursos asignados al PHB adecuado para cada reservación. Realiza operaciones de clasificación, aplicación de políticas y calendarización compuestas. Por consiguiente el comportamiento de reenvío de un encaminador medular es igual al de un encaminador Diffserv, aún cuando utilice RSVP para el control de admisión.

8.1.6 Latencia de señalización

El método de reserva de ancho de banda descrito en esta cláusula requiere que los mensajes RSVP de extremo a extremo atraviesen la red dorsal. Evidentemente esto puede repercutir en la latencia de señalización total y por consiguiente en el retraso posterior a la marcación. Para satisfacer los objetivos de tiempo de espera después de marcar un proveedor se pueden utilizar las técnicas siguientes:

– Reducir la renovación y aumentar la fiabilidad del RSVP.
– Seleccionar un PHB de baja latencia y el DSCP correspondiente para los mensajes de control RSVP.

Esto mismo se aplica para el método que se define en la cláusula siguiente.

8.1.7 Preapropiación

En esta cláusula se describen los mecanismos que pueden utilizarse para el soporte de la preapropiación de reservas (por ejemplo para suministrar recursos a llamadas de emergencia con preferencia sobre llamadas admitidas antes).

El elemento de prioridad por preapropiación definido para uso en RSVP y COPS [6] se PUEDE utilizar en la red dorsal. No se prevé que este objeto lo facilite el MTA, puesto que por lo general no se puede confiar en que los usuarios de extremo determinen su propia prioridad por preapropiación. No obstante, el controlador de puerta proporciona una clase Sesión al AN que éste PUEDE utilizar

para generar un elemento de prioridad por preapropiación válido. En este caso, el AN DEBERÍA utilizar la siguiente correspondencia de valores de la clase Sesión a valores de prioridad por preapropiación.

Tipo de sesión	Valor de la clase sesión	Valor de prioridad por preapropiación
Normal	0x01	32767
Prioridad más alta (emergencia)	0x02	64911

Esta correspondencia DEBERÍA ser configurable. El elemento de prioridad por preapropiación contiene un campo de la prioridad que se defiende y un campo de la prioridad por preapropiación, los cuales DEBERÍAN fijarse al mismo valor.

También es posible que los encaminadores con capacidad RSVP en la red dorsal utilicen COPS para la externalización de las decisiones de política. En este caso el elemento de prioridad por preapropiación PUEDE incluirse dentro de una decisión COPS y los encaminadores DEBEN interpretarlos según lo definido en [6].

8.2 RSVP compuesto

El RSVP compuesto, o RSVP agregado [5] es una extensión lógica al RSVP por flujo a través de la red dorsal Diffserv. Para soportar esta funcionalidad se DEBEN proporcionar las funciones AN, encaminador de contorno y encaminador medular descritas en 8.1. Se proporciona funcionalidad adicional agregando y desagregando encaminadores, según se describe más adelante. La señalización RSVP se realiza entre puntos extremos de llamada (los MTA o AN actuando en representación de los MTA) según se describió en la cláusula anterior. Además de la funcionalidad descrita en 8.1, el RSVP agregado define una posible manera de combinar muchas reservas de RSVP por flujo para formar una sola reserva agregada. Se pueden agregar dos o más reservas RSVP por flujo cuando sus trayectos pasan a través del mismo par de encaminadores. Los encaminadores que pueden agregar y desagregar reservas se designan por encaminadores de agregación. El comportamiento de los encaminadores agregadores y desagregadores se define de manera más formal en IETF RFC 3175 [5].

Los encaminadores de agregación se encargan de crear reservas compuestas a través de una región de agregación, que puede ser la totalidad de la nueve Diffserv o una región de agregación definida dentro de la nube. Cada reserva compuesta representa un flujo de tráfico desde un encaminador de ingreso (o agregador) a un encaminador de egreso (o desagregador). Las reservas compuestas se pueden configurar estáticamente sobre la base del volumen previsto desde un encaminador de ingreso a un encaminador de egreso, o se pueden establecer y redimensionar automáticamente según se describe en [5]. Cada reserva compuesta transporta el tráfico procedente de cierto número de reservas RSVP "de extremo a extremo" que comparten un par común de encaminadores de ingreso/egreso. Una reserva de extremo a extremo representa un único microflujo, y la señalización para dicha reserva se lleva a cabo utilizando el RSVP normalizado. Los mensajes RSVP "de extremo a extremo" los puede originar el MTA, o el AN a nombre del MTA en el caso de la señalización incorprada, según se describió anteriormente. Tales mensajes RSVP de extremo a extremo (o mensajes E2E) son "tunelizados" a través de la región de agregación fijando el número de protocolo IP en el mensaje de trayecto a "RSVP-E2E-IGNORE".

Obsérvese que el agregador y el desagregador pueden ser o no encaminadores de contorno definidos anteriormente. En 8.2.4 se definirá la relación entre estos dispositivos.

8.2.1 Provisión de reservas compuestas

Es posible proveer una reserva compuesta desde un encaminador de ingreso (agregador) a un encaminador de egreso (desagregador). Para ello se necesita conocer de antemano el volumen

previsto entre los encaminadores a fin de determinar el tamaño de la reserva. En este caso, el encaminador de ingreso envía un mensaje PATH de agregación al encaminador de egreso, y el encaminador de egreso responde con un mensaje RESV de agregación hacia el de ingreso. Esto establece una reserva compuesta (o de agregación) para el tráfico que fluye del ingreso al egreso que se marca con el DSCP adecuado según lo determinado en los mensajes RSVP de agregación.

Una vez establecida una reserva compuesta entre un par de encaminadores, se puede tratar como un enlace lógico para los propósitos del control de admisión. El control de admisión para cada llamada se realiza cuando llega un RESV de extremo a extremo (E2E) al encaminador de egreso. Antes de que esto pueda suceder, se DEBE enviar un mensaje E2E Path del ingreso al egreso. El encaminador de ingreso cambia el ID del protocolo a RSVP-E2E-IGNORE, lo que significa que todos los encaminadores entre el ingreso y el egreso ignoran el mensaje Path (Trayecto). Cuando el encaminador de egreso recibe el mensaje E2E Path, el PHOP (salto precedente) identifica el encaminador de ingreso. El encaminador de egreso almacena esta información y seguidamente reenvía el mensaje Path hacia su destino.

Cuando un RESV E2E llega al encaminador de egreso, éste determina a qué reserva compuesta pertenece esta reserva E2E examinando para ello la información de PHOP en el estado Path (Trayecto) que concuerda con el RESV. Este PHOP es el encaminador de ingreso para la reserva compuesta adecuada. El encaminador de egreso DEBE seguir la traza de los recursos asignados a una determinada reserva compuesta a medida que vayan siendo consumidos por reservas E2E admitidas y DEBE rechazar las reservas E2E que no puedan tener cabida en la reserva compuesta adecuada.

8.2.2 Reserva compuesta dinámica

Los inconvenientes más obvios de proveer estáticamente reservas compuestas son que deben dimensionarse de manera adecuada, y que el sobredimensionamiento desperdicia recursos mientras que el subdimensionamiento da lugar a que se bloqueen demasiadas llamadas. Estos inconvenientes se superan creando y redimensionando dinámicamente reservas compuestas en respuesta a la llegada o salida de reservas E2E. En [5] se describe más detalladamente la creación, redimensionamiento y supresión automáticas de reservas compuestas.

Un asunto a tener en cuenta al redimensionar dinámicamente reservas es la cantidad de tara de señalización que puede resultar. Si la dimensión de la reserva compuesta se ajusta para cada reserva E2E que llega o que sale, la tara de señalización permanece igual a la que habría sin la agregación RSVP, aunque no obstante se reduce el estado de reserva almacenado. Si se prevé que una tara de señalización excesiva pueda cuasar problemas, es preferible utilizar una solución heurística para dimensionar la reserva compuesta, por ejemplo redondeando por exceso el ancho de banda compuesto reservado a un valor un poco mayor que la suma de las reservas E2E actuales.

8.2.3 Agregación jerárquica

Según se define en [5], las reservas compuestas pueden agregarse unas a otras. De este modo puede conseguirse reducir aún más el número total de reservas que deben realizarse a través de la red dorsal, aunque evidentemente la reducción real depende mucho de la topología.

8.2.4 Ubicación de los puntos de agregación y del contorno DiffServ

Al igual que en 8.1.2, el contorno DiffServ puede estar en el AN o más hacia el origen en la red dorsal, y se aplican aquí las mismas opciones para el suministro de QoS entre el AN y el contorno DiffServ. Los proveedores disponen de bastante flexibilidad a la hora de ubicar los puntos de agregación (encaminadores agregadores y desagregadores). Un punto de agregación puede coincidir con el contorno DiffServ (es decir, un encaminador de contorno PUEDE realizar agregación) o puede situarse dentro de la nube DiffServ. Los puntos de agregación NO DEBEN situarse fuera de la nube DiffServ.

Una posibilidad es hacer que el AN sea tanto el encaminador de contorno DiffServ como el punto de agregación. En este caso el AN realiza la función de encaminador de contorno y además realiza la agregación y desagregación. Aunque en esta configuración es teóricamente posible prescindir de la señalización RSVP de extremo a extremo de flujos individuales, la señalización RSVP de extremo a extremo tiene dos ventajas.

– La primera es que proporciona una forma sencilla de detectar a cuál de las reservas compuestas, entre las muchas posibles, pertenece un flujo determinado,

– proporciona un mecanismo mediante el cual los puntos extremos pueden reconocer la necesidad de crear dinámicamente una reserva compuesta o aumentar o disminuir el tamaño de una reserva compuesta.

La segunda ventaja no se aplica a reservas compuestas configuradas estáticamente. En algunos casos hay otras maneras de determinar la reserva compuesta a la que pertenece un determinado flujo. Por ejemplo si el AN de agregación y el de desagregación están en la misma zona de una red que utiliza encaminamiento basado en el estado del enlace, puede utilizarse la base de datos de estado del enlace para determinar el desagregador dada la dirección del MTA del extremo lejano.

La realización de la agregación en el AN da lugar a un número posiblemente grande de reservas compuestas en la red dorsal; su magnitud puede ser del orden del cuadrado del número de AN. Si el número de llamadas establecidas entre un par de AN es normalmente pequeño, es más conveniente efectuar más agregaciones en la red dorsal.

Un determinado punto de agregación puede optar por agregar tráfico hacia algunos destinos y no hacia otros en base a una política local (por ejemplo, realizar la agregación únicamente cuando el número de llamadas hacia ese destino sobrepase un cierto umbral).

Al igual que en 8.1.3, la aplicación de políticas de microflujo DEBE realizarse antes de que los paquetes de un flujo entren en la nube DiffServ. Esta función la puede realizar el AN o el encaminador de contorno.

8.3 Intermediario de ancho de banda

El concepto de intermediario de ancho de banda (véase la figura 2) se utilizó por primera vez en [8] y ha sido objeto de importantes investigaciones. Un intermediario de ancho de banda es un agente de control de admisión centralizado al que se le pueden hacer peticiones de ancho de banda. Las peticiones las pueden hacer anfitriones, otros intermediarios en dominios vecinos o encaminadores de contorno. En un entorno IPCablecom cada AN o CMS podría realizar peticiones de ancho de banda a un intermediario de ancho de banda que fuera responsable de gestionar el acceso al ancho de banda para un dominio. Estas peticiones especificarían también el PHB para el cual se ha hecho la petición. El intermediario de ancho de banda para cada dominio es por tanto responsable de realizar peticiones de ancho de banda desde dominios vecinos.

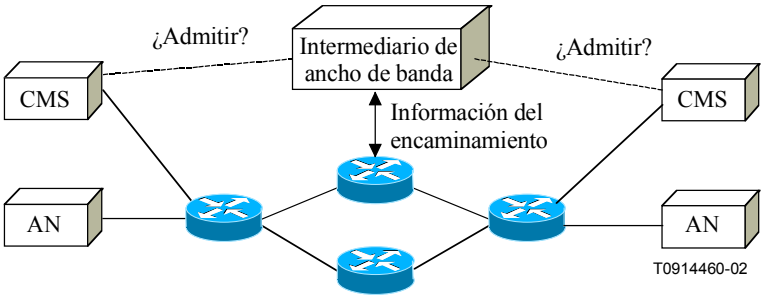


Figura 2/J.174 – Ejemplo de intermediario de ancho de banda

Hay bastante flexibilidad en cuanto al algoritmo y mecanismo de control de admisión que el intermediario de ancho de banda puede utilizar. Cada intermediario debe rechazar toda petición de ancho de banda para un PHB dado que podría comprometer demasiados recursos y degradar la calidad de las llamadas que ya están en curso. Para realizar esta función de control de admisión un intermediario de ancho de banda puede sencillamente limitar el volumen total de tráfico que se permite introducir en el dominio sin tener en cuenta los trayectos que habrán de ser atravesados por las llamadas. En este caso, el operador de red puede hacer algunas suposiciones estadísticas acerca de la distribución de llamadas (por ejemplo que es muy poco probable que todas las llamadas converjan en un mismo enlace) a fin de determinar la cantidad de ancho de banda que puede concederse de manera segura. Una solución más prudente sería suponer el peor caso posible, en el que todas las llamadas convergen en el enlace de recursos más limitados y utilizar la capacidad de dicho enlace para el PHB solicitado como el límite de admisión de peticiones de ancho de banda.

Una solución más sofisticada para el control de admisión podría basarse en que el intermediario de ancho de banda dispusiera de cierta información sobre la topología de red y la ruta que seguirá la llamada. El intermediario de ancho de banda podría configurarse con el conocimiento de la topología de red (quizá limitado a la ubicación de los enlaces de recursos más limitados) o podría aprender dinámicamente la topología, por ejemplo percibiendo anuncios de encaminamiento basados en el estado del enlace, complementados con información sobre los recursos. En este caso las peticiones de ancho de banda que se hagan al intermediario deben incluir suficiente información acerca del destino de la llamada para que el intermediario pueda determinar los enlaces de recursos limitados que atravesará la llamada y por consiguiente si la llamada se puede admitir de manera segura.

Al igual que para RSVP compuesto, no es absolutamente necesario que la señalización se efectúe llamada por llamada – un AN podría agregar peticiones de llamadas con destinos similares. Ahora bien, obsérvese que esto haría necesario que el AN dispusiera de alguna información sobre la topología.

Todavía no existe un protocolo normalizado para la comunicación con o entre intermediario de ancho de banda.

9 Control de admisión para múltiples dominios

Se prevé que las distintas redes de dominio IPCablecom dispondrán de sus propias políticas y procedimientos operacionales. Asimismo se prevé que los operadores de red IPCablecom puedan utilizar, para vehicular su tráfico IPCablecom, distintos proveedores de transporte IP, cada uno de los cuales puede emplear diferentes topologías de red. Por lo tanto es difícil suponer que habrá mecanismos QoS compatibles de extremo a extremo para llamadas que atraviesan las redes dorsales de múltiples proveedores. Según se describe en [4], es posible utilizar RSVP de extremo a extremo sin que todos los dominios que intervienen tengan que estar enterados del RSVP. Por ejemplo, un dominio podría utilizar un modelo Diffserv configurado puro, otro podría utilizar agregación de RSVP y otro podría utilizar RSVP por flujo. Cabe observar que no hay ninguna razón para que las reservas RSVP por flujo o compuestas no puedan atravesar fronteras de dominio si dos dominios adyacentes acuerdan atender las peticiones RSVP del otro. En un entorno de este tipo se pueden obtener garantías más fuertes que las que sería posible obtener si algunos dominios no soportan RSVP. Además, el efecto de la agregación sobre la escalabilidad se puede mejorar si las reservas compuestas pueden atravesar fronteras de dominio ya que esto evita la necesidad de desagregar las peticiones RSVP en el encaminador de frontera.

También es posible que los distintos proveedores opten por soluciones tecnológicas muy diferentes para proporcionar QoS en sus redes dorsales. Por ejemplo, un proveedor puede optar por implementar su red dorsal utilizando ATM, y las reservas RSVP (individuales o compuestas) se pueden satisfacer estableciendo circuitos virtuales ATM con características de QoS adecuadas. Otros proveedores pueden utilizar enlaces de la jerarquía digital síncrona para conectar

directamente los encaminadores. Según se ha dicho anteriormente, los proveedores disponen de flexibilidad similar para decidir si utilizan o no MPLS.

10 Utilización de MPLS

NOTA – La información presentada en esta cláusula tiene únicamente carácter informativo.

En la red dorsal se PUEDE utilizar la conmutación por etiquetas multiprotocolo (MPLS) [12], con trayectos conmutados por etiquetas (LSP, *label switched paths*) para representar reservas compuestas o flujos de tráfico compuestos. Esto puede ofrecer las ventajas siguientes:

1) Aptitud para aplicar la ingeniería de tráfico con mayor precisión que cuando no se utiliza MPLS.
2) Mecanismos de restablecimiento en caso de fallos de enlaces y nodos.
3) Encaminamiento de reservas compuestas basado en la limitación de los recursos.
4) Encaminamiento compatible de mensajes y datos de control compuestos.

La primera ventaja es común a todos los métodos descritos en las cláusulas anteriores. Por ingeniería de tráfico se entiende la aptitud para controlar los trayectos seguidos por los flujos de tráfico compuestos, con el objetivo general de evitar la sobreutilización o subutilización de los enlaces. La ingeniería de tráfico MPLS y sus beneficios se describen en [11].

Según se describe en [15], MPLS también proporciona dispositivos de protección contra fallos de enlaces o nodos en una red. Por ejemplo, se pueden establecer previamente trayectos de respaldo para contornear un enlace o nodo, y protegerlo así contra fallos. Mediante el encaminamiento de paquetes hacia un LSP de respaldo desde un nodo hacia el origen respecto al punto de fallo, es posible evitar el retardo relacionado con la espera hasta que se produzca la reconvergencia del encaminamiento IP después de un fallo. Por consiguiente, se puede reducir considerablemente el periodo de tiempo durante el cual se interrumpe el reenvío de paquetes debido a un fallo del enlace, un fallo del nodo, o la pérdida de paquetes producida por un encaminamiento incompatible.

El encaminamiento de reservas compuestas basado en la limitación de los recursos permite que se seleccionen trayectos sobre la base de su aptitud para cumplir con las restricciones, en particular la disponibilidad de ancho de banda suficiente para dar cabida a una determinada petición de reserva, según se describe en [11]. Normalmente esto permite el establecimiento de más reservas de las que sería posible establecer si todas las peticiones de reserva siguieran el trayecto más corto, según lo determinado por el encaminamiento IP convencional.

La cuarta ventaja, según se explica en [5], se obtiene principalmente cuando el tráfico se divide entre trayectos de igual coste, lo que presenta el riesgo de que un mensaje PATH compuesto siga un trayecto mientras que los datos que requieren una reserva sigan otro. Este problema se evita si los datos son "tunelizados" desde el ingreso hasta el egreso. MPLS proporciona una tecnología de tunelización adecuada.

Otra ventaja de la MPLS es que se puede desplegar gradualmente nodo por nodo, mediante actualizaciones del soporte lógico. Es ventajoso que los mecanismos de encaminamiento y de QoS existentes se puedan preservar y soportar durante la implantación de MPLS por fases.

La decisión de utilizar MPLS en cualquier dominio puede tomarse independientemente de los otros dominios y depende de si el proveedor necesita o desea tratar los tres asuntos enumerados anteriormente.

Obsérvese que se puede utilizar MPLS con cualquiera de los métodos descritos en las cláusulas 7 y 8. En una red dorsal Diffserv pura (sin señalización) las principales ventajas se reflejarían en la ingeniería de tráfico y el reencaminamiento rápido. El encaminamiento de reservas basado en la limitación de los recursos es útil para los métodos descritos en 8.1 y 8.2, mientras que el

encaminamiento compatible de mensajes de control y de datos sólo es importante para el RSVP compuesto (véase 8.2).

11 Puesta en cola y filtrado

11.1 Puesta en cola

La calidad de la voz por redes IPCablecom sólo puede verse afectada por limitaciones de ancho de banda. La latencia, fluctuación de fase y pérdida de paquetes son también parámetros de transmisión que necesitan observarse. La principal manera de reducir el retardo y la fluctuación de fase es mediante una gestión adecuada de las colas en los encaminadores. Como tal, la elección de las tecnologías de puesta en cola puede resultar tan importante como la elección de los mecanismos QoS tales como Diffserv, RSVP por flujo y RSVP compuesto que se utilice. Métodos de puesta en cola cuidadosamente elegidos y adecuadamente configurados permiten obtener una baja fluctuación de fase y una baja latencia para el tráfico especificado.

La puesta en cola atendiendo a la prioridad (PQ, *priority queuing*), por ejemplo, puede dar al tráfico de medios IPCablecom un nivel de prioridad más alto que al de otros tipos de tráfico. La atribución de niveles de prioridad hace posible que otros paquetes, además de los del tráfico de medios IPCablecom, utilicen la cola siempre y cuando se mantenga la QoS para el tráfico IPCablecom. No obstante, si se utiliza PQ se ha de garantizar un tratamiento justo del tráfico de baja prioridad.

La puesta en cola justa ponderada (WFQ, *weighted fair queuing*) puede distribuir el ancho de banda disponible equitativamente entre los flujos de tráfico. Incluso en situaciones de congestión, se mantiene un caudal constante. Sin embargo, como este método no puede dar una prioridad absoluta al tráfico de medios IPCablecom, se puede prever que se producirá degradación de la calidad en los encaminadores congestionados.

También pueden implementarse otros métodos que generen colas dinámicamente o utilicen muchas colas. La posibilidad de aplicación de estos métodos a IPCablecom se ha de examinar teniendo en cuenta su aptitud para mantener la QoS específica para el tráfico de medios. A menudo también se necesita una configuración cuidadosa del método de puesta en cola.

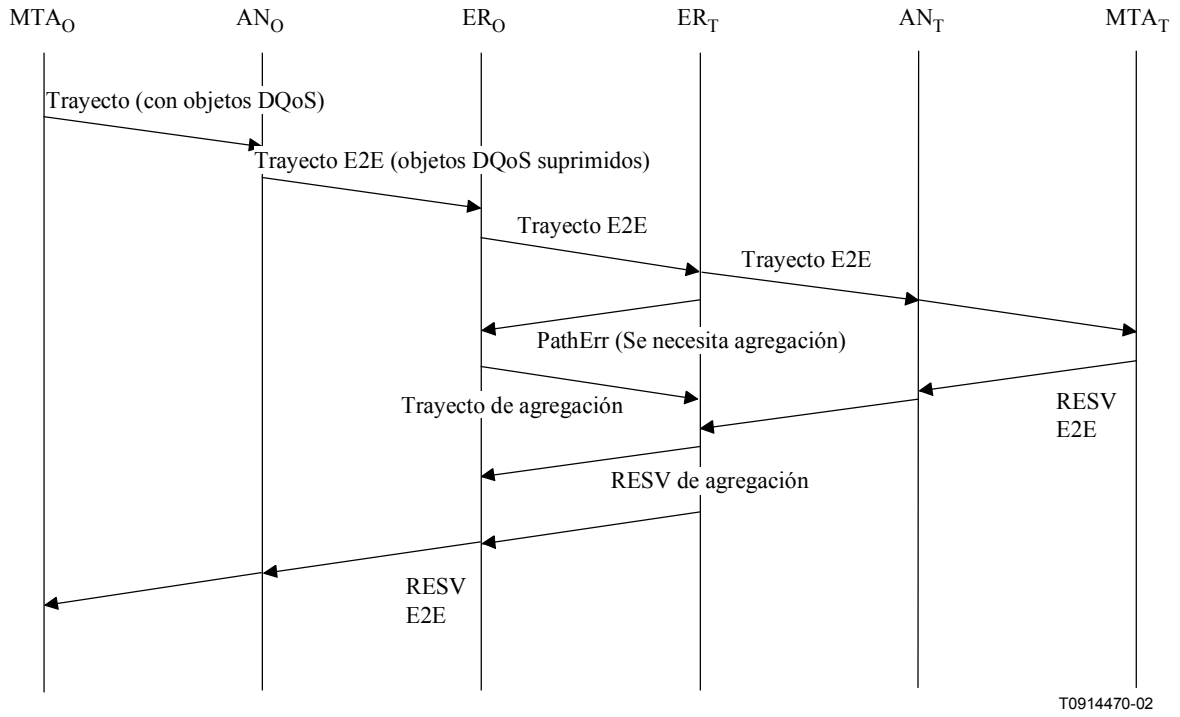
11.2 Filtrado

Por razones de seguridad de la red algunos encaminadores utilizan funciones de filtrado para limitar el tráfico. Las funciones de filtrado pueden consumir recursos, tales como potencia de la CPU y memoria, lo que puede afectar a la calidad de funcionamiento del encaminador y, en consecuencia, provocar la degradación de parámetros de QoS tales como la pérdida de paquetes, fluctuación de fase y latencia. Los encaminadores que utilicen el filtrado de paquetes deberían disponer de recursos suficientes para tratar todo el tráfico que puedan encontrar.

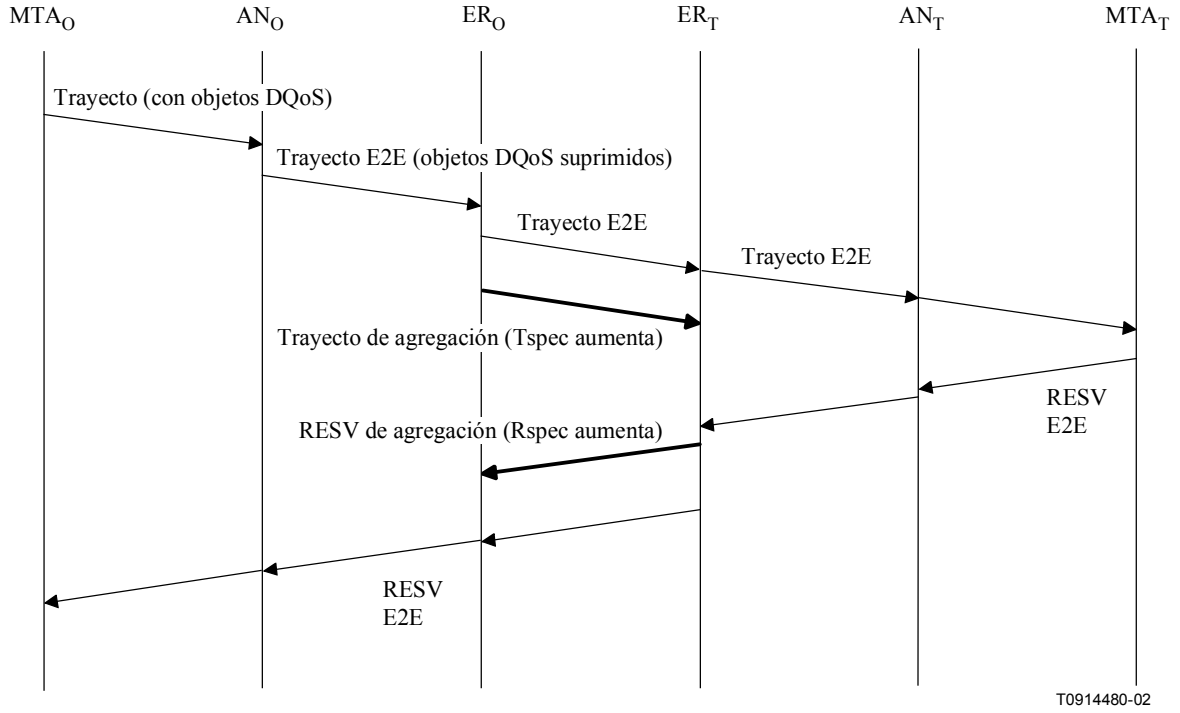
Apéndice I

Ejemplos de flujo de llamada

En los ejemplos, los dos MTA utilizan señalización RSVP con DQoS; y los ER realizan la agregación RSVP. Por razones de claridad sólo se muestra el intercambio de mensajes unidireccionales.



El siguiente ejemplo muestra el aumento del tamaño de una reserva compuesta existente en respuesta a una nueva reserva E2E.



Apéndice II

Bibliografía

[1] Recomendación UIT-T Y.1541 (2002), *Objetivos de la calidad de funcionamiento de la red para servicios basados en IP*.

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

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

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

[5] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

[6] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[7] IETF RFC 2747 (2000), *RSVP Cryptographic Authentication*.

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

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

[10] AWDUCHE [D.] et al.: Extensions to RSVP for LSP Tunnels, *draft-ietf-mpls-rsvp-Lsp-tunnel-09.txt*, agosto 2001.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2002