Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.323

(06/2006)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIA

Infraestructura de los servicios audiovisuales – Sistemas y equipos terminales para los servicios audiovisuales

Sistemas de comunicación multimedia basados en paquetes

Recomendación UIT-T H.323

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIA

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	H.230–H.239
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
Sistemas y equipos terminales para los servicios audiovisuales	**H.300–H.349**
Arquitectura de servicios de directorio para servicios audiovisuales y multimedia	H.350–H.359
Arquitectura de la calidad de servicio para servicios audiovisuales y multimedia	H.360–H.369
Servicios suplementarios para multimedia	H.450–H.499
PROCEDIMIENTOS DE MOVILIDAD Y DE COLABORACIÓN	
Visión de conjunto de la movilidad y de la colaboración, definiciones, protocolos y procedimientos	H.500–H.509
Movilidad para los sistemas y servicios multimedia de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedia	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedia	H.530–H.539
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedia	H.540–H.549
Procedimientos de interfuncionamiento de la movilidad	H.550–H.559
Procedimientos de interfuncionamiento de colaboración en móviles multimedia	H.560–H.569
SERVICIOS DE BANDA ANCHA Y DE TRÍADA MULTIMEDIA	
Servicios multimedia de banda ancha sobre VDSL	H.610–H.619

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

Recomendación UIT-T H.323

Sistemas de comunicación multimedia basados en paquetes

Resumen

La presente Recomendación describe terminales y otras entidades que proporcionan servicios de comunicaciones multimedia por redes por paquetes (PBN) que pueden no proporcionar una calidad de servicio garantizada. Las entidades H.323 pueden proporcionar comunicaciones de audio, vídeo y/o datos en tiempo real. El soporte del audio es obligatorio, mientras que el de datos y vídeo es opcional, pero si se soportan es necesario poder utilizar un modo de funcionamiento común especificado, para que puedan interfuncionar todos los terminales que soporten ese tipo de medios.

La red por paquetes por la cual se comunican las entidades H.323, puede ser una conexión punto a punto, un segmento de red único o una interred que tenga múltiples sistemas con topologías complejas.

Las entidades H.323 pueden utilizarse en configuraciones punto a punto, multipunto o de difusión (descritas en la Rec. UIT-T H.332). Pueden interfuncionar con terminales H.310 por la RDSI-BA, con terminales H.320 por la RDSI-BE, con terminales H.321 por la RDSI-BA, con terminales H.322 en redes LAN de calidad de servicio garantizada, con terminales H.324 por la RTGC y redes inalámbricas, con terminales V.70 por la RTGC, y con terminales vocales por la RTGC o por la RDSI utilizando pasarelas.

Las entidades H.323 pueden estar integradas en computadores personales o implementadas en dispositivos autónomos como son los videoteléfonos.

Ténganse en cuenta que el título de H.323 (1996) "Sistemas y equipos videotelefónicos para redes de área local que proporcionan una calidad de servicio no garantizada" se cambió en la versión 2 por coherencia con la ampliación de su alcance.

Los productos que aleguen conformidad con la versión 1 de H.323 cumplirán todos los requisitos obligatorios de H.323 (1996), que hace referencia a las Recs. UIT-T H.225.0 (1996) y H.245 (1997). Los productos de la versión 1 se identificarán por mensajes H.225.0 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 1} y por mensajes H.245 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) 2}.

Los productos que aleguen conformidad con la versión 2 de H.323 cumplirán todos los requisitos obligatorios de esta Recomendación, H.323 (1998), que hace referencia a las Recs. UIT-T H.225.0 (1998) y H.245 (1998 o posterior). Los productos de la versión 2 se identificarán por mensajes H.225.0 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 2} y por mensajes H.245 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, donde "x" es 3 o superior.

Los productos que aleguen conformidad con la versión 3 de H.323 cumplirán todos los requisitos obligatorios de esta Recomendación, H.323 (1999), que hace referencia a las Recs. UIT-T H.225.0 (1999) y H.245 (1999 o posterior). Los productos de la versión 3 se identificarán por mensajes H.225.0 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 3} y por mensajes H.245 con **protocolIdentifier** = {itu-t (0) recommendation (0) h(8) 245 version (0) x}, donde "x" es 5 o superior.

Los productos que alegan conformidad con la versión 4 de H.323 cumplirán todos los requisitos obligatorios de esta Recomendación, H.323 (2000), que hace referencia a las

Recs. UIT-T H.225.0 (2000) y H.245 (2000 o posterior). Los productos de la versión 4 se identificarán por mensajes H.225.0 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 4} y por mensajes H.245 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, donde "x" es 7 o superior.

Los productos que aleguen conformidad con la versión 5 de H.323 cumplirán todos los requisitos obligatorios de esta Recomendación, H.323 (2003), que hace referencia a las Recs UIT-T H.225.0 (2003) y H.245 (02/2003 o posterior). Los productos de la versión 5 se identificarán por mensajes H.225.0 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 5} y por mensajes H.245 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, donde "x" es 9 o superior.

Los productos que aleguen conformidad con la versión 6 de H.323 cumplirán todos los requisitos obligatorios de esta Recomendación, H.323 (2006), que hace referencia a las Recs. UIT-T H.225.0 (2006) y H.245 (05/2006 o posterior). Los productos de la versión 6 se identificarán por mensajes H.225.0 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 6} y por mensajes H.245 con **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, donde "x" es 13 o superior.

En esta versión de la Rec. UIT-T H.323 (2003) se integran los cambios aprobados en la Enmienda 1 (01/2005) "*Anexo D revisado*" y la Enmienda 2 (01/2005) "*Nuevo anexo M4*".

Orígenes

La Recomendación UIT-T H.323 fue aprobada el 13 de junio de 2006 por la Comisión de Estudio 16 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT 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 en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T H.323

Sistemas de comunicación multimedia basados en paquetes

1 Alcance

La presente Recomendación expone los requisitos técnicos de los sistemas de comunicaciones multimedia en aquellas situaciones en las que la red de transporte subyacente es una red por paquetes (PBN, *packet based network*) que no puede garantizar una calidad de servicio (QoS, *quality of service*) determinada. Estas redes por paquetes pueden ser redes de área local, redes de área empresarial, redes de área metropolitana, intrarredes e interredes (incluida la Internet). También pueden ser conexiones obtenidas por marcación y conexiones punto a punto por la RTGC o por la RDSI, que utilicen transporte subyacente por paquetes tal como el protocolo punto a punto (PPP, *point-to-point protocol*). Estas redes pueden constar de un único segmento de red, o tener topologías complejas que incorporen muchos segmentos de red interconectados por otros enlaces de comunicaciones.

La presente Recomendación describe los componentes de un sistema H.323, entre ellos las pasarelas, controladores de acceso, controladores multipunto, procesadores multipunto y unidades de control multipunto. Los procedimientos y mensajes de control de esta Recomendación definen cómo se comunican estos componentes. La cláusula 6 contiene descripciones detalladas de los mismos.

Los terminales H.323 proporcionan capacidad de comunicaciones de audio y opcionalmente de vídeo y datos en conferencias punto a punto o multipunto. El interfuncionamiento con otros terminales de la serie H, terminales vocales de la RTGC o la RDSI, o terminales de datos de la RTGC o la RDSI se realiza mediante pasarelas; véase la figura 1. Los controladores de acceso proporcionan servicios de control de admisión y de traducción de dirección. Los controladores multipunto, los procesadores multipunto y las unidades de control multipunto dan soporte a las conferencias multipunto.

No son materia de la presente Recomendación la interfaz de red, la red física ni el protocolo de transporte utilizado en la red. Entre estas redes se encuentran, por ejemplo, las siguientes:

– Ethernet (IEEE 802.3).
– Fast Ethernet (IEEE 802.3u).
– FDDI.
– Token Ring (IEEE 802.5).
– ATM.

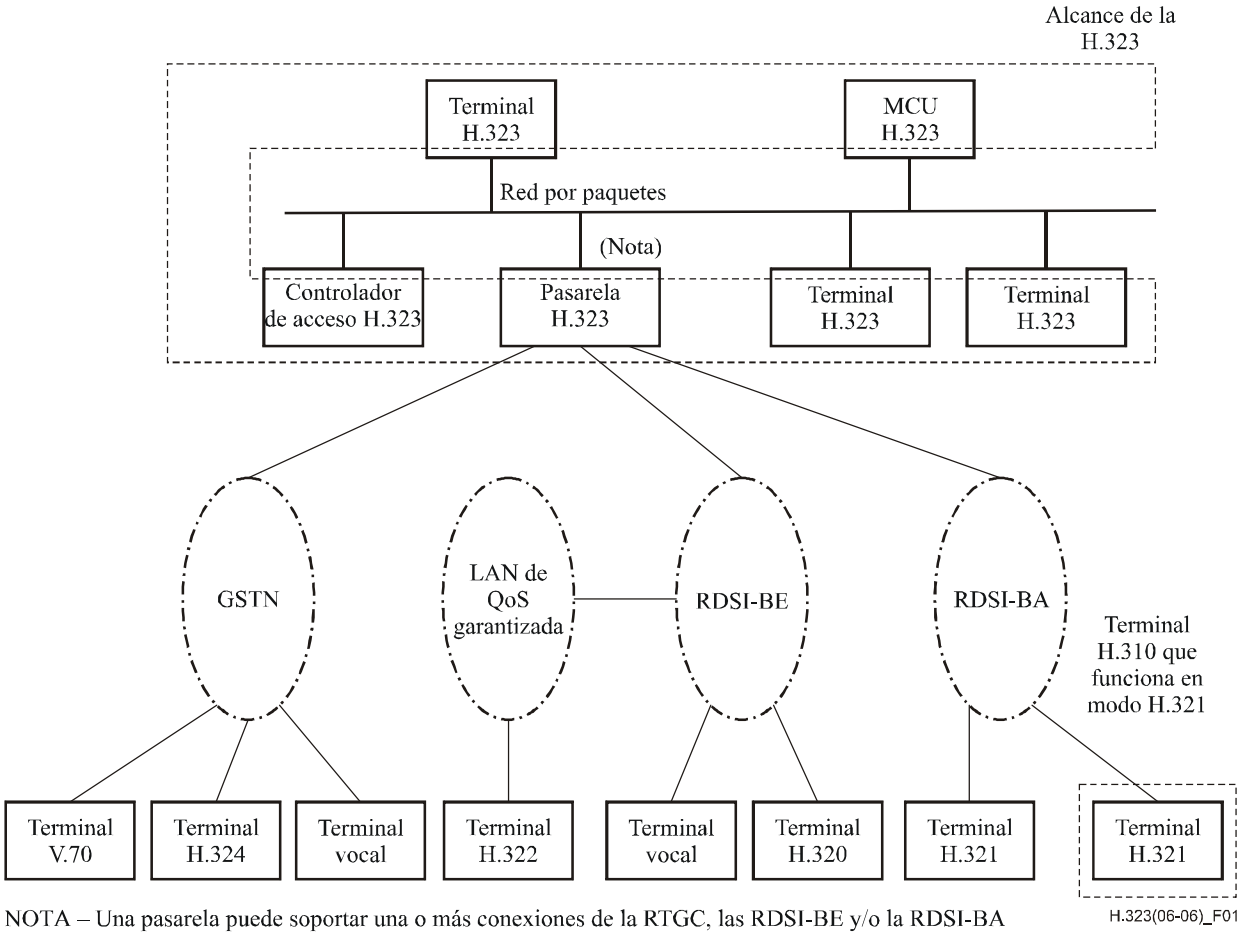


Figura 1/H.323 – Interfuncionamiento de terminales H.323

2 Referencias normativas

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

[1] Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes*.

[2] Recomendación UIT-T H.245 (2006), *Protocolo de control para comunicación multimedia*.

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

[4] Recomendación UIT-T G.722 (1988), *Codificación de audio de 7 kHz dentro de 64 kbit/s*.

[5] Recomendación UIT-T G.723.1 (2006), *Códec de voz de doble velocidad para la transmisión en comunicaciones multimedia a 5,3 y 6,3 kbit/s*.

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

[7] Recomendación UIT-T G.729 (1996), *Codificación de la voz a 8 kbit/s mediante predicción lineal con excitación por código algebraico de estructura conjugada*.

[8] Recomendación UIT-T H.261 (1993), *Códec vídeo para servicios audiovisuales a p ×64 kbit/s*.

[9] Recomendación UIT-T H.263 (2005), *Codificación de vídeo para comunicación a baja velocidad binaria*.

[10] Recomendación UIT-T T.120 (1996), *Protocolo de datos para conferencias multimedia*.

[11] Recomendación UIT-T H.320 (2004), *Sistemas y equipos terminales videotelefónicos de banda estrecha*.

[12] Recomendación UIT-T H.321 (1998), *Adaptación de los terminales videotelefónicos H.320 a entornos de la red digital de servicios integrados de banda ancha (RDSI-BA)*.

[13] Recomendación UIT-T H.322 (1996), *Sistemas y equipos terminales videotelefónicos para redes de área local que proporcionan una calidad de servicio garantizada*.

[14] Recomendación UIT-T H.324 (2005), *Terminal para comunicación multimedia a baja velocidad binaria*.

[15] Recomendación UIT-T H.310 (1998), *Sistemas y terminales para comunicaciones audiovisuales de banda ancha*.

[16] Recomendación UIT-T Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de la llamada básica*.

[17] Recomendación UIT-T Q.932 (1998), *Sistema de señalización digital de abonado N.° 1 – Procedimientos genéricos para el control de los servicios suplementarios de RDSI*.

[18] Recomendación UIT-T Q.950 (2000), *Protocolos de servicios suplementarios, estructura y principios generales*.

[19] ISO/CEI 10646:2003, *Information technology – Universal Multiple-Octet Coded Character Set (USC)*.

[20] Recomendación UIT-T E.164 (2005), *Plan internacional de numeración de telecomunicaciones públicas*.

[21] Recomendación UIT-T H.246 (2006), *Interfuncionamiento de terminales multimedia de la serie H con terminales multimedia de la serie H y terminales de voz/de banda vocal por la RTGC, RDSI y la RMTP*.

[22] Recomendación UIT-T H.235.0 (2005), *Marco de seguridad H.323: Marco de seguridad para sistemas multimedia de la serie H (H.323 y otros basados en H.245)*.

[23] Recomendación UIT-T H.332 (1998), *Recomendación H.323 ampliada para conferencias de bajo grado de acoplamiento*.

[24] Recomendación UIT-T H.450.1 (1998), *Protocolo funcional genérico para el soporte de servicios suplementarios de la Recomendación H.323*.

[25] Recomendación UIT-T I.363.5 (1996), *Especificación de la capa de adaptación del modo de transferencia asíncrono de la RDSI-BA: Capa de adaptación del modo transferencia asíncrono tipo 5*.

[26] Recomendación UIT-T Q.2931 (1995), *Sistema de señalización digital de abonado N.° 2 – Especificación de la capa 3 de la interfaz usuario-red para el control de llamada/conexión básica*.

[27] Recomendación UIT-T I.356 (2000), *Calidad de funcionamiento en la transferencia de células en la capa de modo de transferencia asíncrono de la red digital de servicios integrados de la RDSI-BA*.

[28] Recomendación UIT-T I.371 (2004), *Control de tráfico y control de congestión en RDSI-BA*.

[29] Recomendación UIT-T Q.2961.2 (1997), *Sistema de señalización digital de abonado N.° 2 – Parámetros de tráfico adicionales: Soporte de la capacidad de transferencia del modo de transferencia asíncrono en el elemento información de capacidad portadora de banda ancha*.

[30] Recomendación UIT-T H.282 (1999), *Protocolo de control de dispositivo distante para aplicaciones multimedia*.

[31] Recomendación UIT-T H.283 (1999), *Transporte por canal lógico del control de dispositivo distante*.

[32] ATM Forum, AF-SAA-0124.000 (1999), *H.323 Media Transport Over ATM*.

[33] Recomendación UIT-T Q.2941.2 (1999), *Sistema de señalización digital de abonado N.º 2 – Extensiones del transporte de identificadores genéricos*.

[34] Recomendación UIT-T H.450.2 (1998), *Servicio suplementario de transferencia de llamada para la Recomendación H.323*.

[35] Recomendación UIT-T H.450.4 (1999), *Servicio suplementario retención de llamada para la Recomendación H.323*.

[36] Recomendación UIT-T H.248.1 (2005), *Protocolo de control de las pasarelas: Versión 3*.

[37] ISO/CEI 11571:1998, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Networks – Addressing*.

[38] Familia de Recomendaciones UIT-T Q.951.x, *Descripción de la etapa 3 para los servicios suplementarios de identificación de número que utilizan el sistema de señalización digital de abonado N.º 1*.

[39] Recomendación UIT-T H.450.3 (1998), *Servicio suplementario de desviación de llamada para la Recomendación H.323*.

[40] Recomendación UIT-T H.450.5 (1999), *Servicios suplementarios depósito de llamada y extracción de llamada para la Recomendación H.323*.

[41] Recomendación UIT-T H.450.6 (1999), *Servicio suplementario llamada en espera para la Recomendación H.323*.

[42] Recomendación UIT-T H.450.7 (1999), *Servicio suplementario de indicación de mensaje en espera para la Recomendación H.323*.

[43] Recomendación UIT-T H.450.8 (2000), *Servicio suplementario de identificación de nombres para la Recomendación H.323*.

[44] ISO/CEI 11572:2000, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Circuit mode bearer services – Inter-exchange signalling procedures and protocol*.

[45] Recomendación UIT-T H.222.0 (2006), *Tecnología de la información – Codificación genérica de imágenes en movimiento e información de audio asociada: Sistemas*.

[46] Recomendación UIT-T H.223 (2001), *Protocolo de multiplexación para comunicación multimedia a baja velocidad binaria*.

[47] IETF RFC 2068 (1997), *Hypertext Transfer Protocol – HTTP/1.1*.

[48] IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*.

[49] Recomendación UIT-T Z.100 (2002), *Lenguaje de especificación y descripción*.

[50] IETF RFC 1738 (1994), *Uniform Resource Locators (URL)*.

[51] IETF RFC 2234 (1997), *Augmented BNF for Syntax Specifications: ABNF*.

[52] ISO 4217:2001, *Codes for the representation of currencies and funds*.

[53] Recomendación UIT-T V.21 (1988), *Módem dúplex a 300 bit/s normalizado para uso en la red telefónica general con conmutación*.

[54] Recomendación UIT-T T.30 (2005), *Procedimientos de transmisión de documentos por facsímil por la red telefónica general conmutada*.

[55] Recomendación UIT-T T.38 (2005), *Procedimientos para la comunicación facsímil en tiempo real entre terminales facsímil del grupo 3 por redes con protocolo Internet*.

[56] IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

[57] Recomendación UIT-T H.264 (2005), *Codificación de vídeo avanzada para los servicios audiovisuales genéricos.*

[58] Recomendación UIT-T H.241 (2006), *Señales de control y procedimientos de vídeo extendidos para terminales de la serie H.300.*

3 Definiciones

A los efectos de la presente Recomendación se aplican las definiciones que aparecen en la cláusula 3/H.225.0 [1] y en la cláusula 3/H.245 [2] junto con las que figuran en esta cláusula. Estas definiciones son aplicables solamente en el lado de la red por paquetes. Otros términos pueden ser apropiados cuando se haga referencia al lado red con conmutación de circuitos (RCC). Véase la cláusula 5, Convenios, información sobre el uso de los términos en la presente Recomendación.

3.1 pasarela de acceso: Pasarela que conecta dos redes (por ejemplo, una red SS7 a una red QSIG) y que realiza algunas funciones de interfuncionamiento entre ambas redes.

3.2 controlador multipunto (MC) activo: Controlador multipunto que ha ganado el procedimiento de determinación principal-subordinado y está en esos momentos proporcionando la función de control multipunto para la conferencia.

3.3 conferencia multipunto ad hoc: Conferencia ad hoc que empezó siendo punto a punto y que, en algún momento de la comunicación, se amplió a conferencia multipunto. Esto es posible si uno o más terminales de la conferencia punto a punto inicial contienen un MC, si la comunicación se establece utilizando un controlador de acceso que incluye la funcionalidad MC, o si la llamada inicial se efectúa a través de una unidad de control multipunto MCU como llamada multipunto entre dos terminales solamente.

3.4 direccionable: Una entidad H.323 de la red que tiene una dirección de transporte es direccionable, que no es lo mismo que ser llamable. Un terminal, una pasarela y una MCU son direccionables y llamables. Un controlador de acceso es direccionable pero no llamable. Un MC y un MP no son llamables ni direccionables pero están contenidos dentro de un punto extremo o un controlador de acceso que sí lo son. En una pasarela compuesta, el MGC y la MG son direccionables, pero solo el MGC es llamable.

3.5 bloqueo de audio; enmudecimiento de audio: Supresión de la señal de audio de una fuente o de todas. Bloqueo de emisión significa que el originador de un tren de audio bloquea su micrófono y/o no transmite ninguna señal de audio. Bloqueo de recepción significa que el terminal receptor hace caso omiso de un determinado tren de audio entrante o bloquea su altavoz.

3.6 conferencia por difusión: Conferencia en la que hay un transmisor de trenes de medios y muchos receptores. No hay transmisión bidireccional de trenes de control o de medios. Estas conferencias se deben implementar utilizando facilidades de multidifusión de transporte de red, si se dispone de ellas. Véase también la Rec. UIT-T H.332 [23].

3.7 conferencia de panel con difusión: Combinación de conferencia multipunto y conferencia con difusión. En esta conferencia algunos terminales participan en una conferencia multipunto mientras que otros muchos terminales sólo reciben los trenes de medios. Hay transmisión bidireccional entre los terminales en la porción multipunto de la conferencia pero no hay transmisión bidireccional entre ellos y los terminales en escucha. Véase también la Rec. UIT-T H.332.

3.8 llamada: Comunicación multimedia punto a punto entre dos puntos extremos H.323. La llamada empieza con el procedimiento de establecimiento de la comunicación y termina con el procedimiento de terminación de la llamada. La llamada está formada por el conjunto de canales fiables y no fiables entre los puntos extremos. Una llamada puede producirse directamente entre dos puntos extremos o puede implicar a otras entidades H.323 tales como un controlador de acceso o un MC. En caso de interfuncionamiento con algunos puntos extremos de redes con conmutación de circuitos (RCC) a través de una pasarela, todos los canales terminan en la pasarela donde se convierten en la representación apropiada para el sistema de extremo de la RCC. Normalmente una llamada se efectúa entre dos usuarios con fines de comunicación, pero puede haber llamadas que sólo sean de señalización. Un punto extremo puede ser capaz de soportar varias llamadas simultáneas.

3.9 canal de señalización de llamada: Canal fiable utilizado para llevar los mensajes de establecimiento de la comunicación y de liberación de la llamada (según la Rec. UIT-T H.225.0) entre dos entidades H.323.

3.10 llamable: Capaz de ser llamado, como se describe en la cláusula 8 o en los servicios suplementarios Recs. UIT-T (H.450.x). En otras palabras, una entidad H.323 es considerada llamable en general si un usuario especificase la entidad como un destino. Son llamables los terminales, las MCU, las pasarelas y los MGC, pero no lo son los controladores de acceso, los MC ni los MG.

3.11 conferencia multipunto centralizada: Conferencia en la que todos los terminales participantes comunican punto a punto con una MCU. Los terminales transmiten sus trenes de control, audio, vídeo y/o datos a la MCU. El MC de la MCU gestiona de manera centralizada la conferencia. El MP de la MCU procesa los trenes de audio, vídeo y/o datos y devuelve los trenes procesados a cada terminal.

3.12 pasarela compuesta: Pasarela que no separa las funciones de controlador de pasarela de medios y de pasarela de medios.

3.13 control e indicación: Señalización de extremo a extremo entre terminales compuesta por un control que produce un cambio de estado en el receptor y una indicación que facilita información sobre el estado o el funcionamiento del sistema (véase también la Rec. UIT-T H.245 [2] para más información, en la que figuran las abreviaturas).

3.14 datos: Tren de información distinto del de audio, vídeo y control, transportado por el canal de datos lógico (véase la Rec. UIT-T H.225.0 [1]).

3.15 conferencia multipunto descentralizada: Conferencia en la que cada terminal participante multidifunde su información de audio y vídeo a los demás participantes sin utilizar una MCU. Los terminales se encargan de:

a) agregar los trenes de audio recibidos; y

b) seleccionar uno o más de los trenes de vídeo recibidos para su visualización.

En este caso no se necesita MP de audio o vídeo. Los terminales se comunican por sus canales de control H.245 con un MC que gestiona la conferencia. El tren de datos sigue siendo procesado de manera centralizada por la MCU del MCS que puede estar dentro de un MP.

3.16 pasarela descompuesta: Pasarela que está funcionalmente dividida en un controlador de pasarela de medios y una o más pasarelas de medios.

3.17 punto extremo: Terminal H.323, pasarela o MCU. Un punto extremo puede llamar y ser llamado. Genera y/o termina trenes de información.

3.18 controlador de acceso: Entidad H.323 de la red que facilita la traducción de direcciones y controla el acceso a la red de los terminales H.323, pasarelas y MCU. El controlador de acceso puede prestar también otros servicios a los terminales, pasarelas y MCU, tales como la gestión de anchura de banda y la localización de pasarelas.

3.19 pasarela: Una pasarela H.323 es un punto extremo de la red que proporciona comunicaciones en ambos sentidos en tiempo real entre terminales H.323 de la red por paquetes y otros terminales UIT en una red con conmutación de circuitos, o con otra pasarela H.323. Otros terminales UIT son, por ejemplo, aquellos que cumplen las Recs. UIT-T H.310 (H.320 sobre RDSI-BA), H.320 (RDSI), H.321 (ATM), H.322 (LAN con GQoS), H.324 (RTGC), H.324M (Móviles) y V.70 (Señales vocales y datos simultáneos digitales).

3.20 entidad H.323: Cualquier componente H.323, incluidos terminales, pasarelas, controladores de acceso, MC, MP y MCU.

3.21 canal de control H.245: Canal fiable utilizado para transportar mensajes de información de control H.245 (según la Rec. UIT-T H.245) entre dos puntos extremos H.323.

3.22 sesión H.245: Parte de la llamada que comienza con el establecimiento de un canal de control H.245 y termina con la recepción de la **instrucción finalizar sesión** H.245 o bien la terminación se debe a un fallo. No debe confundirse con una llamada, que está delimitada por los mensajes Establecimiento y Liberación completados H.225.0.

3.23 conferencia multipunto híbrida – audio centralizado: Una conferencia en la que los terminales multidifunden su vídeo a otros terminales participantes y unidifunden su audio al MP para su mezcla. El MP devuelve un tren de audio mezclado a cada terminal.

3.24 conferencia multipunto híbrida – vídeo centralizado: Una conferencia en la que los terminales multidifunden su audio a otros terminales participantes y unidifunden su vídeo al MP para su conmutación o mezcla. El MP devuelve un tren de vídeo a cada terminal.

3.25 tren de información: Flujo de información de un tipo específico de medios (por ejemplo, audio) de una sola fuente a uno o más destinos.

3.26 sincronización con el movimiento de los labios: Operación cuyo fin es dar la sensación de que el movimiento de los labios de la persona visualizada está sincronizado con su discurso.

3.27 red de área local (LAN, *local area network*): Medio compartido o conmutado, red de comunicaciones entre pares que difunde información para que la reciban todas las estaciones de una zona geográfica de tamaño moderado, tal como un solo edificio de oficinas o un campus. La red suele ser propiedad de una sola organización que la utiliza y explota. En el contexto de la presente Recomendación, las LAN incluyen también las interredes formadas por varias LAN que se interconectan mediante puentes o encaminadores.

3.28 canal lógico: Canal utilizado para transportar trenes de información entre dos puntos extremos H.323. Estos canales se establecen siguiendo los procedimientos de **apertura de canal lógico** H.245. Se utiliza un canal no fiable para trenes de información de audio, de control de audio, de vídeo y de control de vídeo. Se utiliza un canal fiable para trenes de datos y de información de control H.245. No hay relación alguna entre un canal lógico y un canal físico.

3.29 pasarela de medios: Pasarela que convierte los medios que se proporcionan en un tipo de red al formato requerido en otro tipo de red. Por ejemplo, una pasarela de medios (MG) puede terminar canales portadores de una red con conmutación de circuitos (es decir, circuitos DS0) y trenes de medios de una red de paquetes (por ejemplo, trenes RTP en una red IP). Esta pasarela puede procesar audio, vídeo y T.120, solos o en cualquier combinación posible, y asimismo puede realizar la traducción de medios dúplex. La MG puede también reproducir mensajes de audio/vídeo y realizar otras funciones IVR o realizar la conferencia de medios.

3.30 controlador de pasarela de medios: Controla las partes del estado de la llamada relativas al control de la conexión para canales de medios en una MG.

3.31 conferencia multipunto mixta: Es aquella en la que algunos terminales (D, E y F, en la figura 2) participan de un modo centralizado mientras que otros (A, B y C) participan de un modo descentralizado. Los terminales ignoran que la conferencia es mixta; sólo conocen el tipo de conferencia en la que cada uno de ellos participa. La MCU proporciona el puente entre los dos tipos de conferencia.

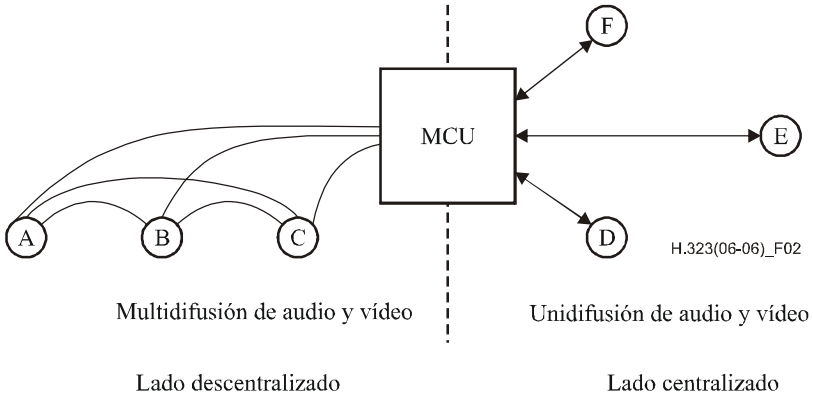


Figura 2/H.323 – Conferencia multipunto mixta

3.32 multidifusión: Proceso de transmisión de unidades de datos de protocolo (PDU) de una fuente a múltiples destinos. El mecanismo efectivamente utilizado (a saber, multidifusión de IP, multiunidifusión, etc.) en este proceso puede ser diferente según las diferentes tecnologías de red.

3.33 conferencia multipunto: Una conferencia multipunto es una conferencia entre tres o más terminales. Los terminales pueden estar en la red o en la RCC. La conferencia multipunto deberá ser controlada siempre por un MC. En esta subcláusula se definen diversos tipos de conferencia multipunto, si bien todos ellos requieren un solo MC por conferencia. Pueden implicar además una o más MCU H.231 en la RCC. Un terminal de la red puede participar también en una conferencia multipunto de RCC conectándose a través de una pasarela con una MCU de la RCC. Para ello no es necesario utilizar un MC.

3.34 unidad de control multipunto: La unidad de control multipunto (MCU) es un punto extremo de la red que permite que tres o más terminales y pasarelas participen en una conferencia multipunto. También puede conectar dos terminales en una conferencia punto a punto que puede llegar a convertirse en multipunto. La MCU funciona por lo general como una MCU H.231, aunque no es obligatorio el procesador de audio. La MCU consta de dos partes: un controlador multipunto obligatorio y procesadores multipunto opcionales. En el caso más sencillo, una MCU puede estar

constituida solamente por un MC, sin procesadores multipunto. Una MCU puede también ser incluida en una conferencia por el controlador de acceso sin ser explícitamente llamada por ninguno de los puntos extremos.

3.35 controlador multipunto: El controlador multipunto (MC) es una entidad H.323 de la red que permite controlar tres o más terminales que participen en una conferencia multipunto. También puede conectar dos terminales en una conferencia punto a punto que puede llegar a convertirse en multipunto. El MC proporciona la capacidad de negociación con todos los terminales para conseguir niveles comunes de comunicación. También puede controlar recursos de conferencia, por ejemplo quién multidifunde vídeo. El MC no efectúa el mezclado ni la conmutación de audio, vídeo ni datos.

3.36 procesador multipunto: El procesador multipunto (MP) es una entidad H.323 de la red que permite el procesamiento centralizado de los trenes de audio, vídeo y/o datos en una conferencia multipunto. El MP proporciona el mezclado, la conmutación u otro tipo de procesamiento de los trenes de medios bajo control del MC. El MP puede procesar un solo tren de medios o varios, dependiendo del tipo de conferencia soportada.

3.37 multi-unidifusión: Procedimiento de transferencia de unidades de datos de protocolo en el que un punto extremo envía más de una copia de un tren de medios, pero lo hace a diferentes puntos extremos. Esto puede ser necesario en redes que no soporten la multidifusión.

3.38 dirección de red: Dirección de capa de red de una entidad H.323 definida por el protocolo de capa de red (entre redes) en uso (por ejemplo, una dirección IP). Esta dirección se hace corresponder con la dirección de capa 1 del sistema respectivo por algún medio definido en el protocolo de interconexión de redes.

3.39 red por paquetes (también red): Cualquier medio compartido, conmutado o punto a punto que proporcione comunicaciones entre pares entre dos o más puntos extremos utilizando un protocolo de transporte por paquetes.

3.40 conferencia punto a punto: Conferencia entre dos terminales, ya sea directamente entre dos terminales H.323 o entre un terminal H.323 y otro RCC a través de una pasarela. Llamada entre dos terminales (véase Llamada).

3.41 canal de registro, admisión y situación: Canal no fiable utilizado para transportar los mensajes de registro, admisión, cambio de ancho de banda y situación (según la Rec. UIT-T H.225.0), entre dos entidades H.323.

3.42 canal fiable: Conexión de transporte utilizada para la transmisión fiable de un tren de información desde su fuente hasta uno o varios destinos.

3.43 transmisión fiable: Transmisión de mensajes desde un emisor a un receptor, transmitiendo los datos en modo conexión. El servicio de transmisión garantiza que, durante la conexión de transporte, los mensajes se transmiten al receptor con orden, sin errores y con control de flujo.

3.44 sesión con protocolo en tiempo real: Para cada participante, la sesión está definida por un par particular de direcciones de transporte de destino (una dirección de red más un par de identificadores TSAP para el protocolo en tiempo real (RTP), y el protocolo de control en tiempo real, (RTCP)). El par de direcciones de transporte de destino puede ser común a todos los participantes, como en el caso de multidifusión IP, o puede ser diferente para cada uno de ellos, como en el caso de direcciones de red de unidifusión individuales. En una sesión multimedia, el audio y el vídeo de los medios se transportan en sesiones de RTP separadas con sus propios paquetes de RTCP. Las sesiones de RTP múltiples se distinguen por direcciones de transporte diferentes.

3.45 red con conmutación de circuitos (RCC): Red de telecomunicaciones conmutada pública o privada, tal como la RTGC, la RDSI-BE o la RDSI-BA.

NOTA – Aunque la RDSI-BA no es estrictamente una red con conmutación de circuitos, presenta algunas de las características de una RCC gracias a la utilización de circuitos virtuales.

3.46 terminal: Un terminal H.323 es un punto extremo de la red que permite la comunicación bidireccional en tiempo real con otro terminal, pasarela o unidad de control multipunto H.323. Esta comunicación consta de control, indicaciones, audio, imágenes de vídeo en color y en movimiento y/o datos entre los dos terminales. Un terminal puede proporcionar sólo voz, voz y datos, voz y vídeo o voz, datos y vídeo.

3.47 dirección de transporte: Dirección de la capa de transporte de una entidad H.323 direccionable definida por el conjunto de protocolos de (inter)red que se utiliza. La dirección de transporte de una entidad H.323 está compuesta por la dirección de red más el identificador TSAP de la entidad H.323 direccionable.

3.48 conexión de transporte: Asociación establecida por una capa de transporte entre dos entidades H.323 para la transferencia de datos. En el contexto de la presente Recomendación, una conexión de transporte proporciona la transmisión fiable de información.

3.49 pasarela troncal: Pasarela que conecta dos redes similares (por ejemplo, dos redes SS7 o dos redes QSIG) en las que se utiliza la tunelización para crear transparencia total y una función tándem verdadera.

3.50 identificador de punto de acceso al servicio de capa de transporte: Elemento de información utilizado para multiplexar varias conexiones de transporte del mismo tipo en una sola entidad H.323 con todas las conexiones de transporte que comparten la misma dirección de red (por ejemplo, el número de puerto en un entorno TCP/UDP/IP). Los identificadores TSAP pueden ser (pre)asignados estáticamente por alguna autoridad internacional o bien ser asignados dinámicamente durante el establecimiento de una comunicación. Los identificadores TSAP asignados dinámicamente son de naturaleza transitoria, es decir, sus valores sólo son válidos mientras dura una llamada.

3.51 unidifusión: Proceso de transmisión de mensajes de una fuente a un destino.

3.52 canal no fiable: Trayecto de comunicación lógico utilizado para la transmisión no fiable de un tren de información desde su fuente a uno o más destinos.

3.53 transmisión no fiable: Transmisión de mensajes desde un emisor a uno o más receptores con transmisión de datos en modo sin conexión. El servicio de transmisión consiste en la entrega *sin garantías* de la unidad de datos de protocolo, lo que significa que cabe la posibilidad de que los mensajes transmitidos por el emisor se pierdan, se dupliquen o los reciba el receptor (o cualquiera de los receptores) sin orden.

3.54 identificador de punto de acceso al servicio de capa de transporte conocido: Identificador TSAP, asignado por una autoridad (internacional) encargada de la asignación de identificadores TSAP, a un protocolo de interconexión de (inter)redes particular y a los protocolos de transporte conexos (por ejemplo, la IANA para números de puerto de TCP y UDP). Este identificador tiene la garantía de ser único en el contexto del protocolo correspondiente.

3.55 zona: Conjunto de todos los terminales (Tx), pasarelas (GW) y unidades de control multipunto (MCU) gestionados por un solo controlador de acceso (GK) (véase la figura 3). Una zona tiene solamente un controlador de acceso. La zona puede ser independiente de la topología de la red y comprender múltiples segmentos de red conectados mediante encaminadores (R) u otros dispositivos.

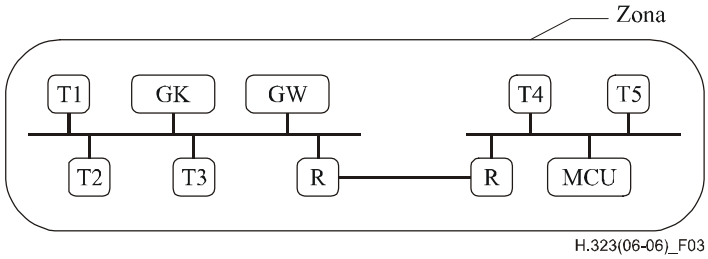


Figura 3/H.323 – Zona

4 Símbolos y abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

4CIF 4 veces CIF (*4 times CIF*)

16CIF 16 veces CIF (*16 times CIF*)

ABNF Forma aumentada de Backus-Naur (*augmented Backus-Naur form*)

ABR Velocidad binaria disponible (*available bit rate*)

ABT/DT Transferencia de bloques ATM/transmisión diferida (*ATM block transfer/delayed transmission*)

ABT/IT Transferencia de bloques ATM/transmisión inmediata (*ATM block transfer/immediate transmission*)

ACF Confirmación de admisión (*admission confirmation*)

AGW Pasarela de acceso (*access gateway*)

APE Entidad de protocolo de aplicación (*application protocol entity*)

ARJ Rechazo de admisión (*admission reject*)

ARQ Petición de admisión (*admission request*)

ATC Capacidad de transferencia ATM (*ATM transfer capability*)

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

BAS Señal de asignación de velocidad binaria (*bit rate allocation signal*)

BCF Confirmación de cambio de anchura de banda (*bandwidth change confirmation*)

BCH Bose, Chaudhuri y Hocquengham

B-HLI Información de capa alta de banda ancha (*broadband high layer information*)

BRJ Rechazo de cambio de ancho de banda (*bandwidth change reject*)

BRQ Petición de cambio de ancho de banda (*bandwidth change request*)

BTC Capacidad de transferencia de banda ancha (*broadband transfer capability*)

CAS Señalización asociada al canal (*channel associated signalling*)

CDV Variación del retardo de célula (*cell delay variation*)

CED Tono de identificación del terminal llamado (*called terminal identification tone*)

CER Tasa de errores de células (*cell error ratio*)

CID Identificador de conferencia (*conference identifier*)

CIF Formato intermedio común (*common intermediate format*)

CLR Tasa de pérdida de células (*cell loss ratio*)

CMR Velocidad de inserción incorrecta de células (*cell misinsertion rate*)

CNG Tono de llamada (*calling tone*)

CTD Retardo de transferencia de células (*cell transfer delay*)

DBR Velocidad binaria determinista (*deterministic bit rate*)

DCF Confirmación de desligamiento (*disengage confirmation*)

DNS Sistema de nombres de dominio (*domain name system*)

DRQ Petición de desligamiento (*disengage request*)

DSVD Voz y datos simultáneos digitales (*digital simultaneous voice and data*)

DTMF Multifrecuencia bitono (*dual-tone multifrequency*)

FAS Señalización asociada a la facilidad (*facility associated signalling)*

FIR Intrapetición completa (*full intra request*)

GCC Control genérico de conferencia (*generic conference control*)

GCF Confirmación de controlador de acceso (*gatekeeper confirmation*)

GID Identificador de llamada global (*global call identifier*)

GIT Transporte de identificador genérico (*generic identifier transport*)

GK Controlador de acceso (*gatekeeper*)

GQoS Calidad de servicio garantizada (*guaranteed quality of service*)

GRJ Rechazo de controlador de acceso (*gatekeeper reject*)

GRQ Petición de controlador de acceso (*gatekeeper request*)

GW Pasarela (*gateway*)

HDLC Control de alto nivel para enlaces de datos (*high level data link control*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

IACK Acuse de recibo de información (*information acknowledgment*)

IANA Autoridad de asignación de números Internet (*Internet assigned numbers authority*)

ID Identificador

IE Elemento de información (*information element*)

IMT Enlace troncal entre máquinas (*inter-machine trunk*)

INAK Acuse de recibo de información negativo (*information negative acknowledgment*)

IP Protocolo Internet (*Internet protocol*)

IPX Intercambio de protocolo de interred (*internetwork protocol exchange*)

IRQ Petición de información (*information request*)

IRR Respuesta a petición de información (*information request response*)

LAN Red de área local (*local area network*)

LCF Confirmación de localización (*location confirmation*)

LRJ Rechazo de localización (*location reject*)

LRQ Petición de localización (*location request*)

MC	Controlador multipunto (*multipoint controller*)
MCS	Sistema de comunicaciones multipunto (*multipoint communications system*)
MCU	Unidad de control multipunto (*multipoint control unit*)
MG	Pasarela de medios (*media gateway*)
MGC	Controlador de pasarela de medios (*media gateway controller*)
MIME	Ampliaciones multifunción del correo Internet (*multipurpose Internet mail extensions*)
MP	Procesador multipunto (*multipoint processor*)
MTU	Unidad de transmisión máxima (*maximum transmission unit*)
NACK	Acuse de recibo negativo (*negative acknowledge*)
NFAS	Señalización no asociada a la facilidad (*non-facility associated signalling*)
NNI	Interfaz red-red (*network-to-network interface*)
NSAP	Punto de acceso al servicio de capa de red (*network layer service access point*)
OLC	Mensaje **openLogicalChannel** H.245 (*H.245* ***openLogicalChannel*** *message*)
PBN	Red por paquetes (*packet based network*)
PDU	Unidad de datos de paquetes (*packet data unit*)
PPP	Protocolo punto a punto (*point-to-point protocol*)
PRI	Interfaz de velocidad primaria (*primary rate interface*)
PU-RDSI	Parte de usuario de la RDSI
QCIF	Cuarto de CIF (*quarter CIF*)
QoS	Calidad de servicio (*quality of service*)
QSIG	Señalización entre puntos de referencia Q definida en [44] (*signalling between the Q reference points defined in [44]*)
RAS	Registro, admisión y situación (*registration, admission and status*)
RAST	Terminal de recepción y emisión (*receive and send terminal*)
RCC	Red con conmutación de circuitos
RCF	Confirmación de registro (*registration confirmation*)
RDSI	Red digital de servicios integrados
RDSI-BA	Red digital de servicios integrados de banda ancha
RDSI-BE	Red digital de servicios integrados de banda estrecha
RIP	Petición en curso (*request in progress*)
RRJ	Rechazo de registro (*registration reject*)
RRQ	Petición de registro (*registration request*)
RTCP	Protocolo de control en tiempo real (*real time control protocol*)
RTGC	Red telefónica general conmutada
RTP	Protocolo en tiempo real (*real time protocol*)
SBE	Extensión de un solo byte (*single byte extension*)
SBR1	Configuración 1 de velocidad binaria estadística (*statistical bit rate configuration 1*)

SBR2 Configuración 2 de velocidad binaria estadística (*statistical bit rate configuration 2*)

SBR3 Configuración 3 de velocidad binaria estadística (*statistical bit rate configuration 3*)

SCI Indicación de control de servicio (*service control indication*)

SCM Modo de comunicaciones seleccionado (*selected communications mode*)

SCR Respuesta de control de servicio (*service control response*)

SDL Lenguaje de especificación y descripción (*specification and description language*)

SECBR Tasa de bloques de células con muchos errores (*severely errored cell block ratio*)

SPX Intercambio de protocolo secuencial (*sequential protocol exchange*)

SQCIF Sub QCIF (*sub QCIF*)

SS7 Sistema de señalización N.º 7

SSRC Identificador de fuente de sincronización (*synchronization source identifier*)

TCP Protocolo de control de transporte (*transport control protocol*)

TGW Pasarela troncal (*trunking gateway*)

TSAP Punto de acceso al servicio de capa de transporte (*transport layer service access point*)

UCF Confirmación de desregistro (*unregister confirmation*)

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

UIT-T Unión Internacional de Telecomunicaciones – Sector de Normalización de las Telecomunicaciones

UNI Interfaz usuario-red (*user-to-network interface*)

URJ Rechazo de desregistro (*unregister reject*)

URQ Petición de desregistro (*unregister request*)

VC Canal virtual (*virtual channel*)

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

El tiempo futuro o la expresión "deberá" indican un requisito obligatorio.

El condicional "debería" indica una forma de proceder aconsejada pero no exigida.

"Puede" o "podrá" indican una forma de proceder opcional más bien que una recomendación de que se realice algo.

Las referencias a cláusulas, subcláusulas, anexos y apéndices lo son a elementos de esta Recomendación, salvo que se indique explícitamente otra especificación. Por ejemplo, 1.4 se refiere a 1.4 de la presente Recomendación; mientras que 6.4/H.245 se refiere a 6.4 de la Rec. UIT-T H.245.

En esta Recomendación, el término "red" se utiliza para indicar cualquier red por paquetes, independientemente de la conexión física subyacente o del ámbito geográfico de la red. El término incluye redes de área local, interredes y otras redes de paquetes. El término "red con conmutación de circuitos" o "RCC" se utiliza explícitamente cuando se alude a redes con conmutación de circuitos tales como la RTGC y la RDSI.

Cuando existan elementos tanto en la red por paquetes como en la RCC, las referencias al elemento de la RCC serán explícitas. Por ejemplo, una MCU es una MCU H.323 en la red por paquetes y una MCU de RCC es una MCU en la RCC.

La presente Recomendación describe la utilización de tres tipos de mensaje diferentes: los H.245, los RAS y los de señalización de llamada H.225.0. Para distinguir entre los diferentes tipos de mensajes se aplica el convenio siguiente: los nombres de los mensajes y parámetros H.245 están formados por varias palabras concatenadas y en negritas (**maximumDelayJitter** (**fluctuación de retardo máxima**)) los nombres de los mensajes RAS se representan mediante abreviaturas de tres letras (ARQ) y los nombres de los mensajes de señalización de llamada H.225.0 constan de una o más palabras que comienzan por mayúscula (Call Proceeding (Llamada en curso)).

6 Descripción del sistema

La presente Recomendación describe los elementos de los componentes H.323, o sea, los terminales, las pasarelas, los controladores de acceso, los MC y las MCU. Dichos componentes se comunican mediante la transmisión de trenes de información. En esta cláusula se describen sus características.

6.1 Trenes de información

Los componentes videotelefónicos se comunican mediante la transmisión de trenes de información. Dichos trenes de información se clasifican en trenes de vídeo, audio, datos, control de las comunicaciones y control de la llamada de la siguiente manera.

Señales de audio que contienen señales vocales digitalizadas y codificadas. Para reducir la velocidad binaria media de las señales de audio, se puede proporcionar activación por la voz. La señal de audio va acompañada por una señal de control de audio.

Señales de vídeo que contienen vídeo en movimiento digitalizado y codificado. El vídeo se transmite a una velocidad no superior a la seleccionada como resultado del intercambio de capacidades. La señal de vídeo va acompañada por una señal de control de vídeo.

Señales de datos que incluyen imágenes fijas, facsímil, documentos, ficheros de ordenador y otros trenes de datos.

Señales de control de las comunicaciones que transfieren datos de control entre elementos funcionales que se comportan como distantes y se utilizan para el intercambio de capacidad, apertura y cierre de canales lógicos, control de modo y otras funciones que forman parte del control de las comunicaciones.

Señales de control de la llamada que se utilizan para el establecimiento de comunicaciones, la desconexión de las mismas y otras funciones del control de la llamada.

Los trenes de información descritos anteriormente son formateados y enviados a la interfaz de red como se describe en la Rec. UIT-T H.225.0.

6.2 Características de los terminales

En la figura 4 se muestra un ejemplo de terminal H.323. El diagrama muestra las interfaces del equipo de usuario, el códec de vídeo, el códec de audio, el equipo telemático, la capa H.225.0, las funciones de control del sistema y la interfaz con la red por paquetes. Todos los terminales H.323 tendrán una unidad de control del sistema, capa H.225.0, interfaz de red y unidad códec de audio. La unidad códec de vídeo y las aplicaciones de datos de usuario son opcionales.

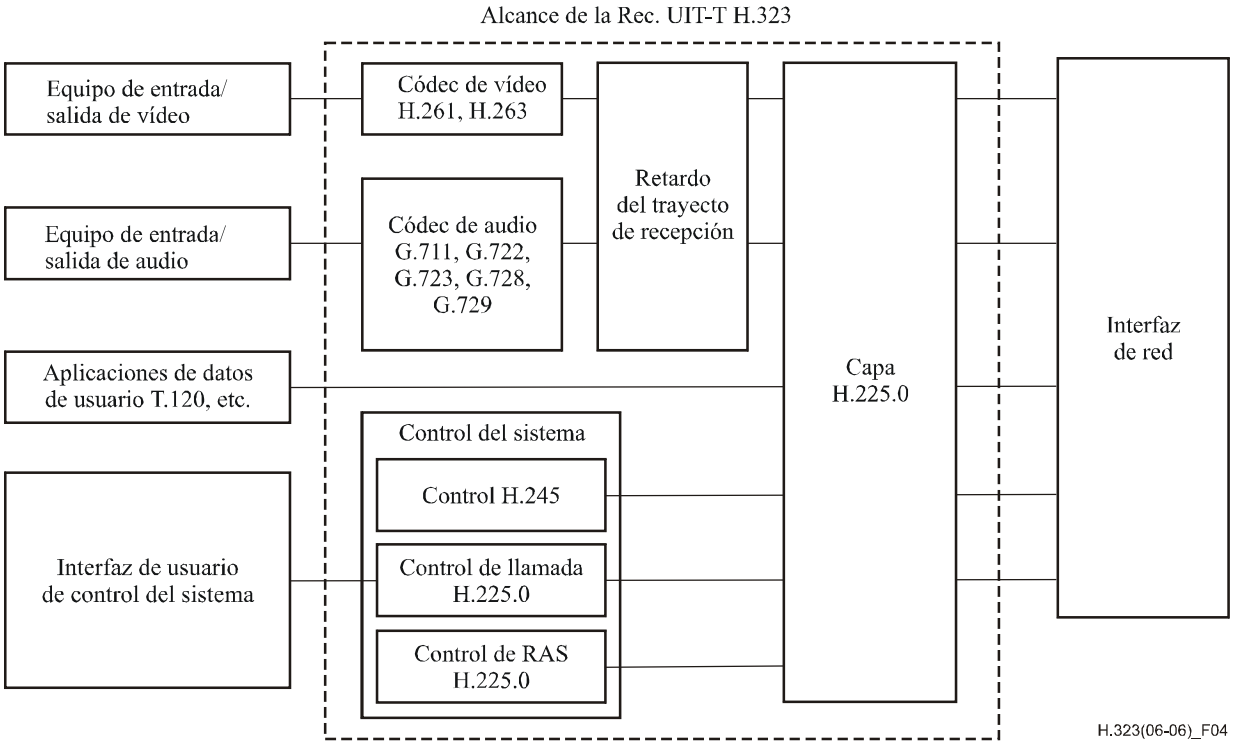


Figura 4/H.323 – Equipo terminal H.323

6.2.1 Elementos de terminal fuera del alcance de la presente Recomendación

Los siguientes elementos quedan fuera del alcance de esta Recomendación y, por consiguiente, no se definen en la misma:

- Los dispositivos de audio asociados, que proporcionan detección de activación por la voz, micrófono y altavoz, instrumento telefónico o equivalente, mezcladores de micrófonos múltiples y compensación del eco acústico.
- El equipo de vídeo asociado, que proporciona cámaras y monitores y su control y selección y el procesamiento de vídeo para mejorar la compresión o proporcionar funciones de división de la pantalla.
- Las aplicaciones de datos e interfaces de usuario asociadas, que emplean T.120 u otros servicios de datos por el canal de datos.
- La interfaz de red asociada, que proporciona la interfaz con la red por paquetes, soportando la señalización apropiada y los niveles de tensión de acuerdo con las normas nacionales e internacionales.
- El control del sistema por el usuario humano, la interfaz de usuario y su funcionamiento.

6.2.2 Elementos del terminal dentro del alcance de la presente Recomendación

Los siguientes elementos quedan dentro del alcance de la presente Recomendación y, por consiguiente, son objeto de normalización y se definen en la misma:

- El códec de vídeo (H.261, etc.), que codifica el vídeo a partir de la fuente de vídeo (es decir, una cámara) para transmisión y decodifica el código de vídeo recibido, que es la salida hacia una presentación visual del vídeo.
- El códec de audio (G.711, etc.), que codifica la señal de audio del micrófono para transmisión y decodifica el código de audio recibido que es la salida hacia el altavoz.

- El canal de datos, que soporta aplicaciones telemáticas tales como pizarras electrónicas, transferencia de imágenes fijas, intercambio de ficheros, acceso a bases de datos, conferencias audiográficas, etc. La aplicación de datos normalizada para conferencia audiográfica en tiempo real es la Rec. UIT-T T.120. Se pueden utilizar también otras aplicaciones y protocolos mediante la negociación H.245, como se especifica en 6.2.7.
- La unidad de control del sistema (H.245, H.225.0), que proporciona la señalización para un funcionamiento adecuado del terminal H.323. Permite el control de la llamada, el intercambio de capacidad, la señalización de instrucciones e indicaciones y facilita mensajes de apertura y descripción completa del contenido de los canales lógicos.
- La capa H.225.0 (H.225.0), que formatea los trenes de vídeo, audio, datos y control transmitidos en mensajes de salida hacia la interfaz de la red y recupera los trenes de vídeo, audio, datos y control recibidos de los mensajes que han sido introducidos desde la interfaz de la red. Además, lleva a cabo la alineación de trama lógica, la numeración secuencial, la detección de errores y la corrección de los mismos según conviene a cada tipo de medio.

6.2.3 Interfaz de la red por paquetes

La interfaz de la red por paquetes es específica de la implementación y queda fuera del alcance de la presente Recomendación. No obstante, la interfaz de red deberá proporcionar los servicios descritos en la Rec. UIT-T H.225.0. Esto significa que el servicio de extremo a extremo fiable (por ejemplo, TCP, SPX) es obligatorio para el canal de control H.245, los canales de datos y el canal de señalización de llamada. El servicio de extremo a extremo no fiable (por ejemplo, UDP, IPX) es obligatorio para los canales de audio, los canales de vídeo y el canal RAS. Estos servicios pueden ser dúplex o símplex y de unidifusión o multidifusión dependiendo de la aplicación, las capacidades de los terminales y la configuración de la red.

6.2.4 Códec de vídeo

El códec de vídeo es opcional. Si se dispone de capacidad de vídeo, se hará con arreglo a las exigencias de la presente Recomendación. Todos los terminales H.323 que proporcionen comunicaciones de vídeo deberán ser capaces de codificar y decodificar vídeo de acuerdo con QCIF H.261. Opcionalmente, un terminal también puede ser capaz de codificar y decodificar vídeo de acuerdo con los otros modos H.261 o H.263. Si un terminal soporta H.263 con CIF o con una resolución mayor, deberá también soportar CIF H.261. Todos los terminales que soporten H.263 deberán soportar QCIF H.263. Los códecs H.261 y H.263 de la red serán utilizados sin corrección de errores BCH y sin alineación de trama en la corrección de errores.

Asimismo, un terminal puede ser capaz de codificar y decodificar vídeo de conformidad con la Rec. UIT-T H.264. En la Rec. UIT-T H.241 se definen las negociaciones de los modos de vídeo H.264.

Se pueden utilizar también otros códecs de vídeo y otros formatos de imagen mediante la negociación H.245. Más de un canal de vídeo puede ser transmitido y/o recibido de acuerdo con lo negociado a través del canal de control H.245. El terminal H.323 puede, opcionalmente, enviar más de un canal de vídeo al mismo tiempo, por ejemplo, para llevar la imagen del conferenciante y una segunda fuente de vídeo. El terminal H.323 puede recibir, opcionalmente, más de un canal de vídeo al mismo tiempo, por ejemplo, para visualizar los múltiples participantes en una conferencia multipunto distribuida.

La velocidad binaria de vídeo, el formato de imagen y las opciones de algoritmo que pueden ser aceptados por el decodificador se definen durante el intercambio de capacidades utilizando H.245. El codificador tiene la libertad de transmitir cualquier cosa que se halle dentro del conjunto de capacidades del decodificador. El decodificador debería tener la posibilidad de generar peticiones de modos determinados vía H.245, pero el codificador está autorizado a ignorar simplemente estas peticiones si no son modos obligatorios. Los decodificadores que indican capacidad para una

determinada opción de algoritmo deberán también ser capaces de aceptar trenes binarios de vídeo que no utilicen esa opción.

Los terminales H.323 habrán de poder funcionar con velocidades binarias de vídeo, velocidades de trama y, si se soporta más de una resolución de imagen, resoluciones de imagen que pueden ser asimétricas. Esto permitirá, por ejemplo, que un terminal con capacidad de CIF transmita QCIF mientras recibe imágenes CIF.

Cuando se abre uno de los canales lógicos de vídeo, se señaliza al receptor el modo de funcionamiento seleccionado que se ha de utilizar en ese canal en el mensaje **openLogicalChannel** (**apertura de canal lógico**) H.245. El encabezamiento dentro del canal lógico de vídeo indica qué modo se utiliza realmente para cada imagen dentro de la capacidad indicada.

El tren de vídeo se formatea como se describe en la Rec. UIT-T H.225.0.

6.2.4.1 Presencia continua basada en terminal

Los terminales H.323 pueden recibir más de un canal de vídeo, en particular para conferencia multipunto. En estos casos, el terminal H.323 quizá necesite realizar una función de mezcla o conmutación de vídeo para presentar la señal de vídeo al usuario. La función puede incluir la presentación del vídeo de más de un terminal al usuario. El terminal H.323 utilizará capacidades simultáneas H.245 para indicar cuántos trenes de vídeo simultáneos es capaz de decodificar. La capacidad simultánea de un terminal no deberá limitar el número de trenes de vídeo que son multidifundidos en una conferencia (esta elección la realiza el MC).

6.2.5 Códec de audio

Todos los terminales H.323 tendrán un códec de audio y serán capaces de codificar y decodificar señales vocales de conformidad con la Rec. UIT-T G.711. Todos los terminales transmitirán y recibirán ley A y ley μ. Un terminal puede, opcionalmente, ser capaz de codificar y decodificar señales vocales utilizando otros códecs de audio que se pueden señalizar mediante negociación H.245. El algoritmo de audio empleado por el codificador se obtendrá durante el intercambio de capacidades utilizando H.245. El terminal H.323 debería tener la posibilidad de funcionamiento asimétrico para todas las capacidades de audio que haya declarado dentro del mismo conjunto de capacidades; por ejemplo, debería poder enviar G.711 y recibir G.728 si es capaz de ambas cosas.

Si se dispone de audio G.723.1, el códec de audio será capaz de codificar y decodificar con arreglo al modo de 5,3 kbit/s o al modo de 6,3 kbit/s.

El tren de audio se formatea como se describe en la Rec. UIT-T H.225.0.

El terminal H.323 puede, opcionalmente, enviar más de un canal de audio al mismo tiempo, por ejemplo, para transportar las señales de dos idiomas.

Los paquetes de audio deberán ser entregados a la capa de transporte periódicamente, con un intervalo determinado por la Recomendación de códec de audio que se utilice (intervalo de trama de audio). La entrega de cada uno de los paquetes de audio tendrá lugar no más tarde de 5 ms después de un múltiplo completo del intervalo de trama de audio, medido desde la entrega de la primera trama de audio (fluctuación de retardo de audio). Los codificadores de audio capaces de limitar más aún su fluctuación de retardo de audio pueden indicarlo utilizando el parámetro **maximumDelayJitter** H.245 de la estructura **h2250Capability** (**capacidad h2250**) contenida en un mensaje del conjunto de capacidades de terminal, de tal manera que los receptores puedan reducir, opcionalmente, sus memorias intermedias de fluctuación de retardo. Esto no es lo mismo que el campo de fluctuación entre llegadas del RTCP.

NOTA – El punto de prueba de fluctuación de retardo máxima se halla a la entrada de la capa de red de transporte. No se incluye la fluctuación de pila de red, de red, de control y de tarjeta interfaz.

6.2.5.1 Mezcla de audio

Los terminales H.323 pueden recibir más de un canal de audio, sobre todo para conferencias multipunto. En estos casos, el terminal H.323 quizá necesite efectuar una función de mezcla de audio para presentar una señal de audio compuesta al usuario. El terminal H.323 utilizará capacidades simultáneas H.245 para indicar cuántos trenes de audio simultáneos es capaz de decodificar. La capacidad simultánea de un terminal no deberá limitar el número de trenes de audio que son multidifundidos en una conferencia.

6.2.5.2 Asimetría máxima de la transmisión audio-vídeo

Para que los terminales H.323 puedan fijar adecuadamente el tamaño de sus memorias intermedias en recepción, dichos terminales transmitirán el mensaje de **h2250MaximumSkewIndication** (**indicación de asimetría máxima h2250**) para indicar la asimetría máxima entre las señales de audio y de vídeo entregadas al transporte de red. El mensaje **indicación de asimetría máxima h2250** se enviará para cada par de canales lógicos de audio y vídeo asociados. Esto no se requiere para conferencias de audio solamente o híbridas. La sincronización con el movimiento de los labios, si se desea, se logrará mediante indicaciones o indicaciones de tiempo.

6.2.5.3 Funcionamiento a baja velocidad binaria

No puede utilizarse audio G.711 en una conferencia H.323 que se cursa por enlaces o segmentos a baja velocidad binaria (< 56 kbit/s). Un punto extremo utilizado para comunicaciones multimedia por dichos enlaces o segmentos a baja velocidad binaria debe tener un códec de audio capaz de codificar y decodificar señales vocales con arreglo a la Rec. UIT-T G.723.1. Un punto extremo utilizado para comunicaciones de sólo audio por dichos enlaces o segmentos a baja velocidad binaria debe tener un códec de audio capaz de codificar y decodificar señales vocales con arreglo a la Rec. UIT-T G.729. Un punto extremo puede soportar varios códecs de audio a fin de proporcionar la más amplia interoperabilidad posible con aquellos puntos extremos que sólo soportan un códec de audio a baja velocidad binaria. El punto extremo indicará en los procedimientos de intercambio de capacidades H.245 al comienzo de cada llamada, la capacidad de recibir audio con arreglo a las Recomendaciones de audio disponibles que puede ser soportada dentro de las limitaciones de velocidad binaria conocidas de la conexión. Un punto extremo que no tiene esta capacidad de audio a baja velocidad binaria no puede operar cuando la conexión de extremo a extremo contiene uno o más segmentos a baja velocidad binaria.

El punto extremo también cumplirá el requisito de 6.2.5 de ser capaz de codificar y decodificar señales vocales con arreglo a la Rec. UIT-T G.711. Sin embargo, el punto extremo no necesita indicar esta capacidad si está seguro de que está comunicando a través de un segmento a baja velocidad binaria. Si un punto extremo desconoce la presencia, en la conexión extremo a extremo, de cualesquiera enlaces o segmentos con capacidad insuficiente para soportar audio G.711 (así como otros trenes de medios deseados, si los hay), el punto extremo declarará entonces la capacidad de recibir audio según la Rec. UIT-T G.711.

6.2.6 Retardo del trayecto de recepción

El retardo del trayecto de recepción incluye el retardo añadido al tren de medios para mantener la sincronización y tener en cuenta la fluctuación de las llegadas de los paquetes de red. Los trenes de medios pueden ser retardados, opcionalmente, en el trayecto de procesamiento del receptor para mantener la sincronización con otros trenes de medios. Además, el tren de medios puede ser retardado, si así se desea, en previsión de los retardos de red que causan la fluctuación de las llegadas de los paquetes. Un terminal H.323 no añadirá retardo a tal fin en su trayecto de medios de transmisión.

Los puntos de procesamiento intermedios, tales como las MCU o las pasarelas, pueden alterar la información de indicación de tiempo de vídeo y audio y transmitirán indicaciones de tiempo de vídeo y audio y números de secuencia convenientemente modificados, reflejando sus señales transmitidas. Los puntos extremos de recepción pueden añadir el retardo que haga falta en el trayecto de audio para lograr la sincronización con el movimiento de los labios.

6.2.7 Canal de datos

Uno o más canales de datos son opcionales. El canal de datos puede ser unidireccional o bidireccional, dependiendo de los requisitos de la aplicación de datos.

La Rec. UIT-T T.120 es la base por defecto de la interoperabilidad de datos entre un terminal H.323 y otro terminal H.323, H.324, H.320 o H.310. Cuando se implemente cualquier aplicación opcional de datos utilizando una o más de las Recomendaciones UIT-T negociables vía H.245, la aplicación T.120 equivalente, si existe, será una de las proporcionadas.

Hay que tener en cuenta que se pueden utilizar aplicaciones de datos no normalizadas (**dataApplicationCapability.application** = **non-standard** application (**aplicación capacidad de aplicación de datos = aplicación no normalizada**)) y datos de usuario transparente (**dataApplicationCapability.application = userData** application (**aplicación capacidad de aplicación de datos = aplicación de datos de usuario**), **dataProtocolCapability** = **transparent** (**capacidad de protocolo de datos = transparente**)) tanto si se proporciona como si no se proporciona la aplicación T.120 equivalente.

La capacidad T.120 se señalará utilizando la **dataApplicationCapability.application** = **t120** application (**aplicación capacidad de aplicación de datos = t120**), la **dataProtocolCapability** = **separateLANStack** (**capacidad de protocolos de datos = pila de LAN separada**).

Dentro de la **MediaDistributionCapability** (**capacidad de distribución de medios**), se utilizará la estructura de **distributedData** (**datos distribuidos**) si está disponible la T.120 multidifusión y/o la estructura **centralizedData** (**datos centralizados**) si está disponible la T.120 unidifusión. Cualquier nodo que soporte la capacidad de datos T.120 soportará la pila unidifusión T.123 normalizada.

En el mensaje **openLogicalChannel**, la elección **distribution** (**distribución**) de la estructura **NetworkAccessParameters** (**parámetros de acceso a la red**) se pone a **unicast** (**unidifusión**) si ha de utilizarse la T.123 o a **multicast** (**multidifusión**) si ha de utilizarse el anexo A/T.125. La elección **networkAddress** (**dirección de red**) se pone a **localAreaAddress** (**dirección de área local**), que debe siempre ser **unicastAddress** (**dirección unidifusión**). Dentro de la secuencia **iPAddress** (**dirección IP**), el campo de **network** (**red**) se pone a la dirección IP binaria y el **tsapIdentifier** (**identificador de TSAP**) se pone al puerto dinámico en el que la pila T.120 estará llamando o escuchando.

El canal de datos se formatea como se describe en la Rec. UIT-T H.225.0.

6.2.7.1 Canales de datos T.120

La conexión T.120 se establece durante una comunicación H.323 como parte intrínseca a la llamada. Los procedimientos para establecer la conexión T.120 antes de la conexión H.323 quedan en estudio.

Se siguen los procedimientos normales de establecimiento de la comunicación de 8.1. Después de que se produce el intercambio de capacidades, se abre un canal lógico bidireccional para la conexión T.120 de acuerdo con los procedimientos H.245 normales, indicando que se va a crear una nueva conexión como se describe a continuación.

La apertura de un canal lógico bidireccional para T.120 puede ser iniciada por la entidad que envía el mensaje **openLogicalChannel** y se siguen después los procedimientos de canal lógico bidireccional de la Rec. UIT-T H.245.

Para abrir realmente el canal lógico, la entidad iniciadora enviará un mensaje **openLogicalChannel** indicando que se ha de abrir un canal de datos T.120 en los **forwardLogicalChannelParameters** (**parámetros de canal lógico directo**), así como en los **reverseLogicalChannelParameters** (**parámetros de canal lógico inverso**). El iniciador incluirá una dirección de transporte en el mensaje **openLogicalChannel**. El punto extremo par puede optar por ignorar la dirección de transporte. Un punto extremo puede utilizar un número de puerto dinámico para la dirección de transporte T.120 en lugar de utilizar el puerto 1503 especificado en la Rec. UIT-T T.123. Si el par (el respondedor) acepta este canal lógico, confirmará la apertura del canal lógico utilizando el mensaje **openLogicalChannelAck** (**acuse de apertura de canal lógico**). En el mensaje **openLogicalChannelAck**, el respondedor incluirá una dirección de transporte incluso si espera que el iniciador origine la llamada T.120. En todos los casos, la dirección de transporte para la conexión T.120 se transportará en el parámetro **separateStack** (**pila separada**), y seguirá siendo válida durante el funcionamiento del canal lógico.

En el mensaje **openLogicalChannel**, puede opcionalmente colocarse la elección **t120SetupProcedure** de la estructura **NetworkAccessParameters** para indicar al respondedor cómo desearía el iniciador establecer la comunicación T.120. El respondedor es libre de contraordenar esta preferencia. El mensaje **originateCall** (**iniciar llamada**) indica que el iniciador desearía que el respondedor efectúe la llamada. El mensaje **waitForCall** (**espera de llamada**) indica que el iniciador desearía que el respondedor reciba la llamada. No se utiliza **issueQuery** (**emitir consulta**) cuando se indica una preferencia.

En el mensaje **openLogicalChannelAck**, puede opcionalmente colocarse la elección **t120SetupProcedure** de la estructura **NetworkAccessParameters** para indicar al iniciador cómo se establecerá la comunicación T.120. Si ningún punto extremo tiene una preferencia, la comunicación T.120 debería establecerse en el mismo sentido que la comunicación H.323. El mensaje **originateCall** indica al iniciador que efectúe la llamada. El mensaje **waitForCall** indica al iniciador que recibirá la llamada. Quienquiera que la origine, emitirá una petición de incorporación o bien una petición de invitación, según en qué punto extremo se resolvió la determinación principal/subordinado (en la conferencia T.120 el principal ocupa siempre una jerarquía superior). **issueQuery** puede ser utilizada por una pasarela para indicar al iniciador que debe originar la llamada y emitir una petición de indagación al punto extremo distante. A continuación debe iniciar la conferencia T.120 con arreglo al contenido de la respuesta de indagación (como se describe en la Rec. UIT-T T.124).

Cuando sea posible, la comunicación T.120 debería establecerse en el mismo sentido que la comunicación H.323. El iniciador OLC no debería indicar una preferencia a menos que sea necesario modificar este comportamiento por defecto. Cuando el iniciador indica una preferencia, el respondedor no debería contraordenarla, a menos que sea necesario. Cuando no se indica ninguna preferencia, el respondedor debería especificar el comportamiento por defecto a menos que sea necesario hacer otra cosa.

En los mensajes **openLogicalChannel** y **openLogicalChannelAck**, el parámetro **associateConference** (**asociación de conferencia**) se pondrá a FALSO.

Las aplicaciones de la Rec. UIT-T T.120 seguirán los procedimientos de la Rec. UIT-T T.123 para la pila de protocolos indicada en la **dataProtocolCapability** (**capacidad de protocolo de datos**) salvo que se emplearán las direcciones de transporte descritas anteriormente para el establecimiento de la conexión.

Si un punto extremo es el MC activo o el principal en una conferencia que incluye T.120, debe estar también en control del nodo proveedor superior T.120.

Si un punto extremo pretende crear una conferencia que incluya audio y/o vídeo más datos T.120, se establecerá entonces el canal de control H.245 antes de que se efectúe la conexión T.120. Esto se aplica a las acciones creación, incorporación e invitación conferencia y las acciones de un MC. Los procedimientos de establecimiento de comunicación H.323 se utilizarán para establecer el MC activo (si lo hay), antes de que se efectúe una conexión T.120.

A fin de establecer una conexión T.120 utilizando una petición incorporación GCC, es necesario que los puntos extremos conozcan el nombre de la conferencia T.120. Si existe un alias que representa un nombre de conferencia H.323 (**conferenceAlias**), debe utilizarse entonces el mismo texto que se utiliza para el alias de conferencia como la parte de texto del nombre de conferencia T.120. Análogamente, el CID H.323 debe utilizarse como nombre de conferencia T.120 numérico como sigue. Cada octeto del CID H.323 se convierte en una serie de tres caracteres ASCII que representa el valor decimal del octeto que se está convirtiendo. Téngase en cuenta que esto exige que el valor de algunos octetos de CID se conviertan de manera que se utilicen caracteres "0" para relleno. El resultado será una cadena de 48 caracteres ASCII.

Puede interrogarse a un MP T.120 al respecto de una lista de conferencias existentes. El CID H.323 puede estar disponible reconvirtiendo de nuevo el nombre conferencia numérica T.120 en la cadena de octetos de 16 octetos. Análogamente el nombre conferencia de texto puede utilizarse como alias de conferencia H.323. Obsérvese que una interrogación de conferencia T.124 puede ocurrir fuera de banda a partir de la H.323 y antes de que un punto extremo establezca una comunicación H.323.

La terminación de la conferencia T.120 asociada no implica la terminación de la llamada H.323. En otras palabras, el cierre del canal T.120 sólo afectará al tren de datos de una llamada H.323 y no afectará a ninguna otra parte de la llamada H.323. Por el contrario, cuando termina una llamada o conferencia H.323, terminará también la conferencia T.120 asociada.

NOTA – El funcionamiento T.120 después de completar el establecimiento de la conexión queda fuera del ámbito de la presente Recomendación.

6.2.7.2 Control de dispositivo distante

Los puntos extremos H.323 pueden soportar el control de dispositivo distante mediante el protocolo H.282. Este protocolo se ha de soportar en un canal lógico H.245 conforme a la Rec. UIT-T H.283. La Rec. UIT-T H.283 describe el transporte de canal lógico para el protocolo H.282 en una conferencia H.323.

La Rec. UIT-T H.282 puede ser utilizada también por sistemas T.120 y transportada en una APE T.120. Además, los sistemas H.323 pueden, opcionalmente, soportar el control de dispositivo distante utilizando la Rec. UIT-T H.282 a través de T.120. Sin embargo, ésta es una opción y un sistema H.323 que soporta H.282 lo hará con la Rec. UIT-T H.283.

Si se soporta H.282 con H.283 y H.282 con T.120, se pueden utilizar ambas combinaciones. La combinación de dos protocolos de capa inferior conforme a H.282 es un asunto local. Sin embargo, H.283 siempre estará activo para dar cuenta de posibles nodos de incorporación tardíos que soportan H.282 a través de H.283 pero no H.282 a través de T.120.

6.2.8 Función de control H.245

La función de control H.245 utiliza el canal de control H.245 para llevar los mensajes de control de extremo a extremo que rigen el funcionamiento de la entidad H.323, incluyendo el intercambio de capacidades, apertura y cierre de canales lógicos, peticiones de modo preferido, mensajes de control de flujo e instrucciones e indicaciones generales.

La señalización H.245 se establece entre dos puntos extremos, un punto extremo y un MC o un punto extremo y un controlador de acceso. El punto extremo establecerá exactamente un canal de control H.245 en cada sentido para cada llamada en la que él participe. Este canal utilizará los mensajes y procedimientos de la Rec. UIT-T H.245. Obsérvese que un terminal, una MCU, una pasarela o un controlador de acceso pueden soportar muchas llamadas y, por ello, muchos canales

de control H.245. El canal de control H.245 se llevará por el canal lógico 0. Se considerará que el canal lógico 0 está permanentemente abierto desde el establecimiento del canal de control H.245 hasta la terminación de este canal. Los procedimientos normales de apertura y cierre de canales lógicos no se aplicarán al canal de control H.245.

La Rec. UIT-T H.245 especifica varias entidades de protocolo independientes que soportan señalización de punto extremo a punto extremo. Una entidad de protocolo se especifica por su sintaxis (mensajes), su semántica y un conjunto de procedimientos que establecen el intercambio de mensajes y la interacción con el usuario. Los puntos extremos H.323 soportarán la sintaxis, la semántica y los procedimientos de las siguientes entidades de protocolo:

- determinación principal/subordinado;
- intercambio de capacidades;
- señalización de canal lógico;
- señalización de canal lógico bidireccional;
- señalización de cierre de canal lógico;
- petición de modo;
- determinación de retardo de ida y vuelta;
- señalización de bucle de mantenimiento.

Las instrucciones e indicaciones generales se elegirán del conjunto de mensajes contenido en la Rec. UIT-T H.245. Además, se pueden enviar otras instrucciones e indicaciones que hayan sido definidas específicamente para transferencia en banda dentro de trenes de vídeo, audio o datos (véase la Recomendación apropiada para determinar si tales señales han sido definidas).

Los mensajes H.245 se clasifican en cuatro categorías: de petición, respuesta, instrucción e indicación. Los mensajes de petición y respuesta son utilizados por las entidades de protocolo. Los mensajes de petición requieren una acción específica por parte del receptor, incluyendo una respuesta inmediata. Los mensajes de respuesta responden a una petición correspondiente. Los mensajes de instrucción requieren una acción específica, pero no una respuesta. Los mensajes de indicación son informativos solamente y no requieren ninguna acción o respuesta. Los terminales H.323 responderán a todas las instrucciones y peticiones H.245 como se especifica en el anexo A y transmitirán indicaciones que reflejen el estado del terminal.

Los terminales H.323 deben ser capaces de descomponer analíticamente todos los mensajes de **multimediaSystemControlMessage** (**mensajes de control de sistema multimedia**) H.245 y enviarán y recibirán todos los mensajes necesarios para implementar las funciones requeridas y aquellas funciones opcionales que soporte el terminal. El anexo A contiene un cuadro en el que se muestran los mensajes H.245 que son obligatorios, opcionales o prohibidos para los terminales H.323. Los terminales H.323 deben enviar el mensaje de **functionNotSupported** (**función no soportada**) en respuesta a cualquier mensaje de petición, respuesta o instrucción no reconocida que reciban.

Se dispone de una indicación H.245, **userInputIndication** (**indicación de entrada de usuario**), para el transporte de caracteres alfanuméricos de entrada del usuario desde un telemando o un teclado, equivalente a las señales multifrecuencia bitono (DTMF, *dual-tone multi-frequency*) utilizadas en telefonía analógica o mensajes de números SBE de la Rec. UIT-T H.230. Esto se puede utilizar para operar manualmente equipos distantes tales como los sistemas de correo vocal o correo vídeo, los servicios de información por medio de un menú, etc. Los terminales H.323 soportarán la transmisión de los caracteres de entrada de usuario 0-9, "*" y "#". La transmisión de otros caracteres es opcional.

Tres mensajes de petición H.245 entran en conflicto con los paquetes de control del RTCP. Se deberían utilizar las peticiones de **videoFastUpdatePicture** (**actualización rápida de imagen de vídeo**), **videoFastUpdateGOB** (**GOB de actualización rápida de vídeo**) y **videoFastUpdateMB** (**MB de actualización rápida de vídeo**) H.245 en vez de los paquetes de control intrapetición completa (FIR, *full intra request*) y acuse de recibo negativo (NACK, *negative acknowledgement*) de la RTPC. La capacidad de aceptar FIR y NACK se señaliza durante el intercambio de capacidades H.245.

6.2.8.1 Intercambio de capacidades

El intercambio de capacidades seguirá los procedimientos de la Rec. UIT-T H.245, que prevé capacidades de recepción y transmisión separadas así como un método mediante el cual el terminal puede describir su aptitud para funcionar con diversas combinaciones de modos simultáneamente.

Las capacidades de recepción describen la posibilidad que tiene el terminal de recibir y procesar trenes de información entrantes. Los transmisores limitarán el contenido de la información que transmiten a lo que el receptor haya indicado que es capaz de recibir. La ausencia de una capacidad de recepción indica que el terminal no puede recibir (es transmisor solamente).

Las capacidades de transmisión describen la posibilidad que tiene el terminal de transmitir trenes de información. Las capacidades de transmisión sirven para ofrecer a los receptores la elección entre posibles modos de funcionamiento, de manera que el receptor pueda pedir el modo en el que prefiere recibir. La ausencia de una capacidad de transmisión indica que el terminal no ofrece la elección del modo preferido al receptor (pero puede aún transmitir cualquier cosa que se halle dentro de la capacidad del receptor).

Las capacidades de recepción y transmisión describen la posibilidad que tiene el terminal de recibir y transmitir trenes de información cuando esas capacidades no son independientes y hace falta que sean las mismas en ambos sentidos. Por ejemplo, un punto extremo podría soportar sólo funcionamiento de códec simétrico para sus códecs (en ambos sentidos según G.711 o en ambos sentidos según G.729, pero no en un sentido según G.711 y en el otro sentido según G.729). Un subordinado deberá reordenar su preferencia de códec en el mismo orden que el principal, por ejemplo, si la preferencia del subordinado es {G.729, G.711} y la preferencia del principal es {G.711, G.729}, el subordinado deberá reordenar su preferencia a {G.711, G.729}. Si el terminal ya ha manifestado su conjunto de capacidades, deberá considerar sus preferencias reordenadas cuando proceda a la apertura de los canales lógicos.

El terminal transmisor asigna a cada uno de los modos en los que el terminal puede funcionar un número de un **capabilityTable** (**cuadro de capacidades**). Por ejemplo, al audio G.723.1, al audio G.728 y al vídeo H.263 con CIF se les asignarían números distintos.

Estos números de capacidades se agrupan en estructuras llamadas **alternativeCapabilitySet** (**conjuntos de capacidades alternativas**). Cada **alternativeCapabilitySet** indica que el terminal es capaz de funcionar exactamente en uno de los modos enumerados en el conjunto. Por ejemplo, un **alternativeCapabilitySet** que indique {G.711, G.723.1, G.728} significa que el terminal puede funcionar en cualquiera de esos modos de audio, pero no en más de uno.

Las estructuras **alternativeCapabilitySet** se agrupan en estructuras **simultaneousCapabilities** (**capacidades simultáneas**). Cada **simultaneousCapabilities** indica un conjunto de modos que el terminal puede utilizar simultáneamente. Por ejemplo, una estructura **simultaneousCapabilities** que contenga las dos estructuras **alternativeCapabilitySet** {H.261, H.263} y {G.711, G.723.1, G.728} significa que el terminal puede operar con cualquiera de los códecs de vídeo al mismo tiempo que opera con cualquiera de los códecs de audio. El conjunto **simultaneousCapabilities** { {H.261}, {H.261, H.263}, {G.711, G.723.1, G.728} } significa que el terminal puede operar con dos canales de vídeo y un canal de audio simultáneamente: un canal de vídeo según H.261, otro canal de vídeo según H.261 o H.263 y un canal de audio según G.711, G.723.1 o G.728.

Cuando se utiliza funcionamiento de códec simétrico (es decir, cuando se utilice la **receiveAndTransmitVideoCapability** (**capacidad de recibir y transmitir vídeo**) o **receiveAndTransmitAudioCapability** (**capacidad de recibir y transmitir audio**)), el principal puede rechazar una petición de **openLogicalChannel** procedente del subordinado si aquél necesita que se utilicen códecs simétricos y el canal propuesto no lo es. En C.4.1.3/H.245 se describen los procedimientos de resolución de conflictos. El campo de motivo en el mensaje **openLogicalChannelReject** (**rechazar apertura de canal lógico**) deberá ser **masterSlaveConflict**.

NOTA 1 – El principal puede enviar un mensaje **requestMode** (**petición de modo**) al subordinado con el códec apropiado antes de enviar el mensaje **openLogicalChannelReject** para pedir de manera explícita un determinado códec.

NOTA 2 – Las capacidades almacenadas realmente en **capabilityTable** son a menudo más complejas que las que aquí se presentan. Por ejemplo, cada capacidad H.263 indica detalles tales como la aptitud para soportar diversos formatos de imagen con intervalos de imagen mínimos dados y la aptitud para utilizar modos de codificación opcionales. Véase una descripción completa al respecto en la Rec. UIT-T H.245.

Las capacidades totales del terminal se describen mediante un conjunto de estructuras **capabilityDescriptor** (**descriptor de capacidades**), cada una de las cuales es una sola estructura **simultaneousCapabilities** y un **capabilityDescriptorNumber** (**número de descriptor de capacidades**). Enviando más de un **capabilityDescriptor**, el terminal puede señalar dependencias entre modos de funcionamiento al describir conjuntos de modos diferentes que puede utilizar simultáneamente. Por ejemplo, si un terminal emite dos estructuras **capabilityDescriptor**, una { {H.261, H.263}, {G.711, G.723.1, G.728} }, como en el ejemplo anterior, y la otra { {H.262}, {G.711} }, ello significa que el terminal puede también operar con el códec de vídeo H.262, pero solamente con el códec de audio G.711 de baja complejidad.

Los terminales pueden añadir capacidades dinámicamente durante una sesión de comunicación emitiendo estructuras **capabilityDescriptor** adicionales o eliminar capacidades enviando estructuras **capabilityDescriptor** revisadas. Todos los terminales H.323 transmitirán por lo menos una estructura **capabilityDescriptor**.

Se pueden emitir capacidades no normalizadas y mensajes de control utilizando la estructura **nonStandardParameter** (**parámetro no normalizado**) que se define en la Rec. UIT-T H.245. Hay que tener en cuenta que si bien el significado de los mensajes no normalizados lo definen organizaciones individuales, los equipos construidos por cualquier fabricante pueden señalar cualquier mensaje no normalizado, siempre que el significado sea conocido.

Los terminales pueden emitir de nuevo conjuntos de capacidades en cualquier momento, de acuerdo con los procedimientos de la Rec. UIT-T H.245.

6.2.8.2 Señalización de canal lógico

Cada canal lógico lleva información de un transmisor a uno o más receptores y se identifica mediante un número de canal lógico que es único en cada sentido de la transmisión.

Los canales lógicos se abren y cierran utilizando los mensajes **openLogicalChannel** y **closeLogicalChannel** (**cerrar canal lógico**) y los procedimientos de la Rec. UIT-T H.245. Cuando se abre un canal lógico, el mensaje **openLogicalChannel** describe totalmente el contenido del canal lógico, incluyendo el tipo de medios, el algoritmo utilizado, cualesquiera opciones y cualquier otra información que necesite el receptor para interpretar dicho contenido. Los canales lógicos se pueden cerrar cuando ya no se necesiten. Los canales lógicos abiertos pueden estar inactivos si la fuente de información no tiene nada que enviar.

La mayoría de los canales lógicos de la presente Recomendación son unidireccionales, por lo que es posible el funcionamiento asimétrico en el que el número y tipo de trenes de información es diferente en cada sentido de la transmisión. Sin embargo, si un receptor sólo admite ciertos modos simétricos de funcionamiento, puede enviar un conjunto de capacidades de recepción que refleje sus

limitaciones, excepto cuando se indique en otros puntos de esta Recomendación. Los terminales pueden ser capaces también de utilizar un modo particular en un solo sentido de transmisión. Ciertos tipos de medios, incluyendo protocolos de datos tales como los T.120, tienen la necesidad intrínseca de un canal bidireccional para su funcionamiento. En tales casos, se puede abrir un único canal lógico bidireccional utilizando los procedimientos de apertura de canal bidireccional de la Rec. UIT-T H.245.

Los canales lógicos se abrirán utilizando el procedimiento siguiente:

El terminal iniciador enviará un mensaje **openLogicalChannel** como se describe en la Rec. UIT-T H.245. Si el canal lógico ha de transportar un tipo de medios que utiliza RTP (audio o vídeo), el mensaje **openLogicalChannel** incluirá el parámetro **mediaControlChannel** (**canal de control de medios**) que contiene la dirección de transporte para el canal RTCP inverso.

El terminal respondedor responderá con un mensaje **openLogicalChannelAck** como se describe en la Rec. UIT-T H.245. Si el canal lógico ha de transportar un tipo de medios que utiliza RTP, el mensaje **openLogicalChannelAck** incluirá el parámetro **mediaChannel** (**canal de medios**) que contiene la dirección de transporte RTP para el canal de medios y el parámetro **mediaControlChannel** que contiene la dirección de transporte para el canal RTCP hacia adelante.

Los tipos de medios (tales como datos T.120) que no utilizan RTP/RTCP omitirán los parámetros **mediaControlChannel**.

Si se abre un canal inverso correspondiente para una determinada sesión RTP existente (identificada por el **sessionID** (**ID de sesión**) del RTP), las direcciones de transporte del **mediaControlChannel** intercambiadas por el proceso **openLogicalChannel** serán idénticas a las utilizadas para el canal directo. Los valores de **sessionID** 1, 2 y 3 están preasignados a sesiones principales de audio, vídeo y datos, respectivamente. Incluso el punto extremo subordinado puede abrir canales lógicos para estas sesiones primarias sin negociar el valor de **sessionID** con el punto extremo principal. El punto extremo principal puede abrir sesiones adicionales con valores particulares de **sessionID** mayores que 3. El punto extremo subordinado puede abrir las correspondientes sesiones con el **sessionID** dado. De lo contrario, el punto extremo subordinado podría abrir sesiones adicionales con **sessionID**=0 en el mensaje **openLogicalChannel**, aunque deberá adquirir el valor real de **sessionID** del mensaje **openLogicalChannelAck** del punto extremo principal. Si se produce una colisión cuando ambos extremos tratan de establecer sesiones RTP contradictorias en el mismo momento, el punto extremo principal rechazará el intento de conflicto como se describe en la Rec. UIT-T H.245. El intento **openLogicalChannel** rechazado se puede repetir en un momento ulterior.

Salvo que se especifique otra cosa para un tipo de datos en particular, los canales de datos fiables son canales bidireccionales y, como tales, contendrán los elementos **forwardLogicalChannelParameters** y **reverseLogicalChannelParameters** sin los elementos **mediaChannel**. El punto extremo que acepta el canal devolverá el elemento **reverseLogicalChannelParameters** y estará preparado para aceptar la conexión fiable del punto extremo solicitante antes de devolver el mensaje **OpenLogicalChannelAck**.

Un punto extremo que acepte un canal fiable bidireccional deberá estar preparado para aceptar una conexión fiable del punto extremo solicitante antes de devolver el mensaje **OpenLogicalChannelAck**.

6.2.8.3 Preferencias de modo

Los receptores pueden solicitar a los transmisores que envíen un modo particular utilizando el mensaje **requestMode** H.245, que describe el modo deseado. Los transmisores deberán atenerse a esa petición cuando sea posible.

Un punto extremo que reciba la **multipointModeCommand** (**instrucción de modo multipunto**) procedente del MC cumplirá a continuación todas las instrucciones **requestMode** si se hallan dentro de su conjunto de capacidades. Téngase en cuenta que en una conferencia descentralizada, al igual que en una conferencia centralizada, todas las instrucciones **requestMode** del terminal van dirigidas al MC. El MC puede responder positivamente o no a la petición; la base para esta decisión se deja a criterio del fabricante.

6.2.8.4 Determinación principal-subordinado

Los procedimientos de determinación principal-subordinado H.245 se utilizan para resolver conflictos entre dos puntos extremos que pueden ser, ambos, el MC de una conferencia o entre dos puntos extremos que están intentando abrir un canal bidireccional. En estos procedimientos, los dos puntos extremos intercambian números aleatorios en el mensaje de **masterSlaveDetermination** (**determinación principal-subordinado**) H.245 para determinar cuál es el punto extremo principal y cuál el subordinado. Los puntos extremos H.323 deberán poder funcionar tanto en el modo principal como en el modo subordinado. Los puntos extremos fijarán el **terminalType** (**tipo de terminal**) en el valor especificado en el cuadro 1 que figura a continuación y fijarán el **statusDeterminationNumber** (**número de determinación de situación**) en un número aleatorio comprendido entre 0 y $2^{24} - 1$. El punto extremo de cada llamada sólo elegirá un número aleatorio, excepto en el caso de números aleatorios idénticos que se describe en la Rec. UIT-T H.245.

Cuadro 1/H.323 – Tipos de terminal H.323 para la determinación principal-subordinado H.245

Cuadro de valores de tipo de terminal	Entidad H.323			
Conjunto de características	**Terminal**	**Pasarela**	**Controlador de acceso**	**MCU**
Entidad sin MC	50	60	NA	NA
Entidad que contiene un MC pero no MP	70	80	120	160
Entidad que contiene MC con MP de datos	NA	90	130	170
Entidad que contiene MC con MP de datos y audio	NA	100	140	180
Entidad que contiene MC con MP de datos, audio y vídeo	NA	110	150	190

El MC activo de una conferencia deberá utilizar un valor de 240.

Si una entidad H.323 simple puede tomar parte en llamadas múltiples, el valor utilizado para **terminalType** en el proceso de determinación principal-subordinado se basará en las características que la entidad H.323 haya asignado o vaya a asignar a la llamada en la que está siendo señalizada.

Un MC que ya esté actuando como MC seguirá siendo el MC activo. Por ello, una vez que un MC haya sido seleccionado como el MC activo de una conferencia utilizará el valor de MC activo en todas las conexiones subsiguientes con la conferencia.

Si no hay ningún MC activo y las entidades son del mismo tipo, la entidad H.323 con el conjunto de características más elevado (que se muestra en el cuadro 1) será la ganadora en la determinación principal-subordinado. Si no hay ningún MC activo y las entidades son de tipos diferentes, un MC que esté situado en una MCU tendrá prioridad con respecto a otro que se halle en un controlador de acceso, el cual tendrá prioridad sobre un MC situado en una pasarela, que a su vez tendrá prioridad sobre un MC situado en un terminal.

Si una entidad H.323 puede ser asociada con dos o más de las clasificaciones mostradas en el cuadro 1, debería utilizar el valor más elevado para el que esté calificada.

6.2.8.5 Valores de temporizador y contador

Todos los temporizadores definidos en la Rec. UIT-T H.245 deberían tener unos periodos de temporización por lo menos iguales al tiempo de entrega de datos máximo permitido por la capa de enlace de datos que lleva el canal de control H.245, incluyendo cualquier retransmisión.

El contador de reintentos N100 H.245 debería ser de al menos 3.

Los procedimientos relativos al tratamiento de errores de protocolo H.245 se analizan en 8.6.

6.2.8.6 Transmisión de trenes multiplexados sobre un único canal lógico

Es posible realizar la multiplexación de varios trenes de medios sobre un único canal lógico. Un tren multiplexado es un tren que contiene múltiples medios, para lo cual utiliza los protocolos de multiplexación H.222.0 [45] o H.223 [46], que se transmiten como una serie de paquetes del RTP. Utilizando estos protocolos de multiplexación, un punto extremo H.323 puede conseguir beneficios, tales como una utilización más eficiente de la anchura de banda, una sincronización precisa de medios o un retardo bajo en la transmisión multimedia.

Existen dos formas de controlar la configuración de un tren multiplexado. La primera forma consiste en transmitir los mensajes H.245 en los paquetes del RTP de los trenes multiplexados. En este caso, los puntos extremos H.323 abren, en primer lugar, canales lógicos bidireccionales para la transmisión del tren multiplexado utilizando el procedimiento H.245 de señalización de canal lógico, tal como se hace en el caso de trenes de medios normales del RTP. El control del tren multiplexado se realiza mediante los mensajes H.245 de los paquetes del RTP del tren multiplexado objetivo. El control del tren multiplexado incluye el intercambio de las capacidades de los códecs de medios disponibles para dichos trenes multiplexados, el intercambio de un cuadro de multiplexación y canales lógicos de apertura/cierre. Los números de los canales lógicos de un tren multiplexado son independientes de los de otros trenes multiplexados o de los de los canales lógicos H.245.

La segunda forma de controlar la configuración de un tren multiplexado es controlando los canales lógicos del tren multiplexado de la misma forma que se hace con los canales lógicos no multiplexados, es decir, los mensajes H.245 del tren multiplexado se transmiten de la misma forma que los restantes mensajes H.245. En este caso, un punto extremo H.323 abre un canal lógico unidireccional o bidireccional para la transmisión de trenes multiplexados utilizando el procedimiento de señalización de canal lógico H.245, tal como se hace con los trenes de medios normales del RTP. Los canales lógicos sobre el tren multiplexado se abren entonces utilizando la señalización de canal lógico con parámetros de configuración del protocolo de multiplexación y el número de canal lógico del tren de multiplexación sobre el que se abre el nuevo canal lógico.

6.2.8.6.1 Intercambio de capacidades relacionado con el tren multiplexado

Los terminales H.323 que soportan trenes multiplexados indican que tienen dicha capacidad incluyendo **MultiplexedStreamCapability** (**capacidad del tren multiplexado**) como parte de la capacidad del terminal. El parámetro **controlOnMuxStream** (**control de tren multiplexado**) de **MultiplexedStreamCapability** indica si el terminal soporta el control del tren multiplexado utilizando mensajes H.245 o utilizando los paquetes del RTP del propio tren multiplexado. Si **controlOnMuxStream** es VERDADERO, la capacidad de los códecs en el tren multiplexado puede ponerse a **capabilityOnMuxStream**. Si **capabilityOnMuxStream** no existe, el terminal realizará el procedimiento del intercambio de capacidades enviando los mensajes H.245 en los paquetes del RTP sobre el tren multiplexado una vez que se ha abierto el canal lógico del tren multiplexado. Si **controlOnMuxStream** es FALSO, la capacidad de los códecs en el tren multiplexado se pone a **capabilityOnMuxStream**.

6.2.8.6.2 Señalización del canal lógico para transportar un tren multiplexado

El canal lógico para el tren multiplexado se abre enviando un mensaje **openLogicalChannel** con el **dataType** (**tipo de datos**) de un tipo **MultiplexedStreamCapability** y **multiplexParameters** (**parámetros de multiplexación**) de **h2250LogicalChannelParameters** (**parámetros de canal lógico h2250**). Si **controlOnMuxStream** de **MultiplexedStreamCapability** es VERDADERO, el canal lógico se abre como canal lógico bidireccional, es decir, se fija **reverseLogicalChannelParameters**. En cualquier otro caso, el canal lógico puede abrirse como canal lógico unidireccional. Obsérvese que si el canal lógico se abre como unidireccional, puede que no se utilicen algunas de las funciones del protocolo de multiplexación, por ejemplo, AL3 de H.223 no puede utilizarse sobre canales lógicos unidireccionales.

El terminal no abrirá más de un canal lógico con **multiplexFormat** (**formato de múltiplex**) de **h223Capability** (**capacidad h223**) y con **controlOnMuxStream** FALSO.

6.2.8.6.3 Señalización del canal lógico para transportar un tren de medios sobre un tren multiplexado

El canal lógico del tren multiplexado se abre enviando un mensaje **openLogicalChannel** con el **dataType** adecuado al medio y con los **multiplexParameters** del protocolo de multiplexación utilizado (es decir, **h223logicalChannelParameters**). En el caso de H.223, también se realiza el procedimiento de señalización del cuadro de multiplexación antes o después de dicha señalización de canal lógico, tal como se describe en 6.4.2/H.324.

Si **controlOnMuxStream** es VERDADERO, los mensajes H.245 se entregan en los paquetes del RTP del tren multiplexado sobre el que se abre el nuevo canal lógico. En el caso de H.223, los **MultimediaSystemControlMessage** H.245 se protegen con el protocolo de retransmisión simple (SRP, *simple retransmission protocol*) y se entregan sobre el canal lógico 0 del tren multiplexado, tal como se describe en 6.5.4/H.324.

Si **controlOnMuxStream** es FALSO, los mensajes H.245 se entregan, como es normal, en el canal de control H.245. En el caso de H.222.0, el **resourceID** (**identificador de recurso**) de **h2220LogicalChannelParameters** toma el valor del número de canal lógico para el tren multiplexado sobre el que se abre este nuevo canal lógico. Obsérvese que en el caso de H.223, no es necesaria dicha señalización debido a que no existe más de un canal lógico.

Los canales lógicos sobre trenes multiplexados se cierran enviando mensajes **closeLogicalChannel**, que se transmiten de la misma forma que los mensajes **openLogicalChannel** del canal.

6.2.8.6.4 Señalización del canal lógico para el cierre del tren multiplexado

El canal lógico del tren multiplexado que se abre con el **controlOnMuxStream** puesto a VERDADERO, puede cerrarse en cualquier instante mediante el mensaje **closeLogicalChannel**. El canal lógico del tren multiplexado que se abre con el **controlOnMuxStream** puesto a FALSO, sólo se cerrará después de haber cerrado todos los canales lógicos del tren multiplexado.

6.2.9 Función de señalización RAS

La función de señalización RAS utiliza mensajes H.225.0 para llevar a cabo los procedimientos de registro, admisiones, cambios de anchura de banda, situación y liberación entre puntos extremos y controladores de acceso. El canal de señalización RAS es independiente del canal de señalización de llamada y del canal de control H.245. Los procedimientos de apertura de canal lógico H.245 no se utilizan para establecer el canal de señalización RAS. En los entornos de red que no tienen un controlador de acceso, no se utiliza el canal de señalización RAS. En los entornos de red que sí tienen un controlador de acceso (una zona), el canal de señalización RAS se abre entre el punto extremo y el controlador de acceso. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323. Este canal se describe de manera detallada en la cláusula 7.

6.2.10 Función de señalización de llamada

La función de señalización de llamada utiliza la señalización de llamada H.225.0 para establecer una conexión entre dos puntos extremos H.323. El canal de señalización de llamada es independiente del canal RAS y del canal de control H.245. Los procedimientos de apertura de canal lógico H.245 no se utilizan para establecer el canal de señalización de llamada. El canal de señalización de llamada se abre antes del establecimiento del canal H.245 y de cualquier otro canal lógico entre puntos extremos H.323. En los sistemas que no tienen un controlador de acceso, el canal de señalización de llamada se abre entre los dos puntos extremos que participan en la llamada. En los sistemas que sí tienen un controlador de acceso, el canal de señalización de llamada se abre entre el punto extremo y el controlador de acceso o entre los propios puntos extremos, según decida el controlador de acceso. Este canal se describe de manera detallada en la cláusula 7.

6.2.11 Capa H.225.0

Los canales lógicos de información de vídeo, audio, datos o control se establecen de acuerdo con los procedimientos de la Rec. UIT-T H.245. Los canales lógicos son unidireccionales e independientes en cada sentido de la transmisión. Algunos canales lógicos, tales como los de datos, pueden ser bidireccionales y están asociados mediante el procedimiento de apertura de canal lógico bidireccional de la Rec. UIT-T H.245. Se puede transmitir cualquier número de canales lógicos de cada tipo de medios, excepto en el caso del canal de control H.245 del que habrá uno por llamada. Además de los canales lógicos, los puntos extremos H.323 utilizan dos canales de señalización para el control de la llamada y las funciones relacionadas con el controlador de acceso. El formato dado a estos canales deberá ser conforme a la Rec. UIT-T H.225.0.

6.2.11.1 Números de canales lógicos

Cada canal lógico se identifica mediante un número de canal lógico (LCN, *logical channel number*), comprendido entre 0 y 65535, que sirve sólo para asociar los canales lógicos con la conexión de transporte. Los números de canal lógico son seleccionados de manera aleatoria por el transmisor, excepto el número 0 de canal lógico que estará permanentemente asignado al canal de control H.245. La dirección de transporte efectiva a la que el transmisor deberá transmitir será devuelta por el receptor en un mensaje **openLogicalChannelAck**.

6.2.11.2 Límites de la velocidad binaria de los canales lógicos

La anchura de banda de un canal lógico tendrá un límite superior especificado por el valor mínimo de la capacidad de transmisión del punto extremo (si está presente) y la capacidad de recepción del punto extremo receptor. En función de este límite, un punto extremo abrirá un canal lógico a una velocidad binaria igual o inferior a ese límite superior. Un transmisor transmitirá un tren de información dentro del canal lógico a cualquier velocidad binaria coincidente con, o inferior a, la velocidad binaria de apertura del canal lógico. El límite se aplica a los trenes de información que son el contenido del canal o los canales lógicos, sin incluir los encabezamientos RTP, los encabezamientos de la parte útil RTP, y los encabezamientos de red ni cualquier otra tara.

Los puntos extremos H.323 obedecerán al mensaje de **flowControlCommand** (**instrucción de control de flujo**) H.245, que establezca un límite a la velocidad binaria de un canal lógico o la velocidad binaria agregada de todos los canales lógicos. Los puntos extremos H.323 que deseen limitar la velocidad binaria de un canal lógico, o la velocidad binaria agregada de todos los canales lógicos, deberán enviar el mensaje **flowControlCommand** al punto extremo transmisor.

Cuando el terminal no tenga información que enviar por un canal determinado, no enviará información. No se enviarán datos de relleno por la red para mantener una velocidad de datos específica.

6.3 Características de la pasarela

La pasarela proporcionará la conversión adecuada entre formatos de transmisión (por ejemplo, H.225.0 a/de H.221) y entre procedimientos de comunicaciones (por ejemplo, H.245 a/de H.242). Esta conversión se especifica en la Rec. UIT-T H.246. La pasarela llevará a cabo además el establecimiento y la liberación de la llamada en el lado red y en el lado RCC. La conversión entre formatos de vídeo, audio y datos también puede efectuarse en la pasarela. Por lo general, la finalidad de la pasarela (cuando no funciona como una MCU), consiste en reflejar las características de un punto extremo de red a un punto extremo de RCC, y a la inversa, de manera transparente.

Un punto extremo H.323 puede comunicar con otro punto extremo H.323 de la misma red directamente y sin que participe en ello una pasarela. Se puede prescindir de la pasarela si no se requieren comunicaciones con terminales RCC (terminales no en la red). También es posible que un terminal de un segmento de la red llame al exterior a través de una pasarela y de nuevo a la red a través de otra pasarela para evitar un encaminador o un enlace de anchura de banda reducida.

La pasarela tiene las características de un terminal H.323 o una MCU de la red y del terminal RCC o una MCU de la RCC. La elección entre terminal o MCU se deja a criterios del fabricante. La pasarela proporciona la conversión necesaria entre los diferentes tipos de terminal. Hay que tener en cuenta que la pasarela puede funcionar al principio como un terminal, pero utilizando más tarde la señalización H.245 empieza a funcionar como una MCU para la misma llamada que inicialmente era punto a punto. Los controladores de acceso saben qué terminales son pasarelas ya que esto es algo que se indica cuando el terminal/la pasarela se registra en el controlador de acceso.

Una pasarela que transfiere datos T.120 entre la RCC y la red puede contener un proveedor de MCS T.120 que conecta a los proveedores de MCS T.120 de la red con los proveedores de MCS T.120 de la RCC.

En la figura 5 están representados cuatro ejemplos de pasarela H.323. Los diagramas muestran la función de terminal H.323 o MCU, la función de terminal RCC o MCU y la función de conversión. La función de terminal H.323 tiene las características descritas en 6.2. La función de MCU H.323 tiene las características descritas en 6.5. La pasarela tiene para los otros terminales H.323 de la red la apariencia de uno o más terminales H.323 o una MCU H.323. Comunica con los demás terminales H.323 utilizando los procedimientos de la presente Recomendación.

El terminal RCC o función de MCU tiene las características descritas en la Recomendación correspondiente (H.310, H.320, H.321, H.322, H.324 y V.70 y los terminales sólo vocales de la RTGC o la RDSI). La pasarela tiene para los terminales RCC la apariencia de uno o más terminales o MCU del mismo tipo. Comunica con otro terminal RCC utilizando los procedimientos descritos en la Recomendación correspondiente a ese terminal. Quedan fuera del alcance de la presente Recomendación los procedimientos de señalización de RCC, incluidos temas tales como la apariencia que tiene la pasarela H.323 para la RCC, ya sea la de un terminal o la de una red. Obsérvese que una pasarela puede convertir H.323 directamente en H.324 o H.310 sin tener que ir a H.320.

Las pasarelas que soportan el interfuncionamiento con terminales sólo vocales de la RTGC o la RDSI deberían generar y detectar señales de multifrecuencia bitono (DTMF) correspondientes a las **userInputIndications** H.245 para 0-9, ∗ , y #. Además, las pasarelas pueden generar y detectar señales de DTMF, tonos de telefonía y señales telefónicas correspondientes a estos eventos transportados con un tipo de parte útil RTP especial, como se describe en 10.5.

La función de conversión proporciona la conversión necesaria de formato de transmisión y trenes de control, audio, vídeo y/o datos entre las diferentes Recomendaciones de terminales. Como mínimo, la pasarela deberá proporcionar una función de conversión del formato de transmisión, las señales y procedimientos de establecimiento de la comunicación y las señales y procedimientos del control de las comunicaciones. Cuando se requiera, la pasarela permitirá la conversión de H.242 a H.245. La pasarela efectúa la conversión apropiada entre la señalización de llamada H.225.0 y el sistema de

señalización de la RCC (Q.931, Q.2931, etc.). La conversión entre mensajes de señalización de llamada H.225.0 de la red y mensajes Q.931 de la RCC se describe en la Rec. UIT-T H.246.

Toda señalización de llamada recibida por la pasarela procedente de un punto extremo de RCC y no aplicable a la pasarela se transferirá a través del punto extremo de red y viceversa. Dicha señalización incluye, de manera no exhaustiva los mensajes de Q.932, Q.950 y H.450. Los puntos extremos H.323, podrán así implementar los servicios suplementarios definidos en esas Recomendaciones. El tratamiento de otros sistemas de señalización de llamada de RCC queda en estudio.

Esta Recomendación describe la conexión de un terminal H.323 de la red a un terminal externo de la RCC a través de la pasarela. El número efectivo de terminales H.323 que pueden comunicar a través de la pasarela no está sujeto a normalización. De manera similar, el número de conexiones de la RCC, el número de conferencias independientes simultáneas, las funciones de conversión de audio/vídeo/datos y la inclusión de funciones multipunto se deja a criterio del fabricante. Si la pasarela incluye una función de MCU en el lado red, dicha función deberá ser una MCU H.323 en el lado red. Si la pasarela incluye una función de MCU en el lado RCC, puede tener la apariencia de una MCU H.231/H.243, o de una MCU para sistemas H.310 o H.324 (en las correspondientes Recomendaciones se indica que estas MCU quedan en estudio) en el lado RCC.

Una pasarela puede conectarse a través de la RCC con otras pasarelas para facilitar la comunicación entre terminales H.323 que no están en la misma red.

Los equipos que proporcionan la interconexión transparente entre las redes sin utilizar protocolos de la serie H (tales como los encaminadores y las unidades de marcación de entrada a distancia) no son pasarelas según lo definido en el marco de la presente Recomendación.

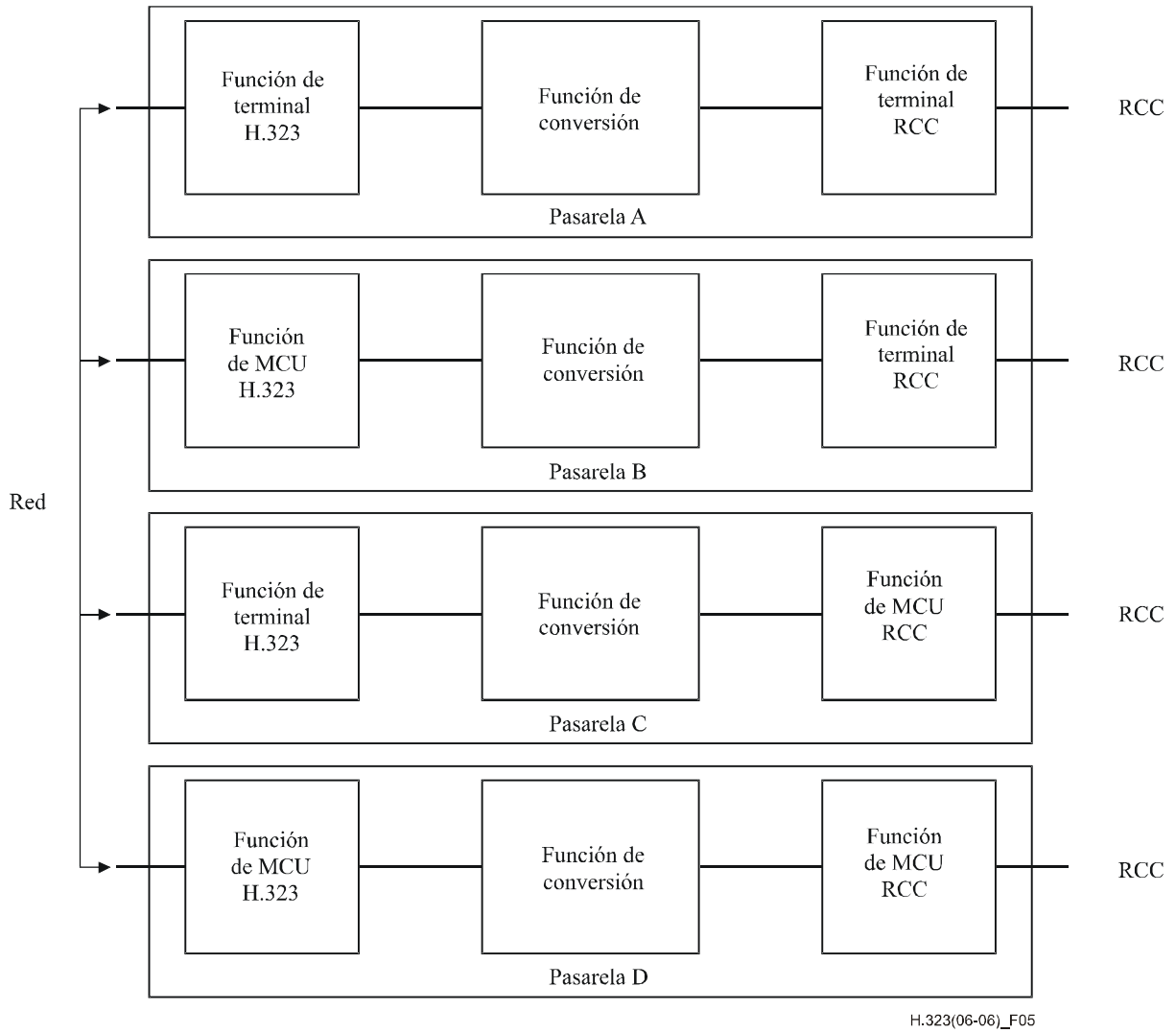


Figura 5/H.323 – Configuraciones de pasarela H.323

6.3.1 Descomposición de la pasarela

En esta cláusula se identifica un grupo de funciones e interfaces que han de utilizarse para descomponer las pasarelas H.323. Se tratan cada una de las interfaces y de los protocolos resultantes, pero algunas implementaciones de pasarela pueden agrupar dos o más componentes funcionales en un único dispositivo físico. Por este motivo, las interfaces pueden proveer la capacidad de soportar de forma transparente otros protocolos.

En la figura 6, la componente de medios de paquetes/circuitos termina el canal de medios de RCC y convierte los flujos en medios basados en paquetes en la interfaz con la red por paquetes. La interfaz A representa el protocolo de control de dispositivo que se define en la Rec. UIT-T H.248.1, utilizado para la creación, modificación y supresión de conexiones de medios de la pasarela. La componente de la lógica de control realizará el interfuncionamiento de señalización entre los lados RCC y H.323 de la pasarela.

La interfaz B representa las componentes de los protocolos H.225.0 y H.245 que conforman las interfaces de señalización H.323 en el lado de paquetes de la pasarela.

La interfaz C describe la función de control de llamada RDSI entre los servicios de la señalización asociada la facilidad (FAS) de la RCC y la lógica de control de la pasarela. La interfaz D es un protocolo que transporta la señalización no asociada a la facilidad (NFAS) de la RCC al controlador. Esta descomposición proporciona la flexibilidad necesaria para conservar los puntos de señalización del SS7 y permitir que los conmutadores del SS7 puedan atender a varios controladores de pasarelas descompuestas.

Los elementos de control de recursos diferencian entre una comprensión de alto nivel de los recursos en el controlador de la pasarela y una comprensión de bajo nivel de los recursos en un dispositivo de la pasarela.

Las interfaces de la RCC se describen como interfaces de bajo nivel que transportan la señalización y una terminación de señalización de la RCC de alto nivel con una interfaz con el controlador de la pasarela. Puede tratarse de señalización FAS, tal como el acceso primario RDSI, o NFAS, como el SS7.

La figura 6 no representa una descomposición física. El reto que se presenta a los suministradores de pasarelas es agrupar todos estos componentes en dispositivos físicos e implementar las interfaces asociadas para conseguir producir pasarelas H.323 escalables y multisuministrador. La interfaz X es la interfaz H.323 externa, la interfaz Y es la interfaz con el medio por paquetes externo (es decir, el RTP) y la interfaz Z es la interfaz de la RCC externa.

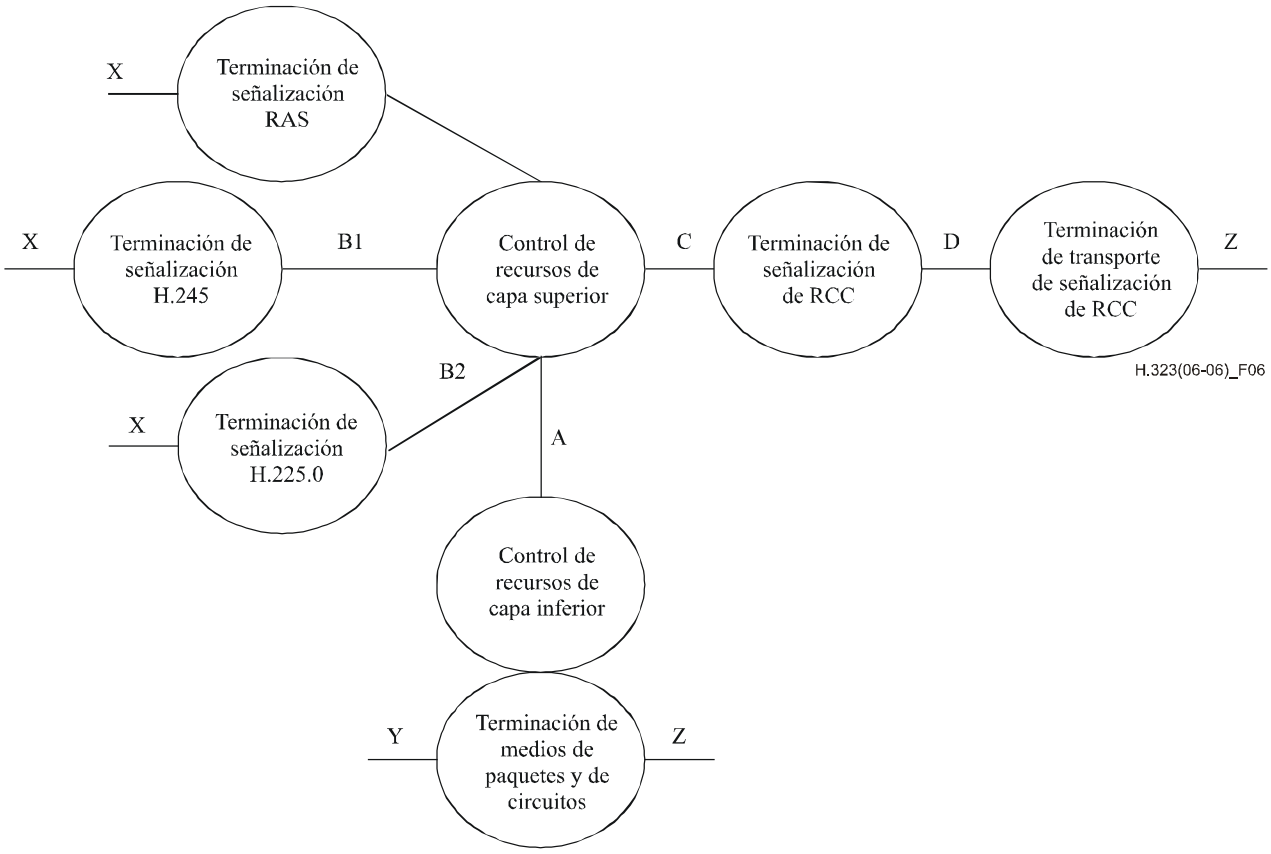


Figura 6/H.323 – Arquitectura funcional de una pasarela descompuesta

6.3.1.1 Descomposiciones físicas

En esta cláusula se describen ejemplos de posibles descomposiciones de pasarelas y de interfaces internas que son necesarias. En todos los casos, las interfaces externas, tales como la H.323 y la RCC, permanecen inalteradas. La parte del controlador de la pasarela física se denomina controlador de pasarela de medios (MGC, *media gateway controller*). Las funciones del MGC son las siguientes:

- maneja mensajes RAS H.225.0 con un controlador de acceso externo;
- opcionalmente, maneja la interfaz de señalización SS7;
- opcionalmente, maneja la interfaz de señalización H.323.

La componente pasarela de medios (MG, *media gateway*):

- termina la interfaz de la red IP;
- termina la parte de la red RCC;
- puede manejar señalización H.323 en algunas descomposiciones físicas;
- puede manejar la señalización FAS RCC en algunas descomposiciones físicas.

Las pasarelas descompuestas no realizan todas las interfaces, pero la división entre MGC y MG, en la cual se hace patente la interfaz A, es obligatoria de todas las descomposiciones. Ello permite que un MGC controle distintos tipos de MG que pueden estar optimizadas para ciertas aplicaciones (por ejemplo, pasarelas H.320/H.323 de voz o multimedia). La descomposición de las interfaces B y C en la MG, que puede exigir un protocolo para soportar la señalización entre la MG y el MGC, queda en estudio.

La MG termina los medios IP o ATM en el lado de la red de paquetes y los canales portadores en las interfaces de red de la RCC. El lado de paquetes puede ser una interfaz IP, ATM, o de red ATM en la que los paquetes de audio y vídeo atraviesan conexiones ATM nativas de acuerdo con el anexo C.

El MGC y la MG distinguen entre elementos de gestión de recursos de bajo nivel y de alto nivel. El MGC es responsable de la gestión de recursos de alto nivel, con conocimiento de la disponibilidad de los recursos, tales como los compensadores de eco, pero sin realizar la asignación de recursos específicos a sesiones de pasarela concretas. La MG es responsable de la gestión y asignación de recursos de bajo nivel, así como de las manipulaciones del soporte físico necesarias para conmutar y procesar trenes de medios en la pasarela de medios.

6.3.1.1.1 Pasarelas SS7 separadas

En la figura 7 se representa una posible descomposición de pasarela en el caso de una pasarela entre PU-RDSI y H.323, en la que las funciones de pasarela SS7, MGC y MG se descomponen en dispositivos físicos separados. Esta disposición muestra claramente una interfaz D de transporte de señalización PU-RDSI y la interfaz A de control de dispositivos.

Para facilitar la interoperabilidad, las configuraciones de pasarela descompuesta deben soportar la interfaz A y contener señalización H.323 y RCC internas en el MGC.

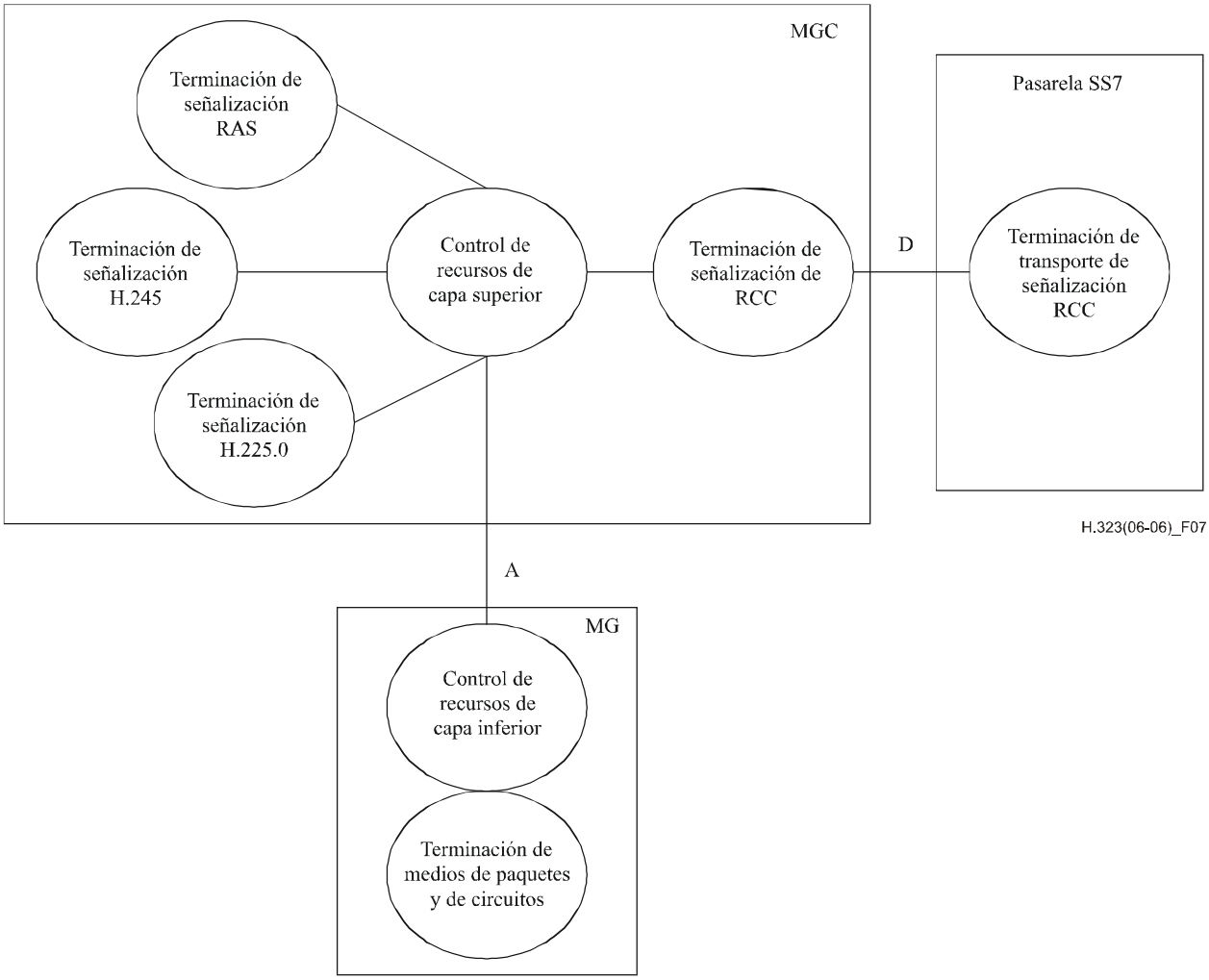


Figura 7/H.323 – Descomposición de la pasarela SS7

6.3.1.1.2 Descomposición de pasarela FAS

La descomposición de pasarela que se muestra en la figura 8 aísla los servicios FAS RCC, tales como el acceso primario RDSI en la MG, y mantiene la señalización H.323 en el MGC. Ello deja al descubierto las interfaces C y A entre la MG y el MGC.

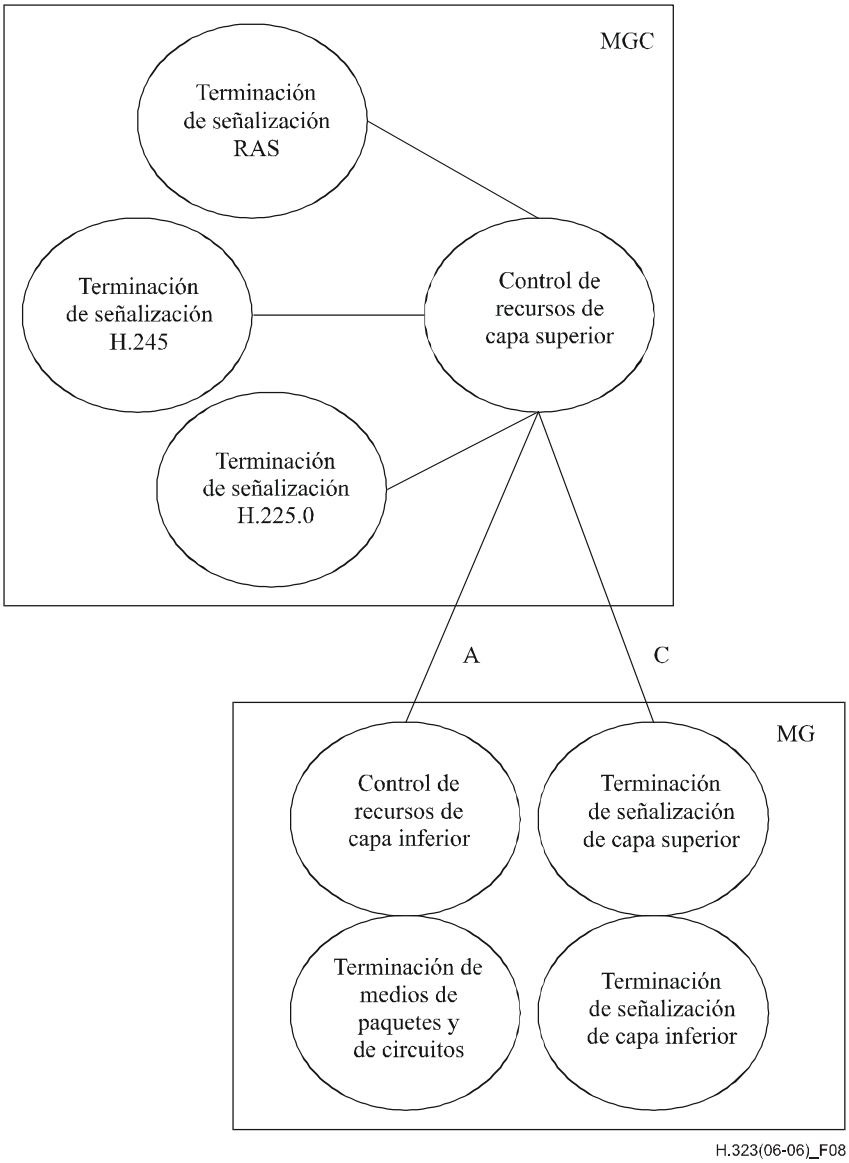


Figura 8/H.323 – Pasarela FAS con señalización H.323 en la MG

6.3.1.1.3 Pasarela SS7 con señalización H.323 en la MG

La descomposición que se muestra en la figura 9 se basa en la interfaz SS7 del MGC y desarrolla la señalización H.323 en la MG mostrando las interfaces D, A y B.

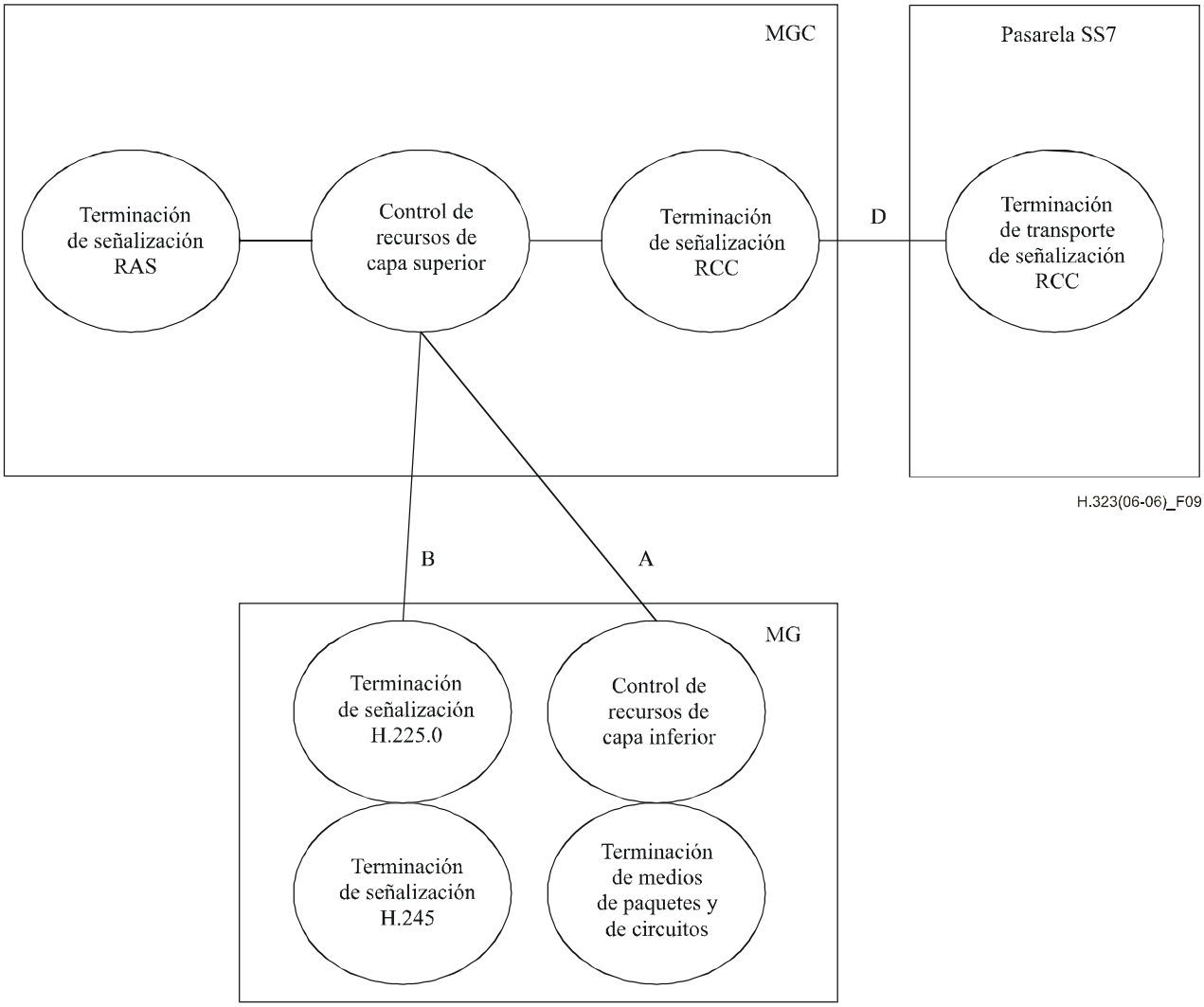


Figura 9/H.323 – SS7 terminada en una pasarela de medios

6.3.1.1.4 Señalización FAS y H.323 en la pasarela de medios

Existen determinados requisitos para las pasarelas H.320, descompuestas de tal forma en la MG, están presentes las señalizaciones H.323 y RCC, junto con las terminaciones de paquetes y circuitos. En esta descomposición, la MG maneja la señalización y las notificaciones de eventos se comunican al MGC (véase la figura 10).

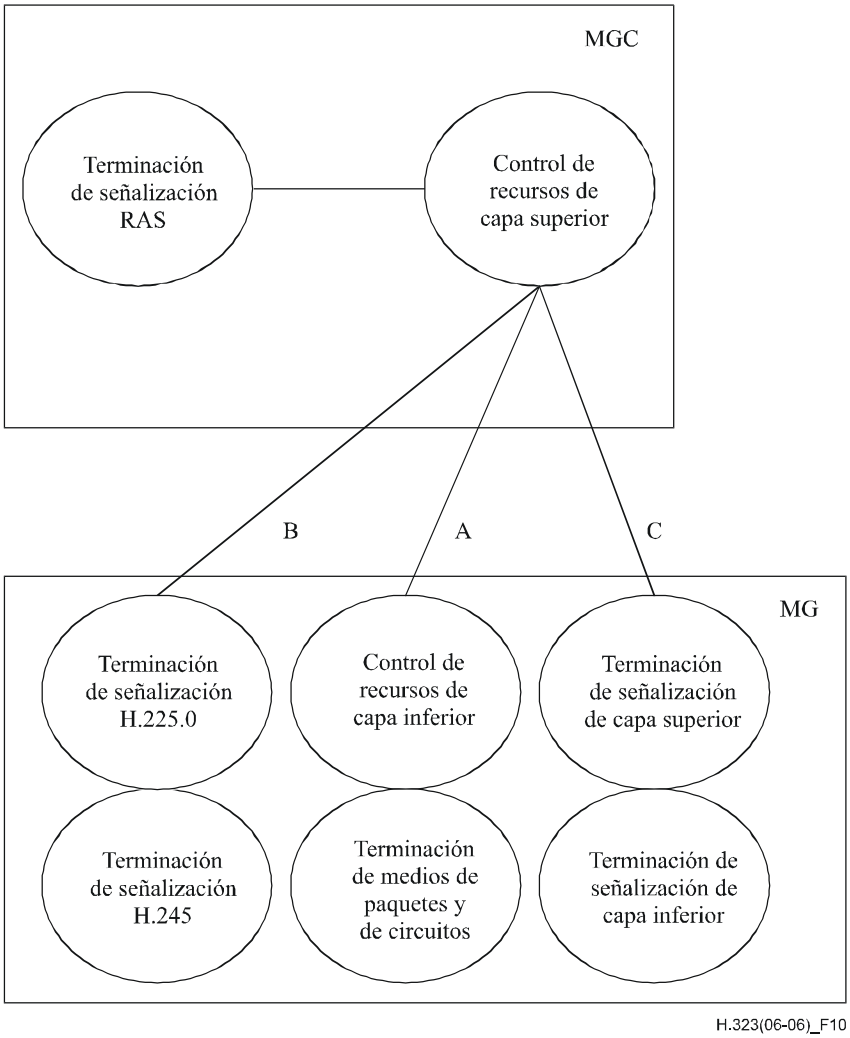


Figura 10/H.323 – Señalización FAS y H.323 en la MG

6.3.1.1.5 SS7 en la pasarela de medios

La descomposición que se muestra en la figura 11 termina la red SS7 en la MG y muestra la interfaz D entre el MGC y la MG.

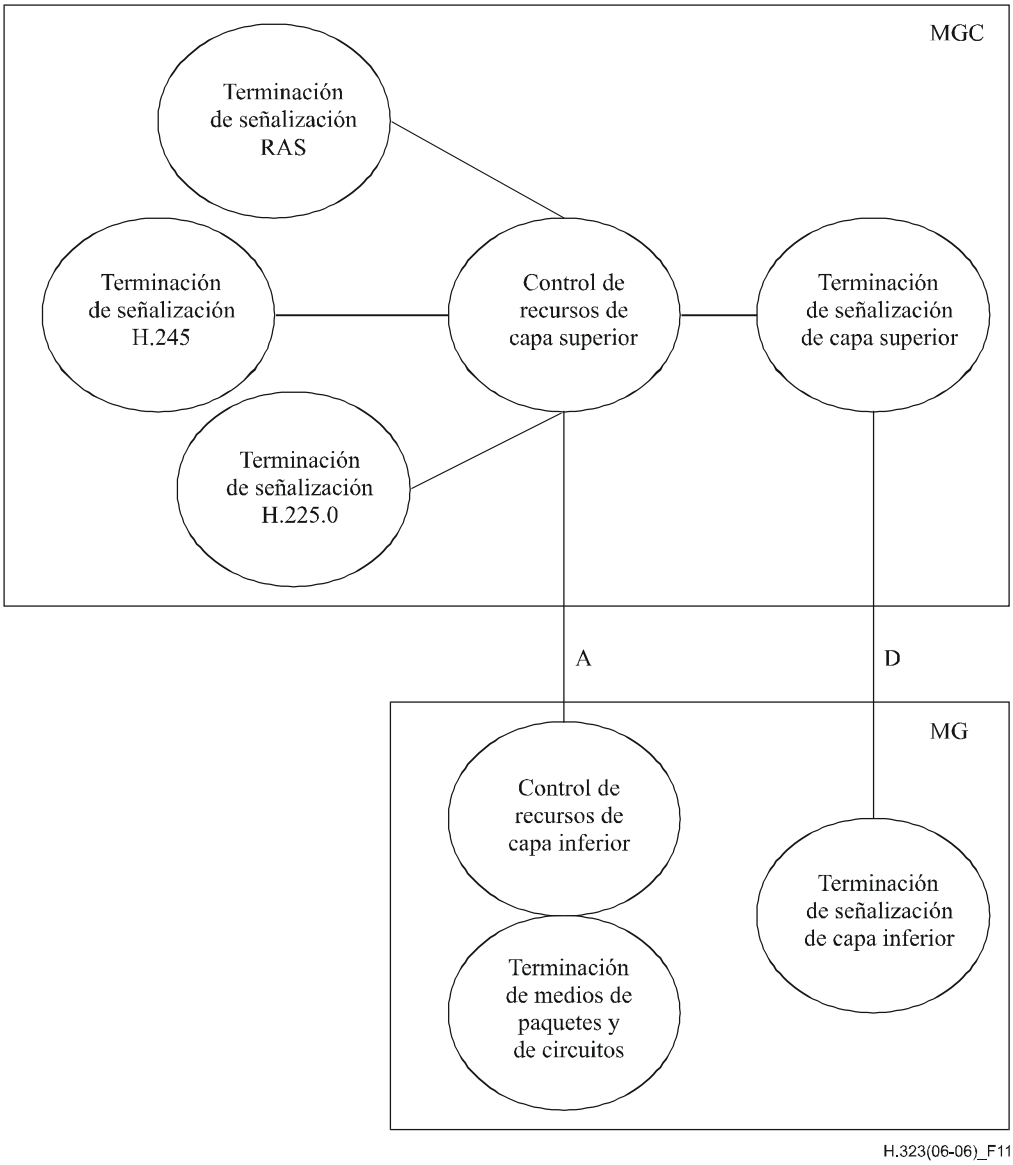


Figura 11/H.323 – SS7 terminada en la MG

6.3.2 Aplicaciones de la pasarela

Existen muchas aplicaciones para pasarelas descompuestas y pasarelas compuestas. Los vendedores y/o los operadores, pueden decidir utilizar una pasarela compuesta o descompuesta en función de los requisitos de la aplicación. La Rec. UIT-T H.248 establece que las pasarelas descompuestas deben interfuncionar con las pasarelas compuestas.

En esta cláusula se analiza vocabulario técnico que comparten los equipos H.323, la RCC y H.248. También proporciona ejemplos de pasarelas de aplicaciones. No pretende ser una lista exhaustiva de todas las aplicaciones. Tampoco pretende ilustrar la única forma en la que pueden soportarse dichas aplicaciones. En esta cláusula, los términos MG, MGC y GW representan ejemplificaciones físicas de dichos dispositivos.

6.3.2.1 Visión general de las pasarelas de la red troncal y de acceso

Los términos pasarela troncal y pasarela de acceso se emplean en H.323 y H.248, y son también parte de la terminología de la conmutación de circuitos, en la que se aplican a las centrales tándem (también denominadas troncales o de tránsito) y a las centrales de acceso. Dado que las mismas palabras se utilizan para significar cosas distintas en el contexto de tres arquitecturas diferentes, este apartado pretende clarificar la diversidad terminológicas.

6.3.2.1.1 Terminología de la RCC

En la RCC, una central "tándem" o "troncal" es una central de conmutación que conecta redes utilizando un protocolo NNI, tal como el SS7/PU-RDSI o un protocolo NNI CAS. Una central de "acceso" es una central que tiene conexiones de usuario utilizando BRI/PRI y que también está conectada mediante protocolos NNI a una red mayor. Una central "mixta" puede tener ambas funciones.

6.3.2.1.2 Terminología H.323

En las redes H.323, una pasarela "troncal" es una pasarela que proporciona una verdadera función tándem que es transparente a las redes conectadas. Dichas redes pueden ser redes SS7, redes QSIG u otras redes. Sin embargo, en todos los casos se utiliza la tunelización para crear una transparencia total y una verdadera función tándem. Se considera que el interfuncionamiento entre elementos PU-RDSI tiene lugar fuera de la red H.323. La tunelización se basa en la negociación del protocolo H.225.0 y en el anexo M.

Una pasarela de "acceso" H.323 proporciona una función de interfuncionamiento con otra red, empresa o punto extremo para los que no es completamente transparente. Los protocolos que interfuncionan pueden incluir los siguientes:

- SS7/PU-RDSI, utilizando el anexo C/H.246;
- QSIG utilizando H.450;
- H.320 utilizando el anexo A/H.246.

Debe notarse que la pasarela "troncal" H.323 y la central "tándem" de la RCC realizan la misma función, pero que la "pasarela de acceso" H.323 y la "central de acceso" de la RCC realizan misiones muy distintas. Un aspecto concreto sobre el que suele haber confusión es el hecho de que H.225.0 actúe como señalización UNI y NNI en una red H.323, realizando tanto el papel de PU-RDSI como de la RDSI (BRI/PRI) de la RCC. La Rec. UIT-T H.323 no hace distinción entre señalización UNI y NNI que se hace en la RCC, y la señalización de una llamada es la misma con independencia de si se establece directamente entre puntos extremos o bien con la mediación de elementos de red, como un controlador de acceso H.323 o un elemento de frontera (BE, *border element*).

En la figura 12 se resumen los aspectos anteriores y se muestra la relación entre los dominios H.323, que tienen algunas características similares a las que presentan las redes RCC. No obstante, es importante tener presente que también se utiliza H.225.0 para señalización de llamadas, ya sean éstas entre terminales, zonas o dominios. Además, las zonas y los dominios son más virtuales que físicos y aunque las centrales de conmutación (por ejemplo, conmutadores ATM utilizados para encaminar tráfico IP) pueden estar presentes, no son visibles por encima de la capa IP en la red de paquetes.

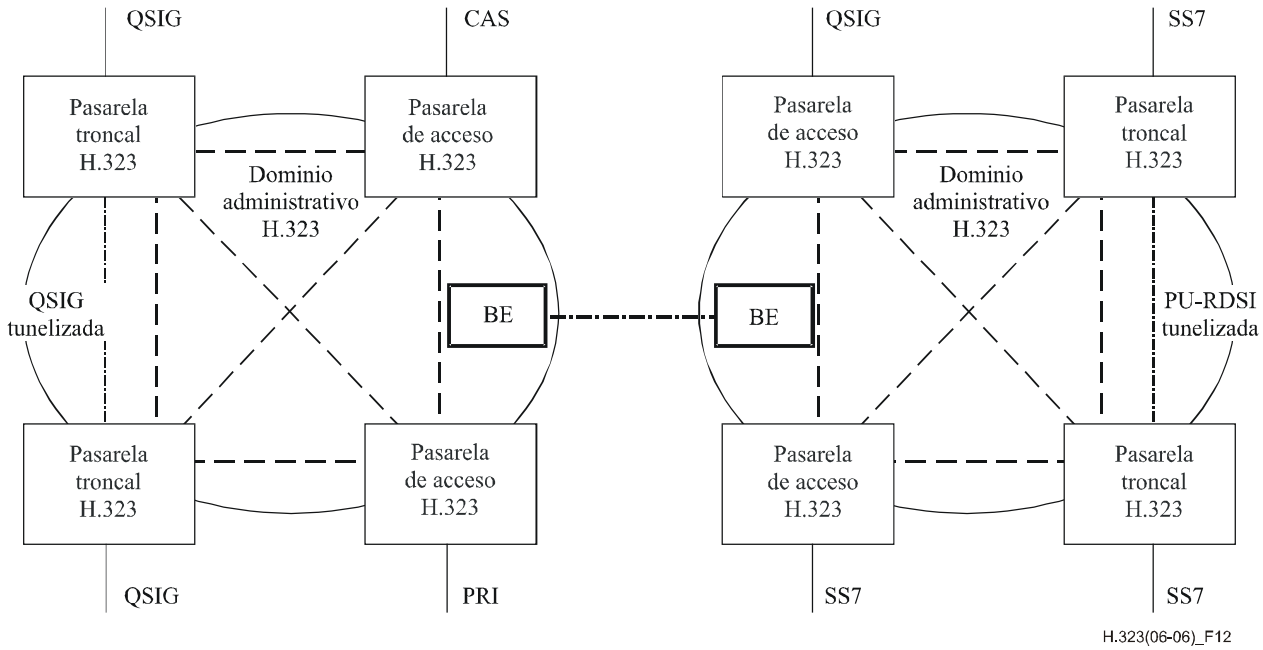


Figura 12/H.323 – Relación entre pasarelas H.323, RCC y H.248

6.3.2.1.3 Terminología H.248

En la Rec. UIT-T H.248.1 también se utilizan los términos pasarela "troncal " y de "acceso". Dado que los dispositivos H.248 pueden considerarse simplemente como descomposiciones en MGC y MG de pasarelas compuestas H.323, se supone que los MGC soportan H.323 e interfuncionan utilizando H.225.0, como hace cualquier otra pasarela H.323, incluyendo la tunelización de la PU-RDSI, etc. Sin embargo, desde una perspectiva descompuesta, los términos tienen significados ligeramente distintos. Una pasarela "troncal" es aquella en la que la señalización se conecta directamente al MGC, es decir, PU-RDSI, mientras que una pasarela de "acceso" es aquella en la que la señalización llega a la MG, y desde ella se pasa al MGC mediante H.248. Es importante señalar que aunque un pasarela de "acceso" puede soportar un protocolo UNI, también puede soportar protocolos CAS NNI, de modo que no es exacto definir una pasarela de "acceso" H.248 como una pasarela que soporta una interfaz UNI.

En la figura 13 se ilustra la arquitectura de la Rec. UIT-T H.248.1. Debe notarse que, tal como se ilustra, las pasarelas compuestas H.323 se utilizan a menudo como pasarelas de "acceso" en sistemas H.248. El diagrama muestra un MGC H.248 y un controlador de acceso H.323 coubicados.

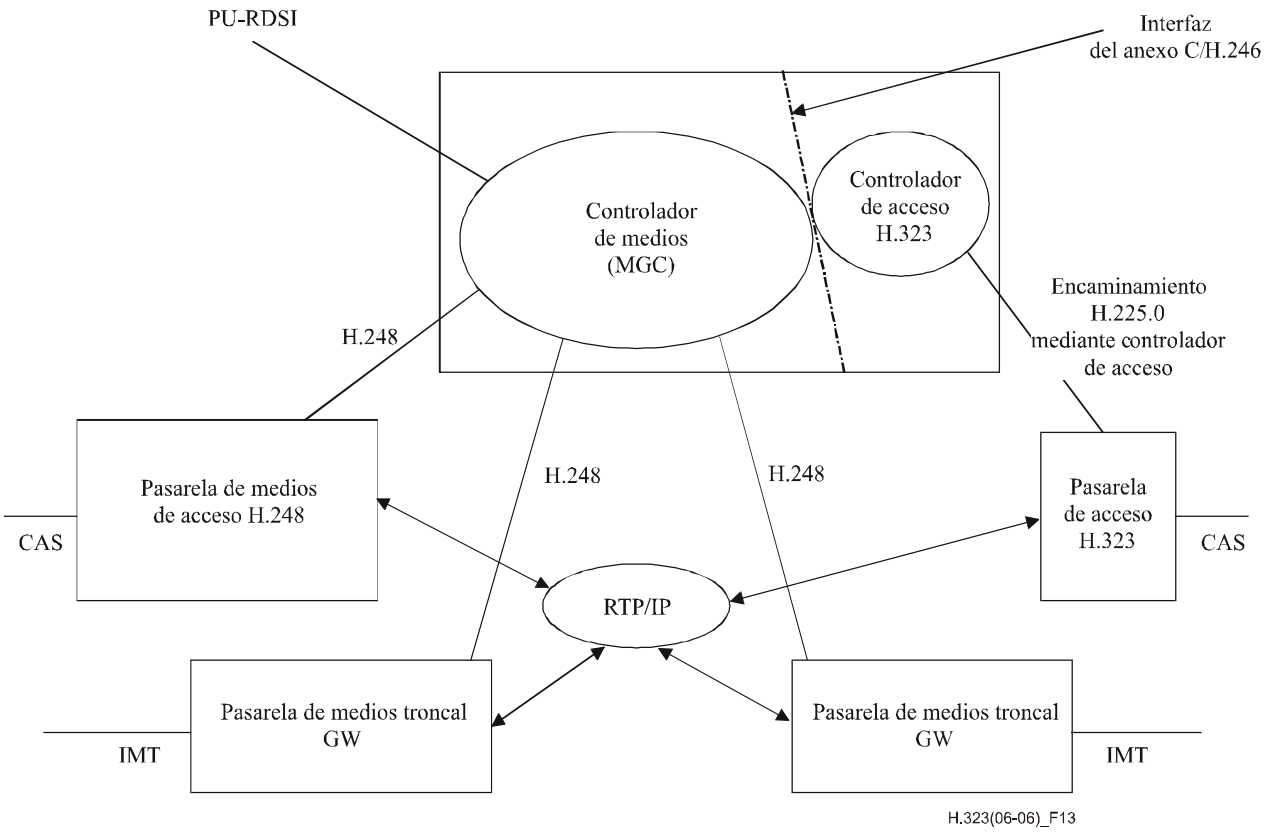


Figura 13/H.323 – Relaciones entre H.323 y H.248

6.3.2.2 Pasarelas troncales de un proveedor de servicios

En la figura 14 se muestra un ejemplo de una llamada que se encamina a través de una red con conmutación de paquetes entre las pasarelas troncales de dos proveedores de servicio. En esta aplicación, la red de paquetes actúa para el proveedor de servicios como una red de voz tándem. La interfaz A se utiliza para el control de las pasarelas de medios (MG). La conexión entre la red de paquetes y la red con conmutación de circuitos se realiza mediante señalización SS7 y enlaces entre centrales. En la figura 14 se ilustra el caso en el que los enlaces A de señalización SS7 se utilizan para establecer la conexión con la red SS7. En este caso, el MGC termina los enlaces de señalización directamente, en lugar de hacerlo a través de la pasarela de señalización. Los MGC se intercambian la información de señalización utilizando la interfaz X (por ejemplo, mediante la tunelización de la PU-RDSI en una conexión H.225.0). El tráfico de voz de establece entre ambas pasarelas.

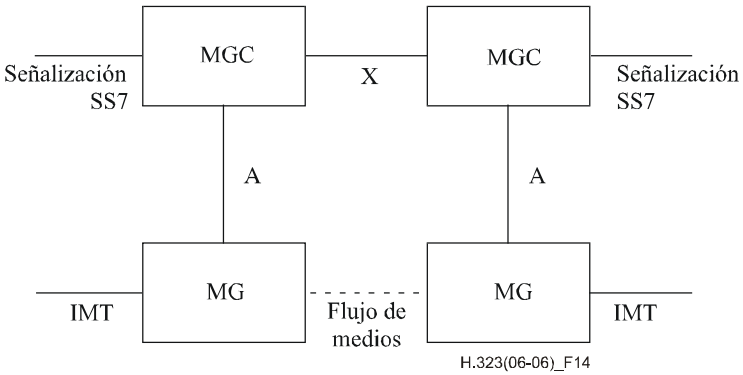


Figura 14/H.323 – Dos pasarelas troncales descompuestas de sendos proveedores de servicios

6.3.2.3 Pasarelas de acceso de proveedor de servicio

En la figura 15 se representa un ejemplo de llamada encaminada a través de una red con conmutación de paquetes entre una pasarela de acceso H.323 compuesta de un proveedor de servicio y una pasarela troncal descompuesta de otro proveedor de servicio. En esta aplicación, el proveedor de servicio facilita una interfaz de señalización asociada al canal para un sistema PBX de empresa que curse su tráfico de voz sobre la red del proveedor. Entre la pasarela compuesta y la pasarela descompuesta se utiliza la señalización de llamada H.225.0. El MGC realiza la adecuada señalización SS7 para la comunicación con la red SS7 y la RCC del proveedor de servicio. En este ejemplo, X es H.225.0 y el MGC implementa la función de interfuncionamiento del anexo E/H.246.

Aunque existen Recomendaciones que describen el interfuncionamiento entre varios protocolos, tales como PU-RDSI y H.323, los proveedores de servicio y los fabricantes deben evaluar cuidadosamente cuando resulta adecuado realizar dicho interfuncionamiento y el número de puntos de interfuncionamiento. El interfuncionamiento puede no producir una traducción perfecta entre los dos protocolos, y la ocurrencia de múltiples traducciones produce una pérdida de transparencia.

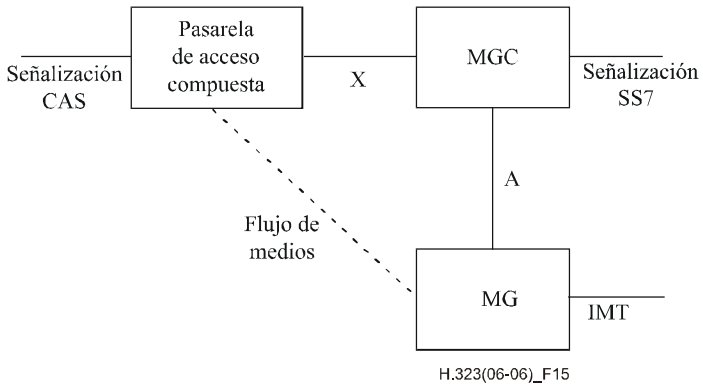


Figura 15/H.323 – Pasarela de acceso compuesta y pasarela troncal descompuesta

En la figura 16 se ilustra la misma aplicación, en la cual la pasarela de acceso del proveedor de servicio también está descompuesta. En este caso, la interfaz A se utiliza para controlar la señalización asociada al canal. Los MGC se comunican entre sí mediante la interfaz X. En este caso concreto, no existen enlaces de conexión entre la MG y el MGC, la cantidad de información sobre la llamada que está disponible para el MGC se limita la definida en la Rec. UIT-T H.248.1. En este ejemplo, X es H.225.0 y el MGC del lado derecho realiza el interfuncionamiento con la PU-RDSI del anexo E/H.246.

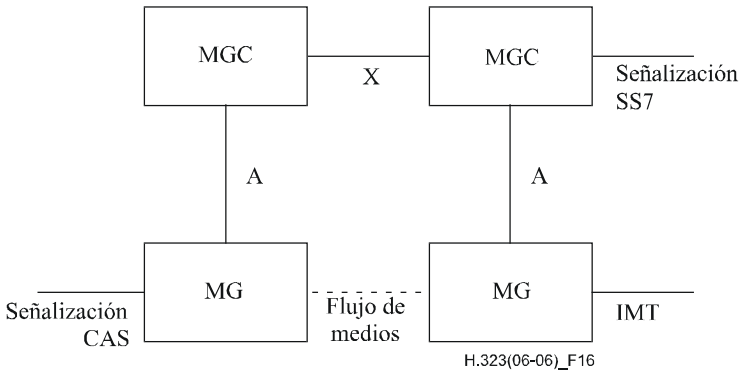


Figura 16/H.323 – Pasarelas troncal y de acceso descompuestas del proveedor de servicio

Cuando se considera cuáles de estos enfoques puede ser el mejor para una aplicación en concreto, se deben tener en cuenta los factores siguientes:

- número de líneas que se deben conectar;
- coste de los enlaces troncales;
- aspectos relativos a la homologación;
- capacidad del MGC;
- número de pasarelas de acceso en relación con el de pasarelas troncales;
- tipo de protocolos CAS que se soportan;
- arquitectura de procesamiento de la llamada del proveedor de servicio;
- diseño de la red.

Para las pasarelas de acceso, el entorno de aplicación determinará si lo más adecuado es una pasarela descompuesta, un terminal H.323 que utilice H.450.x, un terminal de estímulo anexo L o una pasarela compuesta.

6.3.2.4 Pasarelas troncales de empresas

En la figura 17 se ilustra una pasarela de empresa utilizada entre las PBX de una red de voz privada. Para la conexión de las PBX se utiliza una red de paquetes en lugar de una red de circuitos arrendados. En este caso, se utiliza QSIG para la señalización entre las PBX. Dado que QSIG es un tipo de señalización asociada a la facilidad, pueden establecerse conexiones para la señalización entre la pasarela de medios y el controlador de pasarela de medios a través de la interfaz C. La interfaz A se utiliza entre el MGC y la MG para el control de la pasarela. Los MGC se comunican entre sí a través de la interfaz X, que puede ser QSIG con tunelización H.225.0 de acuerdo con el anexo M1.

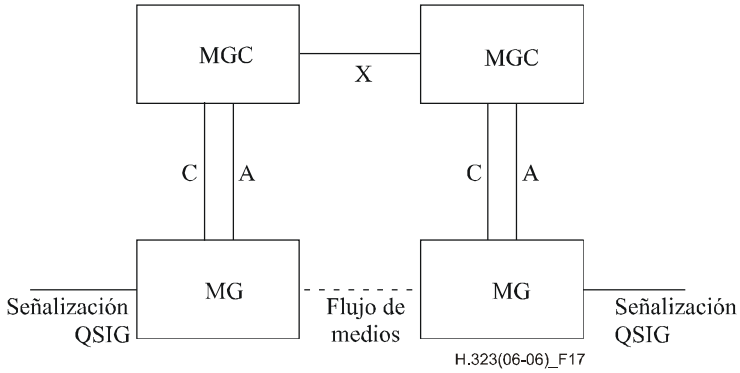


Figura 17/H.323 – Pasarelas troncales de empresa descompuestas

En la figura 18 se ilustra el caso de utilización de pasarelas entre PBX en una red de voz privada. Para la conexión de las PBX se utiliza la red de paquetes en lugar de las líneas arrendadas. En este caso, también se utiliza QSIG para la señalización entre las PBX. Sin embargo, se utiliza la tunelización de QSIG sobre la interfaz X para transportar la señalización QSIG entre una pasarela compuesta y una pasarela descompuesta. También pueden utilizarse otras combinaciones, tales como compuesta-compuesta y descompuesta-descompuesta.

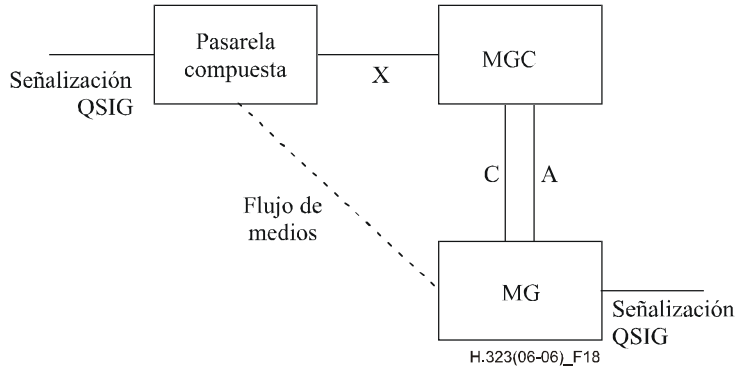


Figura 18/H.323 – Ejemplo de tunelización QSIG

6.3.2.5 Conexión de la empresa a la pasarela de acceso del proveedor de servicio

En algunos casos, una red H.323 de empresa se comunica con la RTPC a través de una pasarela descompuesta. Ello se ilustra en la figura 19. En este caso, la pasarela descompuesta se comunica con los puntos extremos H.323 a través de señalización H.323 (H.225, H.245, etc.). La pasarela descompuesta conecta con la RTPC a través de un PRI de la RDSI. Pueden establecerse conexiones para la señalización del canal D a través de la interfaz C.

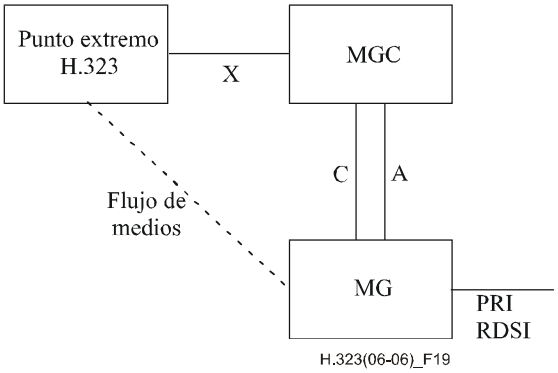


Figura 19/H.323 – Pasarela descompuesta y punto extremo H.323

Otras aplicaciones de acceso de empresas utilizan H.248 para la gestión de terminales, pero la apariencia es la de conexiones de pasarela compuesta a pasarela compuesta en otra ubicación, tal como se muestra en la figura 20. En este ejemplo, se utiliza H.450.x para proporcionar el interfuncionamiento de servicios suplementarios.

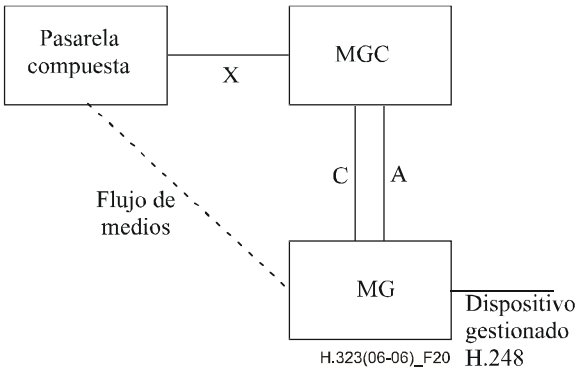


Figura 20/H.323 – Pasarela compuesta y dispositivos gestionados H.248

Una aplicación adicional de acceso para empresas utiliza anexo L para la gestión de terminales, pero tiene la apariencia de una conexión entre pasarelas compuestas en distintas ubicaciones, tal como se muestra en la figura 21. En este ejemplo, se puede utilizar H.450.x para proporcionar el interfuncionamiento entre servicios suplementarios. En este ejemplo, X1 es H.225.0 con H.450, mientras que X2 es H.225.0 con señalización de estímulo anexo L.

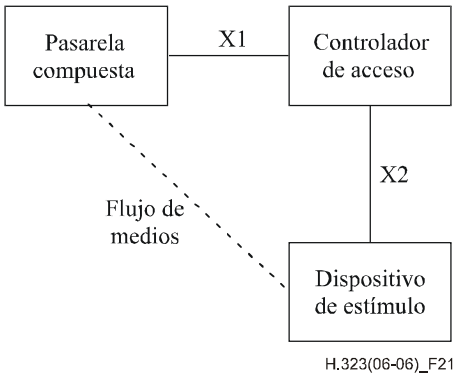


Figura 21/H.323 – Pasarela compuesta y dispositivo anexo L

Obsérvese que los terminales anexo L de la figura 21 pueden interfuncionar con los terminales gestionados H.248 de la figura 20 utilizando H.450.x. Estas configuraciones permiten una amplia capacidad de innovación en cuanto a las características que puede utilizar la empresa, al tiempo que soportan la interoperabilidad entre empresas utilizando H.450.x. Obsérvese que la señalización de llamada encaminada por el controlador de acceso de la figura 21 se utiliza en el controlador de acceso de la empresa que gestiona los terminales anexo L, a pesar de que las restantes pasarelas de la empresa pueden utilizar el modelo de llamada directa y tener un controlador de acceso distinto.

6.4 Características del controlador de acceso

El controlador de acceso, que es opcional en un sistema H.323, presta servicios de control de llamada a los puntos extremos H.323. Puede haber más de un controlador de acceso que se comunican entre sí de una manera no especificada. El controlador de acceso está separado lógicamente de los puntos extremos. Sin embargo, su implementación física puede coexistir con un terminal, MCU, pasarela, MC u otro dispositivo de red no H.323.

En cada zona y cada momento sólo puede haber un controlador de acceso, aunque pueden existir muchos dispositivos que proporcionen la función de controlador de acceso en una zona. Los dispositivos que proporcionan la función de señalización RAS para el controlador de acceso se denominan controladores de acceso alternos. Cada controlador de acceso alterno puede aparecer ante los puntos extremos como un controlador de acceso distinto. La comunicación entre controladores de acceso alternos y otros dispositivos que proporcionan la función de controlador de acceso para la zona en cuestión queda fuera del alcance de esta Recomendación.

Cuando esté presente en un sistema, el controlador de acceso deberá prestar los siguientes servicios:

- Conversión de dirección – El controlador de acceso efectuará la conversión de dirección alias a dirección de transporte. Esto se debe hacer utilizando un cuadro de conversión que se actualiza mediante los mensajes de registro descritos en la cláusula 7. También son posibles otros métodos de actualización del cuadro de conversión.
- Control de admisiones – El controlador de acceso autorizará el acceso a la red utilizando mensajes ARQ/ACF/ARJ H.225.0. La autorización del acceso puede basarse en la autorización de la llamada, en la anchura de banda o en algún otro criterio que se deja a decisión del fabricante. También puede ser una función nula que admita todas las peticiones.
- Control de anchura de banda – El controlador de acceso soportará mensajes BRQ/BRJ/BCF. Esto puede basarse en la gestión de la anchura de banda. También puede ser una función nula que acepte todas las peticiones de cambio de anchura de banda.

- Gestión de zona – El controlador de acceso proporcionará las funciones anteriores para terminales, MCU y pasarelas que se hayan registrado en él como se describe en 7.2.

El controlador de acceso también puede efectuar otras funciones opcionales, tales como:

- Señalización de control de llamada – El controlador de acceso puede optar por completar la señalización de la llamada con los puntos extremos y puede procesar él mismo la señalización de la llamada. De manera alternativa, el controlador de acceso puede encaminar los puntos extremos para que conecten directamente entre ellos el canal de señalización de llamada. De esta manera, el controlador de acceso puede evitar el tratamiento de señales de control de llamada H.225.0. Es posible que tenga que actuar como la red según se define en la Rec. UIT-T Q.931 para soportar servicios suplementarios. Este funcionamiento queda en estudio.
- Autorización de llamada – Utilizando la señalización H.225.0, el controlador de acceso puede rechazar llamadas procedentes de un terminal por ausencia de autorización. Pueden ser motivos de rechazo, entre otros, el acceso restringido hacia/desde terminales o pasarelas particulares y el acceso restringido durante determinados periodos de tiempo. Los criterios para determinar si se da o no la autorización quedan fuera del alcance de la presente Recomendación.
- Gestión de anchura de banda – Control del número de terminales H.323 a los que se permite el acceso simultáneo a la red. Utilizando la señalización H.225.0, el controlador de acceso puede rechazar llamadas procedentes de un terminal debido a limitaciones de anchura de banda. Tal cosa puede ocurrir si el controlador de acceso determina que no hay suficiente anchura de banda disponible en la red para soportar la llamada. Los criterios para determinar si se dispone de anchura de banda quedan fuera del alcance de la presente Recomendación. Téngase en cuenta que esta función puede ser una función nula, es decir, que a todos los terminales se les permita el acceso. Esta función actúa también durante una llamada activa, cuando un terminal pide anchura de banda adicional.
- Gestión de llamada – Por ejemplo, el controlador de acceso puede mantener una lista de llamadas H.323 en curso. Esta información puede ser necesaria para indicar que un terminal llamado está ocupado y proporcionar información para la función de gestión de anchura de banda.
- Modificación del alias de dirección – El controlador de acceso puede devolver un alias de dirección modificado. Si el controlador de acceso devuelve un alias de dirección en una ACF, el punto extremo utilizará el alias de dirección en el establecimiento de la conexión.
- Conversión de los dígitos marcados – El controlador de acceso puede convertir los dígitos marcados en un número E.164 o en un número de red privada.
- Estructura de datos de información de gestión del controlador de acceso – Queda en estudio.
- Reserva de anchura de banda para terminales que no pueden efectuar esta función – Queda en estudio.
- Servicio de directorio – Queda en estudio.

Para el soporte de conferencias multipunto ad hoc, el controlador de acceso puede optar por recibir los canales de control H.245 de los dos terminales de una conferencia punto a punto. Cuando la conferencia pase a ser conferencia multipunto, el controlador de acceso puede reencaminar el canal de control H.245 a un MC. No es preciso que el controlador de acceso procese la señalización H.245, sólo tiene que pasarla entre los terminales o entre los terminales y el MC.

Las redes que contienen pasarelas deberán contener también un controlador de acceso para convertir las direcciones de los **dialledDigits** (**dígitos marcados**) o los **partyNumber** (**números de parte**) (incluidos el **e164Number** (**número E.164**) y el **privateNumber** (**número privado**)) entrantes en direcciones de transporte.

Las entidades H.323 que contienen un controlador de acceso deberán tener un mecanismo para inhabilitar el controlador de acceso interno de manera que, cuando haya múltiples entidades H.323 que contengan un controlador de acceso en una red, las entidades H.323 puedan ser configuradas en la misma zona.

6.5 Características del controlador multipunto

El controlador multipunto (MC) proporciona funciones de control para soportar conferencias entre tres o más puntos extremos de una conferencia multipunto. El MC lleva a cabo el intercambio de capacidades con cada uno de los puntos extremos de una conferencia multipunto y envía un conjunto de capacidades a los puntos extremos de la conferencia indicando los modos de funcionamiento en los que pueden transmitir. El MC puede revisar el conjunto de capacidades que envía a los terminales como consecuencia de la incorporación de terminales a la conferencia o el abandono de terminales de la misma, o por otros motivos.

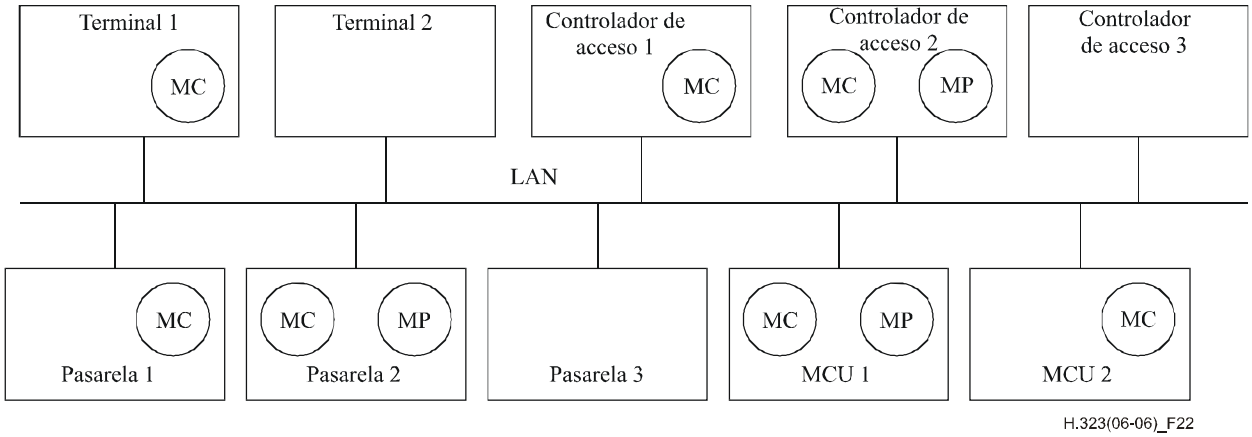
De esta manera, el MC determina el modo de comunicación seleccionado (SCM, *selected communications mode*) para la conferencia. El SCM puede ser común para todos los puntos extremos de la conferencia o, de manera alternativa, algunos de ellos pueden tener un SCM distinto del de los otros puntos extremos. La manera según la cual el MC determina un SCM queda fuera del alcance de la presente Recomendación.

Como parte del establecimiento de una conferencia multipunto, un punto extremo quedará conectado a un MC en su canal de control H.245. La conexión puede producirse:

– vía una conexión explícita con una MCU;
– vía una conexión implícita al MC dentro de un controlador de acceso;
– vía una conexión implícita al MC dentro de otro terminal o pasarela de la conferencia multipunto;
– vía una conexión implícita a través de un controlador de acceso a una MCU.

La elección del modo de conferencia (por ejemplo, descentralizada o centralizada) se produce después de la conexión con el MC utilizando la señalización H.245. Dicha elección puede verse limitada por la capacidad de los puntos extremos o del MC.

El MC puede estar situado dentro de un controlador de acceso, una pasarela, un terminal, o una MCU. Véase la figura 22.



NOTA – La pasarela, el controlador de acceso y la MCU pueden ser un solo dispositivo.

Figura 22/H.323 – Posibles localizaciones del MC y el MP en un sistema H.323

Un MC situado dentro de un terminal no es llamable. Puede ser incluido en la llamada para procesar la señalización H.245 de soporte de las conferencias multipunto ad hoc. En este caso, puede que no haya ninguna diferencia entre el MC y la función de control H.245 (véase 6.2.8) del terminal. Las comunicaciones entre ellas quedan fuera del alcance de la presente Recomendación.

Un MC localizado con el controlador de acceso no es llamable, sin embargo, una MCU localizada con un controlador de acceso sí lo es. Una MCU localizada con un controlador de acceso puede funcionar como una MCU independiente. Un MC localizado con un controlador de acceso puede ser utilizado para soportar conferencias multipunto ad hoc cuando el controlador de acceso reciba los canales de control H.245 desde los puntos extremos. De esta manera, el controlador de acceso puede encaminar los canales de control H.245 al MC al comienzo de la llamada o cuando la conferencia pase a ser conferencia multipunto.

La pasarela puede funcionar como un terminal o una MCU. Cuando funciona como un terminal, puede contener un MC. Éste tiene las mismas características que las descritas anteriormente para un MC dentro de un terminal.

Una MCU contiene siempre un MC. La MCU es llamable y el MC procesa el canal de control H.245 proveniente de todos los demás puntos extremos.

Cuando dos o más puntos extremos participen en una conferencia, utilizarán el procedimiento de resolución principal-subordinado de la Rec. UIT-T H.245 para determinar qué MC controlará la conferencia.

Después del intercambio de capacidades y la determinación principal/subordinado, el MC puede asignar primero un número de terminal a un nuevo punto extremo utilizando **terminalNumberAssign** (**asignación de número de terminal**). El MC notificará a los otros puntos extremos el nuevo punto extremo en la conferencia utilizando **terminalJoinedConference** (**el terminal se incorporó a la conferencia**). El nuevo punto extremo puede pedir una lista de los otros puntos extremos de la conferencia utilizando la **terminalListRequest** (**petición de lista de terminales**).

6.6 Características del procesador multipunto

El MP recibe trenes de audio, vídeo y/o datos de los puntos extremos que participan en una conferencia multipunto centralizada o híbrida. El MP procesa estos trenes de medios y los devuelve a los puntos extremos.

Las comunicaciones entre el MC y el MP no están sujetas a normalización.

El MP puede procesar uno o más tipos trenes de medios. Cuando el MP procese vídeo, procesará los algoritmos y formatos de vídeo descritos en 6.2.4. Cuando procese audio, procesará los algoritmos de audio descritos en 6.2.5. Cuando procese datos, procesará los trenes de datos descritos en 6.2.7.

Un MP que procese vídeo deberá proporcionar conmutación o mezcla de vídeo. La conmutación de vídeo es el proceso de selección del vídeo que el MP envía como salida hacia los terminales desde una fuente a otra. Los criterios utilizados para efectuar la conmutación pueden determinarse mediante la detección de un cambio en el conferenciante (percibido por el nivel de audio asociados) o mediante el control H.245. La mezcla de vídeo es el proceso de creación de un formato correspondiente a más de una fuente de vídeo en el tren de vídeo que el MP envía como salida hacia los terminales. Un ejemplo de mezcla de vídeo es la combinación de cuatro imágenes fuente en una matriz de dos por dos en la imagen de salida de vídeo. Los criterios respecto a qué fuentes y cuántas se mezclan los determina el MC mientras no se definan otros controles. La utilización de las Recomendaciones de la serie T.120 para estas funciones de control queda en estudio.

Un MP que procese audio deberá preparar N salidas de audio a partir de M entradas de audio conmutando, mezclando o combinando ambas cosas. La mezcla de audio requiere la decodificación del audio de entrada en señales lineales (MIC o analógicas), efectuando una combinación lineal de las señales y recodificando el resultado en el formato de audio apropiado. El MP puede eliminar o atenuar algunas de las señales de entrada para reducir el ruido y otras señales no deseadas. Cada salida de audio puede tener una mezcla diferente de señales de entrada facilitando así las conversaciones privadas. Los terminales supondrán que su respectivo audio no está presente en el tren de audio que se les devuelve. La eliminación por los terminales de su propio audio de la salida de audio del MP queda en estudio.

Un MP que procese datos T.120 deberá ser capaz de actuar como un proveedor de MCS sin hojas y debería ser capaz de actuar como un proveedor de MCS superior. Un MP puede procesar también datos no normalizados, datos de usuario transparentes y/u otros tipos de datos.

El MP puede efectuar la conversión de algoritmos y formatos, permitiendo a los terminales participar en una conferencia en diferentes SCM.

El MP no es llamable; la MCU que forma parte de él sí que lo es. El MP termina y origina los canales de medios.

6.7 Características de la unidad de control multipunto

La MCU es un punto extremo que da soporte a conferencias multipunto y deberá estar formada por un MC y cero o más MP. La MCU utiliza los mensajes y procedimientos H.245 para implementar características similares a las que figuran en la Rec. UIT-T H.243.

Una MCU típica, que soporta conferencias multipunto centralizadas, consta de un MC y de un MP de audio, vídeo y datos. Una MCU típica, que soporta conferencias multipunto descentralizadas, consta de un MC y de un MP de datos que soporte la Rec. UIT-T T.120. Se basa en el procesamiento descentralizado de audio y vídeo.

El lado red de una pasarela puede ser una MCU. Un controlador de acceso puede incluir también una MCU. En uno y otro caso, se trata de funciones independientes que casualmente están coubicadas.

La MCU será llamable por otros puntos extremos que utilicen los procedimientos de la cláusula 8.

6.8 Capacidad multipunto

6.8.1 Capacidad multipunto centralizada

Todos los puntos extremos tendrán capacidad multipunto centralizada. En este modo de funcionamiento, los terminales comunican con el MC de la MCU de una manera punto a punto en el canal de control y con el MP en los canales de audio, vídeo y datos. En este modo de funcionamiento, el MC efectúa funciones de control multipunto H.245 mientras que el MP efectúa la conmutación o mezcla de vídeo, la mezcla de audio y la distribución de datos multipunto T.120. El MP devuelve los trenes de vídeo, audio y datos resultantes a los puntos extremos. El MP tiene la capacidad de efectuar la conversión entre diferentes formatos y velocidades binarias de audio, vídeo y datos, permitiendo a los puntos extremos participar en la conferencia mediante diferentes modos de comunicación.

La MCU puede utilizar la multidifusión para distribuir trenes de medios procesados si los puntos extremos de la conferencia pueden recibir transmisiones multidifundidas. La distribución multidifundida de datos procesados queda en estudio.

Este modo es señalado por las siguientes capacidades H.245: **centralizedControl** (**control centralizado**), **centralizedAudio** (**audio centralizado**), **centralizedVideo** (**vídeo centralizado**) y **centralizedData** (**datos centralizados**). Opcionalmente, **distributedAudio** (**audio distribuido**) y **distributedVideo** (**vídeo distribuido**) pueden indicar distribución multidifundida de trenes de medios.

6.8.2 Capacidad multipunto descentralizada

Si los puntos extremos tienen capacidad multipunto descentralizada, comunican con el MC de una MCU, pasarela, controlador de acceso o punto extremo de una manera punto a punto en un canal de control H.245 y, opcionalmente, con un MP en canales de datos. Los puntos extremos deberán tener la capacidad de multidifundir sus canales de audio y vídeo a todos los demás puntos extremos de la conferencia. El MC puede controlar el punto extremo o los puntos extremos que están multidifundiendo audio y/o vídeo activamente (por ejemplo, utilizando **flowControlCommand** en uno u otro canal).

Los puntos extremos reciben canales de vídeo en multidifusión y seleccionan uno o más de los canales disponibles para la presentación visual al usuario. Los puntos extremos reciben canales de audio en multidifusión y realizan una función de mezcla de audio para presentar una señal de audio compuesta al usuario.

El MC puede proporcionar funciones de control de conferencia tales como el control de la presidencia, la difusión de vídeo y la selección de vídeo. Para ello se recibirá H.245 de un punto extremo y se enviará a continuación el control apropiado a los demás puntos extremos, para habilitar o inhabilitar la multidifusión de su vídeo. Las instrucciones T.120 pueden proporcionar, opcionalmente, las mismas funciones.

Este modo es señalado por las siguientes capacidades H.245: **centralizedControl**, **distributedAudio**, **distributedVideo** y **centralizedData**.

6.8.3 Capacidad multipunto híbrida con audio centralizado

Si los puntos extremos y la MCU tienen capacidad multipunto híbrida con audio centralizado, pueden utilizar multipunto distribuido para vídeo y multipunto centralizado para audio. En este modo, los puntos extremos comunican con el MC de una manera punto a punto en el canal de control H.245 y, opcionalmente, con un MP en el canal de datos.

Los puntos extremos tendrán la capacidad de multidifundir sus canales de vídeo a todos los demás puntos extremos de la conferencia. El MC puede controlar el punto extremo o los puntos extremos que están multidifundiendo vídeo activamente. Los puntos extremos reciben canales de vídeo en multidifusión y seleccionan uno o más de los canales disponibles para la presentación visual al usuario.

Todos los puntos extremos de la conferencia transmiten sus canales de audio al MP. El MP realiza la función de mezcla de audio y envía como salida los trenes de audio resultantes a los puntos extremos. El MP puede producir una suma de audio exclusiva para cada punto extremo de la conferencia. La distribución multidifundida del audio procesado queda en estudio.

Este modo es señalado por las siguientes capacidades H.245: **centralizedControl**, **centralizedAudio**, **distributedVideo** y **centralizedData**.

6.8.4 Capacidad multipunto híbrida con vídeo centralizado

Si los puntos extremos y la MCU tienen capacidad de multipunto híbrida con vídeo centralizado, pueden utilizar multipunto distribuido para audio y multipunto centralizado para vídeo. En este modo, los puntos extremos comunican con el MC de una manera punto a punto en el canal de control H.245 y, opcionalmente, con un MP en los canales de datos.

Los puntos extremos tendrán la capacidad de multidifundir sus canales de audio a todos los demás puntos extremos de la conferencia. El MC puede controlar el punto extremo o los puntos extremos que están multidifundiendo audio activamente. Los puntos extremos reciben canales de audio en multidifusión y realizan una función de mezcla de audio para presentar una señal de audio compuesta al usuario.

Todos los puntos extremos de la conferencia transmiten sus canales de vídeo al MP. El MP realiza las funciones de conmutación, mezcla o conversión de formato de vídeo y envía como salida los trenes de vídeo resultantes a los puntos extremos. El MP puede producir un tren de vídeo exclusivo para cada punto extremo de la conferencia o multidifundir un tren de vídeo a todos los puntos extremos participantes para minimizar la anchura de banda utilizada en la red.

Este modo es señalado por las siguientes capacidades H.245: **centralizedControl**, **distributedAudio**, **centralizedVideo** y **centralizedData**.

6.8.5 Establecimiento de modo común

El MC coordinará un modo de comunicaciones común entre los puntos extremos de la conferencia multipunto. El MC puede forzar a los puntos extremos a un determinado modo de transmisión común (según permitan sus conjuntos de capacidades) enviando a cada punto extremo una lista de capacidades de recepción en la que se indique solamente el modo de transmisión deseado, o bien, el MC puede basarse en el **multipointModeCommand** y en las instrucciones de preferencia de modo para aplicar simetría de modo. Debería utilizarse este último procedimiento ya que permite a los puntos extremos conocer la gama completa de capacidades disponibles de conferencia que pueden ser solicitadas.

Si la MCU tiene la capacidad de convertir formatos de audio y/o vídeo, quizás no sea necesario forzar en todos los puntos extremos el mismo modo de comunicaciones.

6.8.6 Adaptación de velocidades en configuraciones multipunto

Puesto que los puntos extremos de cada enlace de una configuración multipunto pueden intentar funcionar a velocidades binarias diferentes, el MC deberá enviar mensajes **flowControlCommand** H.245 para limitar las velocidades binarias transmitidas a las que pueden ser enviadas a los receptores.

6.8.7 Sincronización con el movimiento de los labios en configuraciones multipunto

Un MP que proporciona mezcla de audio en las conferencias multipunto centralizadas o híbridas deberá modificar las indicaciones de tiempo de los trenes de audio y vídeo, teniendo en cuenta su propia base de tiempos, para mantener la sincronización entre audio y vídeo. Además, cuando el MP procese el audio y/o el vídeo para generar un nuevo tren surgido del propio MP, deberá generar sus propios números de secuencia en los paquetes de audio y vídeo.

Cuando se mezcle audio, el MP deberá sincronizar cada uno de los trenes de audio entrantes con su propia temporización, mezclar los trenes de audio y generar a continuación un nuevo tren de audio en función de su temporización con sus propios números de secuencia. Si el MP conmuta también vídeo, se deberá sustituir en el tren conmutado su indicación de tiempo original por la base de tiempos del MP para sincronizarlo con el tren de audio mezclado, y se le deberá asignar un nuevo número de secuencia que represente el tren procedente del MP.

En el caso de conferencias multipunto distribuidas, el punto extremo receptor puede mantener la sincronización del movimiento de los labios alineando el tren de vídeo seleccionado y su audio asociado mediante indicaciones de tiempo RTP. La alineación de otros trenes de audio puede no ser necesaria. Si se visualizan múltiples trenes de vídeo, se deberán alinear los trenes de audio asociados.

Puede ocurrir que no sea posible garantizar la sincronización del movimiento de los labios en conferencias multipunto híbridas.

6.8.8 Criptación multipunto

En una configuración multipunto centralizada, el MP se considera una entidad fiable. Cada puerto del MP descripta los trenes de información procedentes de cada uno de los puntos extremos H.323 y cripta los trenes de información hacia cada punto extremo de acuerdo con 10.1. El funcionamiento de una MCU no fiable queda en estudio.

6.8.9 Unidades de control en configuración multipunto en cascada

La función de control multipunto puede ser distribuida entre varios MC. Esto se denomina puesta en cascada. La puesta en cascada permite a dos o más MC comunicar entre sí a fin de controlar una conferencia multipunto. La puesta en cascada de los MC se hace estableciendo un canal de control H.245 entre los MC. Un MC se define como el MC principal, mientras que los otros MC se definen como MC subordinados.

Los procedimientos para la puesta en cascada de los MC se definen en 8.4.5.

6.9 Modelos para los servicios suplementarios

La capacidad de soportar un gran número de servicios suplementarios y de características constituye un requisito básico de muchas soluciones de telefonía, con independencia de las tecnologías subyacentes.

Para muchos de tales servicios, es igualmente necesario que exista un nivel elevado de interoperabilidad entre equipos de distintos vendedores. Ello conduce a la adopción de soluciones normalizadas.

Al mismo tiempo, los suministradores de equipos desean que los servicios ofrecidos destaquen sus propios productos. Ello puede conseguirse utilizando soluciones propietarias, aunque así se pueda poner en riesgo la interoperabilidad. En algunos casos, ello puede ser aceptable o deseable, pero a menudo no es ese el caso.

Por lo tanto, el objetivo es definir una norma que sea lo suficientemente flexible como para soportar todos (o la mayoría) de los servicios que un vendedor pueda desear ofrecer.

En el entorno H.323, existen varios métodos para poder ofrecer servicios: las Recomendaciones de la serie H.450.x, Rec. UIT-T H.248 asociada a sus paquetes, el anexo L y el anexo K. Aunque existen aspectos comunes en algunos de los objetivos de diseño de dichas soluciones, el énfasis de cada uno de ellos es distinto y resultan más o menos apropiados en función de las circunstancias. Estas soluciones representan una gama de opciones para la implementación del sistema y de sus características, que van desde el control exclusivamente entre pares (modo funcional) hasta el control principal/subordinado (modo estímulo), utilizando el control de una primera o de una tercera parte. Más que de soluciones competitivas, se trata de soluciones complementarias que ofrecen libertad de elección al desarrollador del sistema.

Las Recomendaciones de la serie H.450.x están diseñadas para permitir la interoperabilidad de los servicios a nivel funcional. El hecho de que se deriven de QSIG garantiza el interfuncionamiento con muchos sistemas de redes privadas. Los servicios se definen para relaciones entre pares, residiendo la inteligencia normalmente en el punto extremo. Un servicio H.450 debe estar normalmente soportado de forma explícita por cada uno de los puntos extremos afectados del sistema. La distribución del control del servicio permite que los puntos extremos sean más autosuficientes y autocontenidos, y es mejor soportado por puntos extremos de elevadas prestaciones.

Los restantes protocolos proporcionan control a nivel de estímulo, en los que sólo se requiere que una de las entidades tenga comprensión plena de un servicio, típicamente en una relación principal-subordinado. Los métodos basados en estímulos utilizan un conjunto definido de funciones atómicas, que utilizadas en múltiples combinaciones ofrecen cualquiera número de servicios.

Los protocolos en modo estímulo simplifican la introducción de nuevos servicios. Sin embargo, las distintas implementaciones del mismo servicio pueden diferir lo suficiente como para complicar la interoperabilidad incluso entre redes del mismo tipo.

El anexo L, al igual que H.450, se basa en H.323 de modo que todos los puntos extremos anexo L son, por definición, conformes con H.323. Esto permite la utilización de procedimientos normalizados H.323 para la señalización de llamadas y el control de medios. Las características inteligentes adicionales al control básico de llamadas se implementan en un servidor de características centralizado (asociado a un control de acceso o a un punto extremo H.323). Este protocolo permite la prestación de los servicios por parte de uno o varios servidores de características. Por consiguiente el anexo L constituye un híbrido de los modelos de control entre pares y de control principal/subordinado, en los que la inteligencia se reparte entre el punto extremo y el servidor de características.

El método del anexo K permite el control por una tercera parte de una llamada H.323 sobre la base de un control de canal separado (utilizando HTTP [47]) para la interacción con el usuario. No existe un conjunto fijo de capacidades para la interfaz del usuario, ya que pueden utilizarse dinámicamente diversos tipos de formatos de texto, de imágenes y sonoros como tipos MIME [48] registrados. El proveedor de servicio (el servidor HTTP) es responsable de establecer la correspondencia entre los eventos HTTP y las acciones de control de la llamada (mensajes H.450 u otros) para los servicios suplementarios, de tal forma que el punto extremo H.323 ignora la aplicación HTTP. En una llamada, el proveedor de servicio puede estar asociado al controlador de acceso, a los puntos extremos distantes o al controlador de acceso distante.

El protocolo H.248 es un protocolo genérico de "control de dispositivo" de pasarela, basado en un modelo de control principal/subordinado (modo estímulo) en el que toda la inteligencia se mantiene en una entidad central o principal (el controlador de pasarela de medios o MGC) y en el que un punto extremo (la pasarela de medios o MG) es el subordinado. El protocolo H.248 está diseñado para ser independiente del protocolo de control de llamada y, por lo tanto, no requiere que los puntos extremos sean conformes con H.323. H.248 se desarrolló para el control de pasarelas de medios e implica la existencia de una estrecha relación entre el MGC y la MG, y en el que un

usuario sólo puede subscribirse simultáneamente a las características de un único MGC. H.248 está diseñada para ser fácilmente ampliable mediante la utilización de paquetes que definan una característica específica, de forma que los servicios que puede soportar un sistema basado en H.248 sólo están limitados por los paquetes que soportan el MGC y la MG.

7 Señalización de la llamada

La señalización de la llamada consiste en los mensajes y procedimientos utilizados para establecer una comunicación, pedir cambios de anchura de banda de la llamada, obtener el estado de los puntos extremos de la llamada y desconectar la llamada. En la señalización de llamadas se utilizan mensajes definidos en la Rec. UIT-T H.225.0 y los procedimientos descritos en la cláusula 8. En esta cláusula se exponen algunos conceptos relativos a la señalización de la llamada.

7.1 Direcciones

7.1.1 Dirección de red

Cada una de las entidades H.323 deberá tener por lo menos una dirección de red. Dicha dirección identifica de manera exclusiva la entidad H.323 en la red. Algunas entidades pueden compartir una dirección de red (por ejemplo, un terminal y un MC coubicado). Esta dirección es específica del entorno de red en el que está situado el punto extremo. Entornos de red diferentes pueden tener formatos de dirección de red diferentes.

Un punto extremo puede utilizar direcciones de red diferentes para canales diferentes dentro de la misma llamada.

7.1.2 Identificador TSAP

Por cada dirección de red, cada una de las entidades H.323 puede tener varios identificadores TSAP. Los identificadores TSAP permiten la multiplexación de varios canales que comparten la misma dirección de red.

Los puntos extremos tienen un identificador TSAP conocido definido: el identificador TSAP de canal de señalización de llamada. Los controladores de acceso tienen un identificador TSAP conocido definido: el identificador TSAP de canal RAS y una dirección multidifusión conocida definida: dirección de multidifusión de descubrimiento. Éstos se definen en el apéndice IV/H.225.0.

Los puntos extremos y las entidades H.323 deberían utilizar identificadores TSAP dinámicos para el canal de control H.245, los canales de audio, los canales de vídeo y los canales de datos. El controlador de acceso debería utilizar un identificador TSAP dinámico para los canales de señalización de llamada. Los canales RAS y los canales de señalización pueden ser reencaminados a identificadores TSAP dinámicos durante el proceso de registro.

7.1.3 Dirección alias

Un punto extremo puede tener también una o más direcciones alias asociadas al mismo. Una dirección alias puede representar el punto extremo o puede representar conferencias que el punto extremo está acogiendo. Las direcciones alias proporcionan un método alternativo de direccionamiento del punto extremo. Dichas direcciones incluyen direcciones de **dialledDigits** o de **partyNumber** (incluyendo números telefónicos privados y números E.164 públicos), identidades H.323 (cadenas alfanuméricas que representan nombres, direcciones similares a las del correo electrónico, etc.) y cualesquiera otras direcciones definidas en la Rec. UIT-T H.225.0. Las direcciones alias deberán ser únicas dentro de una zona. Los controladores de acceso, los MC y los MP no tendrán direcciones alias.

NOTA – En las versiones 1, 2 y 3 de las Recs. UIT-T H.323 y H.225.0 se hacía referencia en general a los dígitos marcados como direcciones E.164 (y **dialledDigits** eran **e164**), lo cual no era cierto. Asimismo, dichas versiones de las Recs. UIT-T H.323 y de H.225.0 hacían referencia a las direcciones E.164 como los números públicos de las partes (**e164Number** eran **publicPartyNumber**): en ningún lugar se aclaraba que los números públicos de la parte eran números E.164. Este cambio terminológico no afecta de forma alguna a la retrocompatibilidad. En el apéndice V se presenta un análisis detallado de la utilización de los números E.164.

Cuando no haya controlador de acceso en el sistema, el punto extremo llamante direccionará el punto extremo llamado directamente utilizando la dirección de transporte de canal de señalización de llamada del punto extremo llamado. Cuando haya un controlador de acceso en el sistema, el punto extremo llamante podrá direccionar el punto extremo llamado mediante su dirección de transporte de canal de señalización de llamada o dirección alias. El controlador de acceso convertirá esta última en una dirección de transporte del canal de señalización de llamada.

La dirección **dialledDigits** del punto extremo llamado puede estar formada por un código de acceso opcional seguido del número de teléfono específico del plan de numeración del proveedor de servicio. El código de acceso consta de n cifras de 0 a 9, ∗ y #. El número de cifras y su significado se dejan a criterio del fabricante. Una de las finalidades de este código de acceso podría ser pedir acceso a una pasarela. El controlador de acceso puede alterar esta dirección antes de enviarla a su destino. El controlador de acceso puede asimismo proporcionar un **partyNumber** que se utilice en lugar de los **dialledDigits**.

El ID H.323 consta de una cadena de caracteres de ISO/CEI 10646 definida en la Rec. UIT-T H.225.0. Puede ser un nombre de usuario, un nombre de conferencia, un nombre de correo electrónico u otro identificador.

Un punto extremo puede tener más de una dirección alias (entre ellas, más de una del mismo tipo) que son convertidas a la misma dirección de transporte.

7.1.4 Esquema URL de H.323

Uno de los tipos de alias definidos en la Rec. UIT-T H.323 es el **url-ID**, cuyo objetivo es contener esquemas de URL normalizados que pueden utilizarse para alcanzar recursos. Una entidad H.323 puede aceptar cualquier URL válido pero debería soportar el URL H.323 tal como se define en esta cláusula.

El URL H.323 tiene por objeto ayudar a que una entidad resuelva la dirección de otra entidad H.323. Se compone de dos partes: *user* (*usuario*) y *hostport* (*puerto del anfitrión)*. *User* especifica un alias de la entidad, tal como un usuario o un servicio, sin transportar información alguna sobre la ubicación de la entidad. Por otra parte, *hostport* es el nombre de dominio del punto extremo, controlador de acceso o elemento frontera.

El URL H.323 se define en ABNF como se muestra a continuación. Obsérvese que utiliza las reglas de núcleo que se especifican en 6.1 de [51].

```
H323-URL          =    "h323:" address [ url-parameters ]
address           =    user / "@" hostport / user "@" hostport
user              =    1*(%x21-24 / %x26-3F / %x41-7F / escaped)
                       ; The symbols "%", "@", and symbols with a
                       ; character value below 0x21 may be represented
                       ; as escaped sequences.
hostport          =    host [ ":" port]
host              =    hostname / IPv4address / IPv6reference
hostname          =    *( domainlabel "." ) toplabel [ "." ]
domainlabel       =    alphanum / alphanum *( alphanum / "-" ) alphanum
toplabel          =    ALPHA / ALPHA *( alphanum / "-" ) alphanum
IPv4address       =    1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT
IPv6reference     =    "[" IPv6address "]"
IPV6address       =    hexpart [ ":" IPv4address ]
```

```
hexpart             =    hexseq / hexseq "::" [ hexseq ] / "::" [ hexseq ]
hexseq              =    hex4 *( ":" hex4 )
hex4                =    1*4HEXDIG
port                =    1*DIGIT
url-parameters      =    *( ";" url-parameter )
url-parameter       =    1*(%x21-24 / %x26-3A / %x3C-7F / escaped)
                         ; Specific parameter definitions are for further
                         ; study.  The symbols "%", ";", and symbols with
                         ; a character value below 0x21 may be
                         ; represented as escaped sequences.
alphanum            =    ALPHA / DIGIT
escaped             =    "%" HEXDIG HEXDIG
```

El *anfitrión* no distingue mayúsculas de minúsculas.

User es una cadena Unicode [19] a la que se deberá codificar de acuerdo con UTF-8 y aplicar a continuación un escape, según proceda. Salvo por los caracteres con valor numérico por debajo de 0x80, *u*ser es función del caso de que se trate. Los caracteres con un valor numérico por debajo de 0x80 no son función del caso de que se trate.

El conjunto de caracteres y la dependencia con respecto al caso del *parámetro url* se especifican en la definición de cada parámetro.

Si un punto extremo se registra ante un controlador de acceso y no proporciona una cadena de caracteres para *hostport*, el controlador de acceso puede añadir una cadena de caracteres de *hostport* al URL cuando éste devuelva el alias del punto extremo en un mensaje RCF. El punto extremo aceptará los alias modificados y los utilizará cuando envíe ulteriores peticiones al controlador de acceso, incluyendo mensajes URQ para desregistrar el alias.

7.2 Canal de registro, admisión y estado (RAS)

El canal RAS se empleará para transportar mensajes utilizados en los procesos de descubrimiento de controlador de acceso y de registro de punto extremo que asocian una dirección alias de punto extremo con su dirección de transporte de canal de señalización de llamada. El canal RAS deberá ser un canal no fiable.

Como los mensajes RAS se transmiten por un canal no fiable, H.225.0 recomienda plazos y cuentas de reintento para diversos mensajes. Un punto extremo o un controlador de acceso que no puede responder a una petición en el plazo especificado puede utilizar el mensaje petición en curso (RIP, *request in progress*) para indicar que está aún procesando la petición. Un punto extremo o controlador de acceso que recibe la RIP reiniciará su temporizador de plazo y su contador de reintentos.

7.2.1 Descubrimiento del controlador de acceso

El descubrimiento del controlador de acceso es el proceso que utiliza un punto extremo para determinar en qué controlador de acceso se tiene que registrar. El proceso puede ser manual o automático. El descubrimiento manual se basa en métodos que quedan fuera de alcance de la presente Recomendación para determinar con qué controlador de acceso está asociado un punto extremo. El punto extremo se configura con la dirección de transporte del controlador de acceso asociado. Por ejemplo, se puede introducir en la configuración del punto extremo o en un fichero de inicialización. De esta manera, el punto extremo conoce *a priori* con qué controlador de acceso está asociado. El punto extremo puede registrarse a continuación en ese controlador de acceso.

El método automático permite que la asociación punto extremo-controlador de acceso cambie con el tiempo. Es posible que el punto extremo no conozca quién es su controlador de acceso, o quizás necesite identificar otro controlador de acceso debido a un fallo, lo que puede hacerse mediante el descubrimiento automático. El descubrimiento automático permite una tara administrativa menor al configurar puntos extremos individuales y permite además reemplazar un controlador de acceso existente sin reconfigurar manualmente todos los puntos extremos afectados. Obsérvese que los

procedimientos de controlador de acceso asignado que se definen en 7.2.6.1, también se pueden utilizar para automatizar la asignación de los puntos extremos a sus controladores de acceso asociados.

Para utilizar el método automático, el punto extremo puede multidifundir un mensaje (o utilizar a tal efecto otros métodos, como los que se describen en el apéndice IV/H.225.0) de petición de controlador de acceso (GRQ, *gatekeeper request*) preguntando "¿Quién es mi controlador de acceso?". El mensaje se envía a las direcciones multidifusión de descubrimiento conocidas. Uno o más controladores de acceso puede responder con el mensaje de confirmación de controlador de acceso (GCF, *gatekeeper confirmation*) indicando "Yo puedo ser su controlador de acceso" conteniendo la dirección de transporte del canal RAS del controlador de acceso. Si un controlador de acceso no desea que un punto extremo se registre en él, deberá devolver un rechazo de controlador de acceso (GRJ, *gatekeeper reject*), véase la figura 23. Si responde más de un controlador de acceso, el punto extremo puede elegir el controlador de acceso que desea utilizar. En este momento, el punto extremo conoce en qué controlador de acceso se tiene que registrar. El punto extremo se puede ahora registrar en él.

Si el punto extremo conoce la localización del controlador de acceso por algún medio *a priori*, puede elegir unidifundir la GRQ al controlador de acceso a los efectos del intercambio criptológico H.225.0.

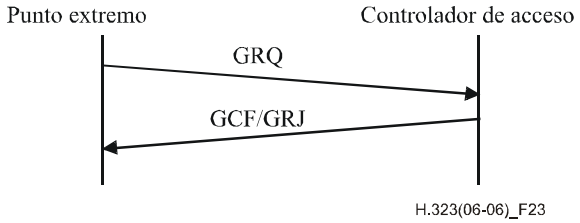


Figura 23/H.323 – Descubrimiento automático

A fin de dotar de redundancia a los sistemas que utilizan un controlador de acceso, el controlador de acceso puede indicar controladores de acceso alternativos que pueden utilizarse en el caso de un fallo de controlador de acceso primario. Esta lista de controladores de acceso alternativos se proporciona en el campo **alternateGatekeeper** (**controlador de acceso alternativo**) de los mensajes GCF/GRJ y RCF/RRJ. El punto extremo también puede utilizar los procedimientos del controlador de acceso asignado para volver a registrarse en su controlador de acceso primario cuando éste quede nuevamente disponible. El controlador de acceso puede proporcionar al punto extremo la dirección de su controlador de acceso asignado en el campo **assignedGatekeeper** de los mensajes GCF/GRJ y RCF/RRJ.

Si no responde ningún controlador de acceso dentro de un plazo determinado, el punto extremo puede intentar de nuevo la GRQ. Un punto extremo no deberá enviar una GRQ durante los 5 s siguientes al envío de la petición previa. Si no se recibe respuesta, el punto extremo puede utilizar el método de descubrimiento manual.

Si en cualquier momento un punto extremo determina que tiene un registro no válido en su controlador de acceso, deberá redescubrir su controlador de acceso. El punto extremo puede considerar que un registro no es válido al recibir un mensaje RRJ de un controlador de acceso en respuesta a una RRQ del punto extremo o al no recibir respuesta alguna a una RRQ en un plazo estipulado.

La GRQ puede repetirse periódicamente (es decir, al arrancar el punto extremo), por lo que el controlador de acceso podrá tratar múltiples peticiones procedentes del mismo punto extremo.

7.2.2 Registro del punto extremo

El registro es el proceso por el cual un punto extremo se incorpora a una zona y comunica al controlador de acceso sus direcciones de transporte y sus direcciones alias. Como parte de su proceso de configuración, todos los puntos extremos se registrarán en el controlador de acceso identificado mediante el proceso de descubrimiento. El registro deberá tener lugar antes de que se intente cualquier llamada y podrá producirse periódicamente, según se necesite (por ejemplo, al arrancar el punto extremo).

Una pasarela o una MCU puede registrar una sola dirección de transporte o múltiples direcciones de transporte como su dirección de señalización de llamada, y puede registrar una sola dirección de transporte o múltiples direcciones de transporte como su dirección de RAS. La utilización de múltiples direcciones de transporte indicará una lista de direcciones priorizada para intentar cuando se comunica con un determinado punto extremo a través de su canal RAS o de señalización de llamada.

Un punto extremo debería enviar una petición de registro (RRQ, *registration request*) al controlador de acceso. La petición se enviará a la dirección de transporte de canal RAS del controlador de acceso. El punto extremo tiene la dirección de red del controlador de acceso desde el proceso de descubrimiento de aquél y utiliza el identificador TSAP de canal RAS conocido. El controlador de acceso responderá con una confirmación de registro (RCF, *registration confirmation*) o un rechazo de registro (RRJ, *registration reject*), véase la figura 24. Un punto extremo se registrará en un único controlador de acceso.

La RRQ puede repetirse periódicamente (por ejemplo, al arrancar el terminal), con lo que el controlador de acceso podrá tratar múltiples peticiones procedentes del mismo punto extremo. Si un controlador de acceso recibe una RRQ que tiene la misma dirección alias (o lista de direcciones alias) y las mismas direcciones de transporte que una dirección de transporte, responderá con RCF. Si un controlador de acceso recibe una RRQ que tiene la misma dirección alias (o lista de direcciones alias) que un registro activo y direcciones de transporte diferentes, puede confirmar la petición, en particular, si cumple la política de registro. Si la petición no cumple la política de registro del controlador de acceso, éste deberá rechazar el registro indicando registro repetido o no válido. Si el controlador de acceso recibe una RRQ que tiene las mismas direcciones de transporte que un registro activo y una dirección alias (o lista de direcciones alias) diferente y no se especifica que la RRQ sea una RRQ aditiva, deberá sustituir las inscripciones de cuadro de conversión. El controlador de acceso puede tener un método para autenticar estos cambios.

Un punto extremo puede indicar direcciones de transporte de reserva, redundantes o alternativas utilizando la estructura **alternateEndpoint** (**punto extremo alternativo**) dentro de los mensajes RAS. Esto permite que un punto extremo tenga como reserva una interfaz de red secundaria o un punto extremo H.323 secundario. El controlador de acceso rechazará los registros ambiguos. Podrá rechazar el registro por otros motivos, tales como cambios en el descubrimiento o por cuestiones de seguridad.

Si el punto extremo no incluye una dirección alias en el mensaje RRQ, el controlador de acceso puede asignar una. El controlador de acceso devolverá la dirección alias asignada al terminal en el mensaje RCF.

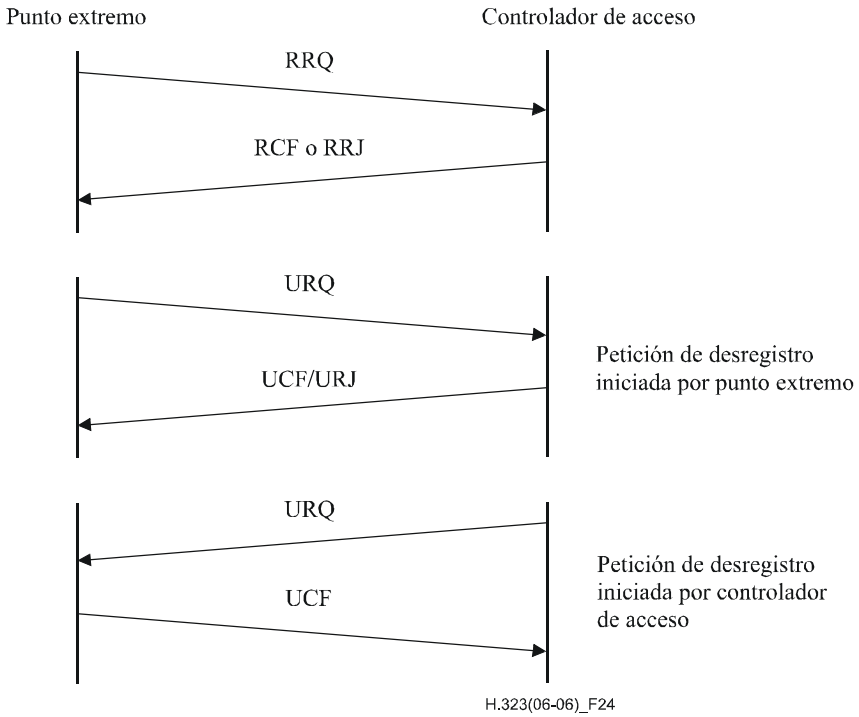


Figura 24/H.323 – Registro

Un punto extremo puede cancelar su registro enviando al controlador de acceso un mensaje de petición de desregistro (URQ, *unregister request*). De esta manera, un punto extremo puede cambiar la dirección alias asociada a su dirección de transporte o viceversa. El controlador de acceso responderá con un mensaje confirmación de desregistro (UCF, *unregister confirmation*) o con un mensaje derechazo de desregistro (URJ, *unregister reject*) de acuerdo con la política del controlador de acceso.

Si el punto extremo envía un mensaje URQ que contenga una lista de direcciones alias, el controlador de acceso sólo desregistrará los alias enumerados en la lista, en caso de que acepte la petición. Si el punto extremo envía un mensaje URQ sin ninguna dirección alias, el controlador de acceso desregistrará todos los alias del punto extremo, si hay alguno, si acepta la petición.

Un controlador de acceso puede cancelar el registro de un punto extremo enviando un mensaje de petición de desregistro (URQ) al punto extremo. El punto extremo responderá con un mensaje de confirmación de desregistro (UCF) y se registrará de nuevo en un controlador de acceso antes de iniciar cualquier llamada. Es posible que para ello haga falta que el punto extremo se registre en un controlador de acceso nuevo.

Si el controlador de acceso envía un mensaje URQ que contenga una lista de direcciones alias, el punto extremo considerará que sólo se desregistran dichas direcciones alias. Un mensaje URQ sin ninguna dirección alias indicará una petición de desregistro del punto extremo.

Un punto extremo que no está registrado en un controlador de acceso se llama punto extremo no registrado. Los puntos extremos de este tipo no solicitan permiso de admisión de un controlador de acceso y, por ello, no pueden participar en las funciones de control de admisiones, control de anchura de banda, conversión de dirección y otras funciones efectuadas por el controlador de acceso.

7.2.2.1 Empleo de mensajes RRQ ligeros

Un registro de punto extremo en un controlador de acceso puede tener una vida finita. Un punto extremo puede solicitar un **timeToLive** (**tiempo de vida**) en el mensaje RRQ al controlador de acceso. El controlador de acceso puede responder con un RCF que contenga el mismo **timeToLive**, uno mayor o uno menor. Si el punto extremo no pudiera acomodar el **timeToLive** mayor propuesto por el controlador de acceso, deberá utilizar el máximo valor de **timeToLive** que pueda soportar, inferior al **timeToLive** propuesto por el controlador de acceso. Transcurrido ese tiempo, el registro expirará. El **timeToLive** se expresa en segundos. Antes del tiempo de expiración, el punto extremo puede enviar un mensaje RRQ que tenga fijado el bit **keepAlive** (**mantener vivo**). El mensaje RRQ mantener vivo puede incluir una cantidad mínima de información como se describe en la Rec. UIT-T H.225.0. El RRQ mantener vivo reiniciará el temporizador de tiempo de vida en el controlador de acceso, permitiendo la ampliación del registro. Transcurrido ese tiempo, el punto extremo debe registrarse nuevamente en un controlador de acceso utilizando el mensaje RRQ completo.

Si el controlador de acceso no incluye un valor **timeToLive** en la RCF, el punto extremo de registro considerará que el controlador de acceso no soporta el mecanismo mantener vivo. Los puntos extremos no enviarán a los controladores de acceso mensajes RRQ que tengan fijado el campo **keepAlive**, lo que indica que no soportan el mecanismo mantener vivo. Un controlador de acceso no debe suponer que un punto extremo soporta el mecanismo mantener vivo salvo que dicho punto extremo facilite un valor **timeToLive** en el RRQ.

Los controladores de acceso no darán curso a un mensaje RRQ con el campo **keepAlive** puesto en registro completo (es decir, para actualizar o inicializar sus tablas de traducción).

Los puntos extremos deberían tener en cuenta los retardos de procesamiento y tratamiento de mensajes cuando determinan el tiempo de expiración de sus registros (es decir, la duración de su propio temporizador de tiempo de vida) en el controlador de acceso.

La expiración del temporizador tiempo de vida en el controlador de acceso produce la expiración del registro del punto extremo. Un controlador de acceso puede enviar una URQ al punto extremo como notificación de dicha expiración. Esto causa la pérdida de sincronización entre los temporizadores de tiempo de vida del controlador de acceso y el punto extremo. También indica la necesidad de un nuevo registro en los puntos extremos que no soportan el mecanismo mantener vivo.

Un punto extremo que envía un mensaje RRQ ligero a su controlador de acceso después que el temporizador tiempo de vida ha expirado en el controlador de acceso, recibirá una respuesta RRJ con la indicación **rejectReason** (**rechazar razón**) de **fullRegistrationRequired** (**registro completo requerido**) o de **discoveryRequired** (**descubrimiento requerido**), en función de los requisitos del controlador de acceso.

Un punto extremo que envía un mensaje ARQ a su controlador de acceso después que el temporizador tiempo de vida ha expirado en el controlador de acceso recibirá un mensaje ARJ con la indicación **rejectReason** de **callerNotRegistered** (**llamador no registrado**) o **calledPartyNotRegistered** (**parte llamada no registrada**). Un punto extremo que inicia una nueva llamada a través de su controlador de acceso después de la expiración del temporizador tiempo de vida del mismo, recibirá un mensaje Liberación Completa con la razón **callerNotRegistered** o **calledPartyNotRegistered**.

La disposición de las llamadas existentes con la expiración del temporizador tiempo de vida depende de la implementación.

7.2.2.2 Utilización de registros aditivos

El soporte de registros aditivos es facultativo tanto en el controlador de acceso como en el punto extremo. Un controlador de acceso que soporte registros aditivos lo indica incluyendo el campo **supportsAdditiveRegistration** (**soporte de registros aditivos**) en el mensaje RCF, al tiempo que cumple los procedimientos que se detallan en esta cláusula. Además, un punto extremo no utilizará el procedimiento de registros aditivos descrito en esta cláusula si el campo **supportsAdditiveRegistration** del RCF no está presente.

Si el controlador de acceso recibe una petición de registro (RRQ) con el campo **additiveRegistration** incluido, considerará que la RRQ es una adición de información a un registro existente para el punto extremo especificado en el campo **endpointIdentifier**. Cuando se recibe una RRQ aditiva, el controlador de acceso añadirá el alias (o la lista de alias) de los campos **terminalAlias** (**alias del terminal**) y **terminalAliasPattern** (**esquema de alias del terminal**) a las entradas de la tabla de traducciones existentes para el punto extremo. Asimismo, el controlador de acceso añadirá los prefijos soportados por el campo **supportedPrefixes** (**prefijos soportados**) del campo **terminalType** a las entradas de la tabla de traducciones existentes para el punto extremo. Cualquier alias de dirección previamente registrada o cualesquiera prefijos soportados por el punto extremo permanecerán registrados. El controlador de acceso sustituirá las direcciones de señalización de llamada y las direcciones RAS del punto extremo con los valores especificados en los campos **callSignalAddress** (**dirección de señal de llamada**) y **rasAddress** (**dirección de ras**), si alguno de ellos está presente, y sustituirá los puntos extremos alternos del punto extremo con los valores incluidos en el campo **alternateEndpoints**, si está presente. El campo **keepAlive** será FALSO si el campo **additiveRegistration** está incluido en la RRQ. Sin embargo, la recepción de una RRQ aditiva hará que el controlador de acceso reinicie el contador del tiempo de vida del punto extremo si es que existe alguno en marcha.

Un punto extremo que envíe una RRQ aditiva a su controlador de acceso cuando el punto extremo no está registrado, recibirá una respuesta RRJ cuya **rejectReason** es **fullRegistrationRequired** o **discoveryRequired**, dependiendo de cuales sean los requisitos del controlador de acceso.

NOTA – Puesto que la RRQ aditiva no constituye un registro completo, el controlador de acceso puede ignorar los campos en la RRQ aditiva a los que no se hace referencia específica en esta cláusula.

7.2.3 Localización de punto extremo

Un punto extremo o un controlador de acceso que tiene una dirección alias para un punto extremo y quisiera determinar su información de contacto puede emitir un mensaje de petición de localización (LRQ, *location request*). Este mensaje puede ser enviado al identificador TSAP de canal RAS del controlador de acceso específico o puede ser multidifundido como el mensaje GRQ a la dirección de multidifusión de descubrimiento conocida del controlador de acceso. El controlador de acceso con el que está registrado el punto extremo solicitado responderá con el mensaje de confirmación de localización (LCF, *location confirmation*) que contiene información de contacto del punto extremo o del controlador de acceso del punto extremo. La información de contacto incluirá las direcciones del canal de señalización de llamada y del canal RAS que han de utilizarse para alcanzar el punto extremo y opcionalmente información de destino adicional que puede proporcionar información de marcación e información de extensión relativa al punto extremo solicitado.

Todos los controladores de acceso en los que no está registrado el punto extremo solicitado, devolverán un mensaje de rechazo de localización (LRJ, *location reject*) si han recibido el LRQ por el canal RAS. Los controladores de acceso en los que no está registrado el punto extremo no responderán a LRQ si reciben el LRQ en la dirección multidifusión de descubrimiento.

Un punto extremo o un controlador de acceso puede incluir una o más extensiones de **dialledDigits** o de **partyNumber** que desea conectar en el campo **destinationInfo** (**información de destino**) del LRQ para tratar de localizar una pasarela disponible fuera de su zona. Un controlador de acceso que recibe un LRQ solicitando una pasarela disponible no está obligado a hacer sus pasarelas disponibles a dicha petición.

Un controlador de acceso puede conocer la dirección alias y la información de conexión de los puntos extremos en la RCC. Este controlador de acceso podría responder a un LRQ solicitando información sobre el punto extremo de la RCC con la información de conexión necesaria para alcanzar ese punto extremo. Ésta incluiría la información necesaria para direccionar la pasarela, así como el punto extremo de la RCC. Téngase en cuenta que el punto extremo de la RCC no está registrado en el controlador de acceso en el sentido de que intercambia mensajes RRQ/RCF con el controlador de acceso. El método por el cual el controlador de acceso conoce la información de punto extremo de la RCC cae fuera del alcance de esta Recomendación.

7.2.4 Admisiones, cambio de anchura de banda, situación y liberación

El canal RAS se emplea también para la transmisión de mensajes de admisiones, cambio de anchura de banda, situación y liberación. Estos mensajes se producen entre un punto extremo y un controlador de acceso y se utilizan para proporcionar funciones de control de admisiones y gestión de anchura de banda. La utilización detallada de estos mensajes se describe en la cláusula 8.

El mensaje de petición de admisión (ARQ, *admission request*) especifica la anchura de banda de la llamada pedida. Se trata de un límite superior a la velocidad binaria agregada de todos los canales de audio y de vídeo transmitidos y recibidos, excluidos los encabezamientos RTP, los encabezamientos de parte útil RTP, los encabezamientos de red y otras taras. Los canales de datos y de control no se incluyen en este límite. El controlador de acceso puede reducir la anchura de banda de llamada pedida en el mensaje de confirmación de admisión (ACF, *admission confirm*). Un punto extremo deberá garantizar que la velocidad binaria agregada promediada en un segundo de todos los canales de audio y de vídeo transmitidos y recibidos es igual o inferior a la anchura de banda de llamada. Un punto extremo o el controlador de acceso puede intentar modificar la anchura de banda de llamada durante una llamada utilizando el mensaje de petición de cambio de ancho de banda (BRQ, *bandwidth change request*).

El mensaje de secuencia de confirmación de admisión permite al control de acceso proporcionar una única respuesta a un ARQ que contenga información de encaminamiento alternativo, información de origen diferente, testigos diferentes, etc. Cuando un punto extremo recibe un mensaje de secuencia de confirmación de admisión conteniendo más de un ACF, procesará el primer ACF de la secuencia intentando establecer la comunicación con arreglo a lo descrito en esta Recomendación. En el caso de que el punto extremo sea incapaz de establecer la comunicación debido a algún fallo imprevisto, el punto extremo puede seleccionar el siguiente mensaje ACF de la secuencia y volver a intentar establecer la comunicación sin tener que consultar previamente al controlador de acceso. Sin que ello afecte a la definición, entre los "fallos imprevistos" se pueden encontrar los circuitos ocupados; los problemas con el encaminamiento del transporte (por ejemplo "no hay camino hacia el anfitrión"); o el agotamiento de los recursos de la pasarela. Corresponde al punto extremo decidir el intentar establecer comunicaciones por rutas alternativas cuando se presenta un fallo de encaminamiento.

Los puntos extremos que opten por soportar el mensaje de secuencia de confirmación de admisión deberán señalar que disponen de esta capacidad poniendo el campo **acfSequences** del mensaje RRQ a TRUE (VERDADERO). El controlador de acceso interpretará la ausencia de este campo como el valor FALSE (FALSO). Los controladores de acceso no enviarán el mensaje de secuencia de confirmación de admisión a los puntos extremos que no hayan indicado en el RRQ que soportan este mensaje. Un punto extremo puede modificar el valor del campo **acfSequences** en los mensajes RRQ subsiguientes. Cuando el punto extremo modifique este valor de TRUE a FALSE, el punto extremo estará preparado para recibir los mensajes de secuencia de confirmación de admisión que

pudieran estar en camino como resultado de haber anunciado con anterioridad el soporte de los mensajes de secuencia de confirmación de admisión.

Dado que la secuencia de confirmación de admisión constituye simplemente un medio de proporcionar información de encaminamiento alternativo que no podía facilitarse en un mensaje de confirmación de admisión, esta Recomendación no establece más distinciones en ninguno de sus puntos, en cuanto a la diferencia semántica entre el mensaje de confirmación de admisión y el mensaje de secuencia de confirmación de admisión. En toda la Recomendación, "confirmación de admisión" o "ACF" se refiere o bien a un único mensaje de confirmación de admisión o a un mensaje de secuencia de confirmación de admisión.

7.2.5 Testigos de acceso

Un testigo de acceso es una cadena que se pasa en algunos mensajes RAS y en el mensaje Establecimiento. Los testigos de acceso tienen dos usos. En primer lugar, pueden ofrecer privacidad protegiendo una información de dirección de transporte y dirección alias de un punto extremo contra una parte llamante. Un usuario puede revelar sólo el testigo de acceso que ha de utilizar una parte llamante para alcanzar el punto extremo. El controlador de acceso conocerá el punto extremo correspondiente al testigo de acceso a partir del proceso de registro, por lo que las llamadas que utilizan el testigo de acceso pueden ser encaminadas a través del controlador de acceso al punto extremo llamado. La utilización del testigo de acceso se aplica únicamente al modelo de llamada encaminada al controlador de acceso cuando se intenta ocultar la dirección de transporte desde el punto extremo.

El segundo uso del testigo de acceso es asegurar que las llamadas se encaminan correctamente a través de entidades H.323. Un testigo de acceso retornado por un controlador de acceso se utilizará en cualesquiera mensajes establecimiento posteriores enviados por el punto extremo. Este testigo de acceso puede ser utilizado por una pasarela para asegurar que el punto extremo tiene permiso para utilizar los recursos de pasarela, o puede ser utilizado por un punto extremo llamado para asegurar que el punto extremo llamante pueda señalizarlo directamente.

El testigo de acceso puede también ser distribuido por métodos fuera de banda para asegurar el acceso adecuado a las pasarelas y puntos extremos de los sistemas que no tienen controladores de acceso.

7.2.6 Procedimientos de controlador de acceso alternativo

Con el fin de asegurar la disponibilidad, redundancia y escalabilidad del sistema, el controlador de acceso puede proporcionar la función de señalización RAS utilizando múltiples dispositivos físicos o lógicos, a los que se hace referencia como controladores de acceso alternativos. Si el punto extremo soporta los procedimientos de controlador de acceso alternativo definidos en esta cláusula, debe asimismo incluir el campo **supportsAltGK** (**soporte de controlador de acceso alternativo**) en los mensajes GRQ y RRQ.

Cuando un punto extremo inicia una comunicación con el controlador de acceso, puede recibir una lista de controladores de acceso alternativos mediante el mensaje GCF. Si el controlador de acceso no responde a mensajes RRQ posteriores, el punto extremo intentará registrarse con el controlador de acceso utilizando la lista de controladores de acceso alternativos proporcionados en el mensaje GCF. Si ningún controlador de acceso alternativo responde, el punto extremo reiniciará el proceso de descubrimiento del controlador de acceso.

Si el punto extremo recibe un mensaje GRJ que contenga información de controladores de acceso alternativos y no recibe un mensaje GCF, enviará mensajes GRQ a uno o más controladores de acceso alternativos de la lista de controladores de acceso alternativos recibida en el mensaje GRJ. Si se reciben varios mensajes GRJ, el punto extremo puede seleccionar uno de los mensajes GRJ del cual extraer información sobre controladores de acceso alternativos. Si ningún controlador de acceso alternativo envía un mensaje GCF, el punto extremo puede intentar utilizar cualquier lista de

controladores de acceso alternativos nueva recibida para el descubrimiento del controlador de acceso, o bien puede iniciar de nuevo el proceso de descubrimiento de controlador de acceso.

Si el punto extremo no se ha registrado con el controlador de acceso o ha reiniciado el proceso de descubrimiento del controlador de acceso, ignorará el campo **needToRegister** (**necesidad de registro**) de la lista de controladores de acceso alternativos y considerará que el valor es VERDADERO.

Si el punto extremo se ha registrado con el controlador de acceso y éste deja de responder, el punto extremo intentará comunicarse con un controlador de acceso alternativo. Por consiguiente, el punto extremo puede utilizar los procedimientos de controlador de acceso asignado que se definen en 7.2.6.1 para registrarse nuevamente de manera automática en su controlador de acceso primario cuando éste quede nuevamente disponible.

El controlador de acceso puede redireccionar explícitamente un punto extremo a un controlador de acceso alternativo devolviendo un mensaje de rechazo RAS con una lista de controladores de acceso alternativos. Si en dicha redirección el campo **altGKisPermanent** (**controlador de acceso alternativo permanente**) es FALSO, la redirección se considera temporal ya que sólo se aplica a un único mensaje RAS.

Un controlador de acceso puede enviar un mensaje URQ a un punto extremo con una lista de controladores de acceso alternativos, en cuyo caso el punto extremo responderá con un mensaje UCF e intentará comunicarse con un controlador de acceso alternativo. Un punto extremo no incluirá ninguna lista de controladores de acceso alternativos en los mensajes URQ que envíe.

Un punto extremo sólo mantendrá una lista de controladores de acceso alternativos. Dicha lista será la última lista recibida en un mensaje RAS, con la excepción de que si el punto extremo ha sido redireccionado temporalmente a un controlador de acceso alternativo y el controlador de acceso alternativo devuelve un mensaje de rechazo con una lista de controladores de acceso alternativos (incluso si la lista está vacía), el punto extremo interpretará el rechazo como una redirección. El punto extremo puede ignorar la lista de controladores de acceso alternativos que se proporciona en dicha redirección y continuar utilizando la lista de controladores de acceso alternativos recibida en el mensaje de rechazo original.

Si el controlador de acceso desea eliminar de la lista del punto extremo los controladores de acceso alternativos, por ejemplo, cuando el controlador de acceso se reconfigura para no utilizar controladores de acceso alternativos, deberá devolver una lista vacía, que es una lista con elementos cero, de controladores de acceso alternativos al punto extremo en el mensaje RCF. Si se omite el parámetro opcional **alternateGatekeeper** en el mensaje RCF, se indica al punto extremo que conserve la lista de controladores de acceso vigente.

El punto extremo utilizará el campo **priority** (**prioridad**) para indicar el orden en el que se comunica con los controladores de acceso alternativos. Si varios controladores de acceso alternativos tiene el mismo valor del campo **priority**, el punto extremo puede ordenar los controladores de acceso alternativos que tienen el mismo valor de **priority** tal como él decida.

Cuando un punto extremo es redireccionado a un controlador de acceso alternativo, ignorará el campo **needToRegister** y supondrá que su valor es FALSO, retransmitiendo sólo el mensaje RAS redireccionado a un controlador de acceso alternativo temporal. Los restantes mensajes RAS se seguirán enviando al controlador de acceso tal como es habitual. Obsérvese que ello no impide que el controlador de acceso redireccione temporalmente un punto extremo a un controlador de acceso alternativo devolviendo un mensaje RRJ a un mensaje RRQ o a un mensaje RRQ ligero.

Si distintas peticiones RAS son redireccionadas a controladores de acceso alternativos temporales, cada uno de los mensajes se enviará cada vez a un único controlador de acceso alternativo temporal, aunque distintos mensajes RAS puedan ser enviados a distintos controladores de acceso alternativos temporales simultáneamente. Si el punto extremo determina que un controlador de acceso

alternativo no responde, intentará retransmitir la petición RAS a otro controlador de acceso alternativo. Si ninguno de los controladores de acceso alternativos responde a una petición RAS, el punto extremo considerará que la petición RAS ha sido rechazada. Si la petición había sido una RRQ, el punto extremo reiniciará el proceso de descubrimiento del controlador de acceso.

Si el controlador de acceso deja de responder o si redirecciona el punto extremo devolviéndole una lista de controladores de acceso alternativos con el campo **altGKisPermanent** puesto a VERDADERO, el punto extremo intentará comunicarse con un controlador de acceso alternativo. El punto extremo sólo intentará la comunicación con un controlador de acceso alternativo. Sólo después de que el punto extremo determine que el controlador de acceso alternativo no responde, intentará la comunicación con el siguiente controlador de acceso alternativo. Si ninguno de los controladores de acceso alternativos responde, el punto extremo reiniciará el proceso de descubrimiento del controlador de acceso. Si es necesario el registro con un controlador de acceso alternativo, el punto extremo intentará en primer lugar enviar un mensaje RRQ al controlador de acceso alternativo, en lugar de un mensaje GRQ. Sólo si el controlador de acceso devuelve un mensaje RRJ cuyo motivo sea **discoveryRequired**, el punto extremo enviará un mensaje GRQ al controlador de acceso alternativo. Cuando el punto extremo se encuentre permanentemente en transición a un controlador de acceso alternativo, enviará todos los mensajes RAS restantes al controlador de acceso alternativo, incluyendo las peticiones RAS pendientes cuya temporización haya vencido. El punto extremo debe reiniciar los contadores de reintentos para todos los mensajes RAS pendientes antes de transmitirlos al controlador de acceso alternativo por primera vez. En ese caso, el punto extremo puede utilizar los procedimientos de controlador de acceso asignado definidos en 7.2.6.1 para volver a registrarse automáticamente en su controlador de acceso primario cuando éste quede nuevamente disponible.

Si un controlador de acceso alternativo al que se ha redireccionado un punto extremo devuelve un mensaje de rechazo sin una lista de controladores de acceso alternativos, el punto extremo aceptará el mensaje como un rechazo del mensaje original. Si lo que se rechazó fue un mensaje RRQ, el punto extremo reiniciará el proceso de descubrimiento del controlador de acceso. Si el controlador de acceso alternativo redirecciona el punto extremo devolviendo un mensaje de rechazo con una lista de controladores de acceso alternativos, el punto extremo intentará enviar la petición a otro controlador de acceso alternativo. Si todos los controladores de acceso alternativos redireccionan el punto extremo, éste considerará en última instancia que la petición ha sido rechazada.

Un punto extremo no enviará un mensaje URQ cuando se encuentre cambiando de controlador de acceso alternativo, aunque el campo **needToRegister** sea VERDADERO, excepto en el caso en que el controlador de acceso envíe un mensaje URQ con una lista de controladores de acceso alternativos.

Si un punto extremo se redirecciona a un controlador de acceso alternativo especificado como permanente (es decir, el campo **altGKisPermanent** es VERDADERO) o si se vio forzado a iniciar la comunicación con un controlador de acceso alternativo después de que su controlador de acceso haya dejado de responder, considerará que el controlador de acceso alternativo está preparado para aceptar peticiones relativas a llamadas existentes. Enviará todos los mensajes BRQ, DRQ e IRR relativos a llamadas en curso al controlador de acceso alternativo. Asimismo, el controlador de acceso alternativo está preparado para manejar dichos mensajes. En ese caso, el punto extremo puede utilizar los procedimientos de controlador de acceso asignado definidos en 7.2.6.1 para volver a registrarse automáticamente en su controlador de acceso primario cuando éste quede nuevamente disponible.

Si un punto extremo comienza la comunicación con un controlador de acceso alternativo con el que no era necesario realizar el registro, incluyendo controladores de acceso alternativos temporales, el campo **gatekeeperIdentifier** (**identificador de controlador de acceso**) de los mensajes URQ, ARQ, BRQ, LRQ y DRQ contendrá el campo **gatekeeperIdentifier** del controlador de acceso

alternativo de la lista de controladores de acceso alternativos. Este campo puede no estar presente cuando se requiere el registro.

7.2.6.1 Procedimientos de controlador de acceso asignado

El controlador de acceso asignado es una extensión opcional del procedimiento de controlador de acceso alternativo examinado precedentemente. La combinación de esos dos procedimientos brinda un esquema de redundancia más sólido que permite al punto extremo "fallar con respecto" a uno de sus controladores de acceso alternativos cuando su controlador de acceso asignado no responde, y entonces "reenviarlo" a su controlador de acceso asignado cuando responda nuevamente.

El campo **assignedGatekeeper** (controlador de acceso asignado) sólo se incluirá en mensajes procedentes del controlador de acceso si el campo **alternateGatekeeper** también está presente, incluso si la lista de **alternateGatekeeper** está vacía. Si el punto extremo soporta los procedimientos de controlador de acceso asignado definidos en este párrafo, incluirá el campo **supportsAssignedGK** en sus mensajes GRQ y RRQ.

En un momento determinado, sólo puede designarse un controlador de acceso como controlador de acceso asignado de puntos extremos. La dirección del controlador de acceso asignado se comunica al punto extremo en el campo **assignedGatekeeper** de los mensajes GCF, RCF/RRJ, ACF/ARJ, UCF, DCF e IRQ. En el caso en que el punto extremo utilice el mecanismo de multidifusión GRQ para descubrir dinámicamente un controlador de acceso disponible, y si responden más de un controlador de acceso, el controlador de acceso asignado será el especificado en el mensaje GCF seleccionado por el punto extremo, conforme a 7.2.1.

La dirección del **assignedGatekeeper** puede cambiar a lo largo del tiempo. Cada vez que el punto extremo recibe una dirección **assignedGatekeeper** que es diferente a su dirección **assignedGatekeeper** vigente, el punto extremo aceptará la dirección como la de su nuevo controlador de acceso asignado e inmediatamente comenzará a poner en práctica el procedimiento de reenvío descrito en esta cláusula para registrarse con él. Esto proporciona al administrador un método automático para cambiar el controlador de acceso asignado de los puntos extremo sin tener que programarlos nuevamente. El método utilizado por el controlador de acceso para almacenar esta asociación entre punto extremo y controlador de acceso está fuera del ámbito de esta Recomendación, pero se supone que el controlador de acceso mantiene algún tipo de banco de datos para almacenar esa información y proporcionar algún tipo de interfaz para que el administrador aprovisione a esas asociaciones.

La funcionalidad de reenvío puede ser suministrada tanto por el controlador de acceso como por el punto extremo, conforme a lo que se describe a continuación. El punto extremo utilizará el modelo especificado por el controlador de acceso en el cual está actualmente registrado. Si el controlador de acceso no especifica ningún modelo, **endpointBased** será el modelo por defecto.

1) **Funcionalidad basada en el controlador de acceso**

   Cuando el punto extremo se registre en el controlador de acceso alternativo indicará cuál es su controlador de acceso asignado vigente en el mensaje RRQ. Después del registro del punto extremo, el controlador de acceso alternativo puede utilizar el mecanismo GRQ que se describe más adelante para determinar si el controlador de acceso asignado del punto extremo se encuentra activo. Una alternativa es que puede escoger utilizar un mecanismo propietario a fin de determinar el estado del controlador de acceso de punto extremo y en qué momento solicitar que el punto extremo se registre en el controlador de acceso asignado.

   Un controlador de acceso alternativo que utilice el mecanismo GRQ para determinar si el controlador de acceso asignado de punto extremo se encuentra activo enviará mensajes GRQ periódicos al controlador de acceso asignado de punto extremo para determinar si se encuentra activo. El intervalo entre dos mensajes GRQ será de por lo menos 60 segundos. Al recibir un GCF del controlador de acceso asignado, deberá enviar un URQ con la

información del campo del controlador de acceso asignado en el campo alternativo GK, y el motivo URQ deberá ponerse en **registerWithAssignedGK**. También puede enviar un mensaje RRJ con RegistrationRejectReason puesto en **registerWithAssignedGK** o un mensaje ARJ con AdmissionRejectReason puesto en **registerWithAssignedGK** para solicitar el reenvío del punto extremo. Al utilizar este modelo, el punto extremo no sondeará a su controlador de acceso asignado mediante el envío de sus propios mensajes periódico GRQ.

El campo **endpointType** contendrá, en los mensajes GRQ enviados desde el controlador de acceso alternativo hacia el controlador de acceso asignado, el campo **gatekeeper**.

Un controlador de acceso asignado que recibe un mensaje GRQ enviado por el controlador de acceso alternativo responderá con un mensaje GCF sólo si se encuentra activo y es capaz de recibir registros nuevos. No enviará un mensaje GCF en caso de recibir un pequeño número de registros adicionales que produzcan una sobrecarga por la cual los puntos extremos se intercambiarán entre ambos controladores de acceso. La determinación del punto a partir del cual se produce sobrecarga está fuera del ámbito de esta Recomendación.

2) **Funcionalidad basada en el punto extremo**

Cuando un controlador de acceso asignado de punto extremo no responde, el punto extremo comenzará a aplicar un mecanismo de sondeo mediante el envío periódico de mensajes GRQ a su controlador de acceso asignado a fin de obtener el reenvío lo antes posible. Una vez que el controlador de acceso asignado comienza a responder nuevamente (es decir, el punto extremo recibe un mensaje GCF como respuesta a uno de sus mensajes GRQ) el punto extremo procurará obtener el reenvío a su controlador de acceso asignado enviándole un mensaje RRQ. Si el punto extremo está registrado en otro controlador de acceso cuando procura iniciar este procedimiento de reenvío, no necesita enviar un mensaje URQ a su controlador de acceso vigente.

El modelo de reenvío "basado en el controlador de acceso" tiene la ventaja, si se le compara con el modelo de reenvío "basado en el punto extremo", de que reduce el tráfico de mensajes GRQ. Si tanto el punto extremo como el controlador de acceso soportan el reenvío, el controlador de acceso especificará cuál de los dos modelos se ha de utilizar en el **rehomingModel** de los campos GCF y RCF.

El intervalo con que se envían los mensajes GRQ al controlador de acceso asignado no debe ser inferior a 60 segundos. Ello se aplica tanto al modelo basado en el controlador de acceso como al basado en el punto extremo.

El campo **assignedGatekeeper** que figura en los mensajes enviados del punto extremo al controlador de acceso indica cuál es el controlador de acceso asignado vigente del punto extremo. El campo **assignedGatekeeper** que figura en los mensajes enviados del controlador de acceso al punto extremo se utiliza para establecer el controlador de acceso asignado del punto extremo.

El punto extremo supondrá que, al ser reenviado, el controlador de acceso asignado estará preparado para aceptar las peticiones relativas a las llamadas existentes, y el nuevo controlador de acceso asignado estará preparado para manejar esos mensajes. Ello permite que las llamadas activas y los mensajes pendientes entre el punto extremo y el controlador de acceso vigente continúen durante el procedimiento de reenvío. Si el punto extremo recibe una respuesta a una petición pendiente de un controlador de acceso después de efectuar el reenvío a su controlador de acceso asignado, el punto extremo aceptará la respuesta y procederá normalmente. Después del reenvío, todos los mensajes recientemente generados o retransmitidos relacionados esa llamada y las llamadas activas existentes, se direccionarán hacia el controlador de acceso asignado en el cual está actualmente registrado. Durante esta transición puede haber un periodo de tiempo corto durante el cual los controladores de acceso aún no se han sincronizado con respecto al estado del registro

de los puntos extremos y ambos controladores de acceso envían mensajes IRQ al punto extremo para determinar el estado de la llamada. El punto extremo responderá sólo a los mensajes IRQ procedentes del controlador de acceso asignado en el cual está actualmente registrado.

Si el punto extremo recibe un mensaje de rechazo procedente de su controlador de acceso, como mensaje GRJ, RRJ o ARJ (o recibe un mensaje URQ procedente de su controlador de acceso), con una lista de controladores de acceso alternativos y el campo **altGKisPermanent** se pone a VERDADERO, el punto extremo seguirá los procedimientos de controlador de acceso alternativo que se describen en 7.2.6, considerando que el campo **needToRegister** es VERDADERO y enviando un mensaje RRQ a uno de sus controladores de acceso alternativo. No obstante, si se está utilizando el modelo de reenvío basado en el punto extremo, el punto extremo deberá, asimismo, iniciar inmediatamente el mecanismo de sondeo descrito a fin de efectuar el reenvío a su controlador de acceso asignado lo antes posible. Si el controlador de acceso desea reencaminar de manera permanente el punto extremo hacia un controlador de acceso alternativo y no desea reenviarle el punto extremo, deberá proporcionar al punto extremo una nueva dirección **assignedGatekeeper** o suprimir el valor de controlador de acceso asignado mediante el envío de un campo vacío **assignedGatekeeper**.

Cada vez que el punto extremo recibe una nueva dirección **assignedGatekeeper**, ignorará el campo **needToRegister** y supondrá que el valor es VERDADERO. Si el campo **altGKisPermanent** se pone en FALSO, y la dirección del campo assignedGatekeeper (controlador de acceso asignado) es diferente del valor del controlador de acceso asignado vigente de los puntos extremos, el punto extremo ignorará el hecho de que el campo **altGKisPermanent** se haya puesto a FALSO y retransmitirá el mensaje a su nuevo controlador de acceso asignado. Sólo si este controlador de acceso no responde, el punto extremo procederá a seguir los procedimientos de controlador de acceso alternativo que se describen en 7.2.6 mediante la retransmisión del mensaje a su lista de controladores de acceso alternativos. Si se está utilizando el modelo de reenvío basado en el punto extremo, deberá iniciar inmediatamente el mecanismo de sondeo que se describe en esta cláusula a fin de efectuar el reenvío al nuevo controlador de acceso asignado. El punto extremo puede efectuar esas dos acciones en paralelo.

El controlador de acceso puede incluir el campo **assignedGatekeeper** en cualquier mensaje GCF, RCF/RRJ, ACF/ARJ, UCF, DCF o IRQ. Si la dirección proporcionada es diferente del valor del controlador de acceso asignado vigente del punto extremo, y si se está utilizando el modelo de reenvío basado en el punto extremo, el punto extremo iniciará inmediatamente el mecanismo de sondeo precedentemente descrito a fin de efectuar el reenvío a su nuevo controlador de acceso asignado.

El controlador de acceso puede comprender opcionalmente un valor **gatekeeperIdentifier** en el campo **assignedGatekeeper**. Esto es útil cuando el controlador de acceso asignado gestiona múltiples zonas y, por consiguiente tiene configurados múltiples **gatekeeper identifiers** (**identificadores de controlador de acceso**). Si el **gatekeeperIdentifier** enviado por el punto extremo no corresponde a ninguno de los identificadores de controladores de acceso configurados, el controlador de acceso enviará de retorno un mensaje de rechazo. Ese mensaje de rechazo puede incluir el valor correcto de **gatekeeperIdentifier** en el campo **assignedGatekeeper**, en cuyo caso el punto extremo transmitirá la petición con el valor correcto de **gatekeeperIdentifier**. Una alternativa consiste en que el controlador de acceso proporcione un valor vacío de **gatekeeperIdentifier** en el campo **assignedGatekeeper**, en cuyo caso el punto extremo retransmitirá la petición con un valor de **gatekeeperIdentifier** vacío.

7.2.7 Comunicación de información de utilización

Un punto extremo puede poder recopilar y comunicar su información de utilización de llamada, lo cual puede ser útil con fines de contabilidad y facturación. Un controlador de acceso puede solicitar que un punto extremo comunique esta información. Esta característica pretende permitir el interfuncionamiento con las características de comunicación de la información de utilización de los sistemas que implementan el anexo G/H.225.0.

Obsérvese que esta característica está pensada para escenarios en los que el punto extremo del que se solicita la información de utilización es fiable, tal como ocurre cuando una pasarela y un controlador de acceso son administrados por el mismo proveedor de servicios. Es decir, se asume que el punto extremo comunica con precisión su información de utilización.

7.2.7.1 Anuncio de las capacidades de comunicación de la información de utilización

Un punto extremo puede anunciar a un controlador de acceso su capacidad de recopilar y comunicar información de utilización. Estas capacidades las especifica el campo **usageReportingCapability** (**capacidad de comunicación de utilización**) del mensaje RRQ. Si el punto extremo ha comunicado sus capacidades y éstas cambian ulteriormente, el punto extremo enviará otro mensaje RRQ especificando sus capacidades. La ausencia de un campo **usageReportingCapability** en un mensaje RRQ indica que el punto extremo no puede comunicar información de utilización.

7.2.7.2 Solicitud de comunicaciones de información de utilización

Un controlador de acceso puede solicitar información de utilización de un punto extremo por medio de los mensajes RCF, ACF e IRQ. Un controlador de acceso debería considerar que si un punto extremo que no ha anunciado su capacidad para comunicar un tipo particular de información de utilización, es porque no comunicará nada acerca de dicha información, no debiendo solicitar esa información del punto extremo.

Un controlador de acceso puede solicitar información de utilización mediante el campo **usageSpec** (**especificación de utilización**) del mensaje RCF. Esta petición es la **usageSpec** "por defecto". Incluyendo este campo, el controlador de acceso solicita que el punto extremo recopile y comunique la información de utilización especificada para todas las llamadas nuevas. La petición no se aplica a las llamadas en curso.

Una vez que el controlador de acceso ha entregado una **usageSpec** por defecto mediante el mensaje RCF, considera que la petición sigue siendo válida hasta que emite otra **usageSpec** por defecto. Si el controlador de acceso no desea modificar una **usageSpec** por defecto previamente emitida, puede indicarlo no incluyendo la **usageSpec** cuando envía un mensaje RCF. Para modificar una petición de información de utilización por defecto previa, un controlador de acceso enviará una nueva **usageSpec** en su siguiente mensaje RCF. Para solicitar que un punto extremo deje de comunicar información de utilización, un controlador de acceso enviará una **usageSpec** sin que los campos **when** (**cuando**) o **required** (**requerida**) incluyan opción alguna.

Un controlador de acceso puede solicitar información de utilización para una llamada en particular mediante el campo **usageSpec** del mensaje ACF de dicha llamada. Esta petición se denomina **usageSpec** "por llamada". Si existe, esta petición sustituye para dicha llamada a cualquier especificación de utilización por defecto que el controlador de acceso haya podido proporcionar en un mensaje RCF.

Un controlador de acceso puede también solicitar información de utilización para una llamada concreta mediante el campo **usageInfoRequested** (**información de utilización solicitada**) de un mensaje IRQ. La respuesta a esta petición debe venir inmediatamente a continuación en un mensaje IRR. Esta petición no afecta a la especificación de utilización por defecto enviada mediante un mensaje RFC o la especificación de utilización por llamada enviada mediante un mensaje ACF.

Un controlador de acceso que desee que un punto extremo comunique información de utilización periódicamente en mensajes IRR no solicitados, lo indicará seleccionando la opción **inIrr** del campo **when** de **usageSpec**. También especificará **irrFrequencyInCall** (**frecuencia de irr en la llamada**) en el campo **preGrantedARQ** (**ARQ previamente concedida**) del mensaje RCF, o **irrFrequency** en el mensaje ACF, según proceda para una llamada en particular.

Un controlador de acceso que solicite que la información de utilización se comunique al principio de una llamada o en mensajes IRR no solicitados (es decir, que seleccione las opciones **start** o **inIrr** en el campo **when** de **usageSpec**) debería acusar recibo de los mensajes IRR para asegurar que la información de utilización solicitada se entrega de forma fiable. Para indicar que acusará recibo de los mensajes IRR, el controlador de acceso pone el campo **willRespondToIRR** (**responderá a IRR**) del mensaje RCF o ACF a VERDADERO.

7.2.7.3 Envío de comunicaciones de información de utilización

Un punto extremo puede comunicar a un controlador de acceso información de utilización mediante los mensajes BRQ, IRR y los mensajes DRQ y DCF. Un punto extremo puede enviar información de utilización a un controlador de acceso que no la haya solicitado. Si un punto extremo anuncia su capacidad para recopilar y comunicar un tipo particular de información de utilización y un controlador de acceso solicita dicha información, el punto extremo comunicará la información solicitada. Un punto extremo ignorará peticiones erróneas relativas a información de utilización (tales como una petición de la hora de terminación de la llamada al inicio de la misma). Un punto extremo puede ignorar una petición de información de utilización que no entre dentro de las capacidades de comunicación anunciadas por el mismo.

Si un controlador de acceso envía a un punto extremo una **usageSpec** por defecto en un mensaje RCF, el punto extremo fijará los parámetros de comunicación de información de utilización para todas las nuevas llamadas sobre la base de esta plantilla, salvo que el controlador de acceso suministre una **usageSpec** por llamada para una llamada en concreto en un mensaje ACF. Si así ocurre, la **usageSpec** por llamada sustituye a la **usageSpec** por defecto para dicha llamada. Un punto extremo puede aplicar una **usageSpec** por defecto actualizada a las llamadas existentes para las que no se hubiese proporcionado una **usageSpec** por llamada.

Un punto extremo interpretará una **usageSpec** sin opciones que haya sido seleccionada en los campos **when** o **required**, como una petición de no comunicar información de utilización.

Cuando se comunica información de utilización mediante un mensaje IRR, y el controlador de acceso ha indicado mediante el campo **willRespondToIRR** de un mensaje RCF o ACF que acusará recibo de los mensajes IRR, un punto extremo fijará el campo **needResponse** a VERDADERO y retransmitirá la información si no se recibe un acuse de recibo. Esta regla se aplica con independencia de que el mensaje IRR sea solicitado o no solicitado.

Si el controlador de acceso ha solicitado que la información de utilización se comunique al inicio de la llamada (es decir, se ha seleccionado **start** del campo **when** de **usageSpec**), y la información solicitada forma parte de las capacidades de anunciadas de comunicación del punto extremo, éste informará sobre la información solicitada inmediatamente después del inicio de la llamada. Si el punto extremo envía una BRQ en ese instante, puede incluir la información de utilización solicitada en el campo **usageInformation** (**información de utilización**) del mensaje BRQ. En cualquier otro caso, el punto extremo enviará un mensaje IRR no solicitado con la información de utilización solicitada en el campo **usageInformation** por llamada.

Si el controlador de acceso ha solicitado que la información de utilización debe comunicarse al final de la llamada (es decir, ha seleccionado **end** en el campo **when** de **usageSpec**), y la información solicitada forma parte de las capacidades anunciadas de comunicación del punto extremo, éste informará sobre la información solicitada inmediatamente después del final de la llamada en el mensaje DRQ (o en el DCF si la llamada es terminada por parte del controlador de acceso).

Si el controlador de acceso ha solicitado que la información de utilización debe comunicarse en mensajes IRR no solicitados (es decir, ha seleccionado **inIrr** en el campo **when** de **usageSpec**), y la información solicitada forma parte de las capacidades de anunciadas de comunicación del punto extremo, éste informará sobre la información solicitada en cada mensaje IRR no solicitado que envíe.

El punto extremo no aplicará la **usageSpec** por defecto ni por llamada cuando envíe mensajes IRR solicitados (es decir, respuestas a mensajes IRQ). Si el controlador de acceso solicita información de utilización mediante el campo **usageInfoRequested** del mensaje IRQ, y si dicha información está incluida en las capacidades de comunicación de información anunciadas por el punto extremo, éste comunicará la información solicitada en el campo **usageInformation** por llamada del mensaje IRR. Si el controlador de acceso no solicitó información de utilización en el mensaje IRR, el punto extremo no debería incluir un campo **usageInformation** en la respuesta.

7.2.8 Capacidades relacionadas con el crédito de una llamada

Un punto extremo puede recibir del controlador de acceso, utilizando las capacidades facultativas relativas al crédito de la llamada, información sobre la situación de crédito o de débito de un usuario antes y después de que el usuario establezca una comunicación. A su vez, el punto extremo puede retransmitir esta información al usuario final mediante un anuncio. El punto extremo tiene también la capacidad de limitar la duración de la llamada del usuario a un tiempo por él especificado. Así, el punto extremo puede deshacer la llamada cuando se haya terminado el tiempo o el dinero de la cuenta del usuario.

Además, el controlador de acceso puede enviar al punto extremo avisos relativos a la situación del balance y puede indicar un límite en la duración de las llamadas al punto extremo.

7.2.8.1 Avisos del punto extremo sobre capacidades relativas al crédito

El punto extremo indica que soporta las características relativas al crédito de llamadas mediante el mensaje RRQ. La capacidad de generar o mostrar avisos relativos a la situación del balance del llamador puede anunciarse mediante un nuevo campo **supportedH248Packages** (**paquetes H248 soportados**). El campo **supportedH248Packages** consta de una lista facultativa de **H248PackagesDescriptors** (**descriptores de paquetes H248**) en formato binario.

Para enviar el texto de un anuncio, el punto extremo y el controlador de acceso pueden utilizar el paquete "Visualización" (**PackageID** dis, 0x0014), que se define en la Rec. UIT-T H.248.3. La Rec. UIT-T H.248.3 incluye facilidades para controlar la localización del texto en el visualizador del terminal y otras funciones.

Para enviar el índice de un aviso vocal fijo o parametrizado almacenado localmente en el punto extremo, tanto el punto extremo como el controlador de acceso pueden utilizar el paquete "Anuncio genérico" (**PackageID** an, 0x001D) que se define en la Rec. UIT-T H.248.7.

Alternativamente a la utilización de paquetes H.248, el punto extremo puede indicar mediante señalización de llamada H.225.0 que puede incluir el balance del usuario en un aviso de texto que él mismo construye. Esta capacidad puede indicarse mediante la bandera **canDisplayAmountString** (**puede visualizar cadena de cantidad**).

El punto extremo puede indicar mediante la bandera **canEnforceDurationLimit** (**puede limitar duración**) si puede cumplir su propio plazo de duración de llamada.

7.2.8.2 Información de balance enviada por el controlador de acceso al punto extremo

El controlador de acceso puede enviar anuncios (vocales o de texto) al punto extremo mediante una "señal" H.248 en la estructura del **ServiceControlDescriptor** (**descriptor de control del servicio**) de los mensajes ACF, SCI y/o DRQ. Alternativamente, el controlador de acceso puede enviar una cadena de texto al punto extremo en el campo **amountString** (**cadena de cantidad**) que indique la situación de la cuenta, por ejemplo, "$10,50", en la correspondiente moneda. En este caso, el punto

extremo es responsable de incluir la cadena de cantidad en un anuncio (por ejemplo, "Balance actual de la tarjeta de débito: $10,50") que sea adecuado para el punto extremo concreto de que se trate. Obsérvese que la norma ISO 4217 define abreviaturas normalizadas para las diversas monedas, tal como "USD" para dólares de los Estados Unidos de América. El campo **amountString** se debe codificar utilizando Unicode.

También se añade el campo **billingMode** (**modo de facturación**) para permitir que el controlador de acceso pueda indicar el modo de facturación de la llamada. Un modo **debit** (**débito**) indica que la llamada se cargará contra la cantidad disponible en la cuenta del usuario. Un modo **credit** (**crédito**) indica que la llamada creará un cargo que deberá ser pagado posteriormente por el usuario. Un punto extremo puede utilizar esta información para, por ejemplo, determinar el tipo de aviso que debe realizar o visualizar.

El campo **callDurationLimit** (**límite de duración de llamada**) de la estructura **CallCreditServiceControl** (**control del servicio de crédito de llamada**) indica el tiempo que resta para una llamada en particular. La bandera **enforceCallDurationLimit** (**limitación de duración de llamada**) indica si el punto extremo aplicará la limitación de duración de llamada. El campo **callStartingPoint** (**instante de inicio de la llamada**) indica el instante en que se inicia la temporización de una llamada cuando el punto extremo aplica la limitación de duración de la llamada.

Si el punto extremo ha anunciado que puede limitar la duración de la llamada y el controlador de acceso solicita al punto extremo que lo haga, el punto extremo terminará la llamada cuando venza el plazo de tiempo. La temporización de la duración de la llamada comenzará con la transmisión o la recepción del mensaje Conexión o del mensaje aviso según indique el campo **callStartingPoint**.

7.2.9 Direcciones de transporte alternativas

Un punto extremo puede indicar que soporta protocolos de transporte alternativos proporcionando el campo **alternateTransportAddresses** (**direcciones de transporte alternativas**) en el mensaje RRQ. El controlador de acceso puede ordenar al punto extremo el protocolo de transporte de señalización que se debe utilizar para realizar llamadas incluyendo el campo **useSpecifiedTransport** (**utilización de transporte especificado**) en los mensajes RCF o ACF. El controlador de acceso sólo incluirá en el campo **useSpecifiedTransport** los protocolos que los puntos extremos han indicado que pueden soportar. Cuando un punto extremo recibe el campo **useSpecifiedTransport**, utilizará el protocolo de transporte especificado para el establecimiento de la comunicación.

El controlador de acceso puede dar al punto extremo alternativas de elección para el protocolo de transporte de señalización de llamadas incluyendo el campo **alternateTransportAddresses** en el mensaje RCF o ACF, y no incluyendo el campo **useSpecifiedTransport**. En este caso, el punto extremo utilizará el protocolo especificado en el campo **destCallSignalAddress** (**dirección de señalización de llamada del destino**) o los seleccionará de entre los indicados en el campo **alternateTransportAddresses**.

El controlador de acceso también puede proporcionar a una entidad H.323 el campo **alternateTransportAddresses** de un punto extremo que se ha registrado con él en un mensaje LCF.

7.3 Canal de señalización de llamada

El canal de señalización de llamada se empleará para transportar mensajes de control de llamada H.225.0. El canal de señalización será un canal fiable.

En redes que no disponen de un controlador de acceso, los mensajes de señalización de llamada se pasan directamente entre los puntos extremos llamante y llamado utilizando las direcciones de transporte de señalización de llamada. En dichas redes, se supone que el punto extremo llamante

conoce la dirección de transporte de señalización de llamada del punto extremo llamado y, por tanto, puede comunicar directamente.

En las redes que disponen de un controlador de acceso, el intercambio de mensajes de admisión inicial tiene lugar entre el punto extremo llamante y el controlador de acceso utilizando la dirección de transporte de canal RAS del controlador de acceso. Durante el intercambio de mensajes de admisión inicial, el controlador de acceso indica en el mensaje ACF si la señalización de llamada se envía directamente al otro punto extremo o se encamina a través del controlador de acceso. Los mensajes de señalización de llamada se envían bien a la dirección de transporte de señalización de llamada del punto extremo o bien a la dirección de transporte de señalización de llamada del controlador de acceso.

El canal de señalización de llamada puede transportar diversas llamadas concurrentes, utilizando el valor de referencia de llamada para asociar el mensaje con la llamada. Una entidad indica su capacidad para cursar múltiples llamadas concurrentes en la misma conexión de señalización de llamada fijando la bandera **multipleCalls** (**llamadas múltiples**) en VERDADERO en mensajes que envía por el canal de señalización de llamada. Una entidad puede fijar dinámicamente el valor de **multipleCalls** para indicar cuál es su capacidad actual de soportar conexiones múltiples en el canal de señalización de llamada. Si el punto extremo desea cambiar el valor de **multipleCalls** en un instante en el que no se están intercambiando otros mensajes H.225.0 en el canal de señalización de llamada, transmitirá el campo **multipleCalls** mediante el mensaje facilidad cuyo valor de referencia de llamada (CRV) es referencia de llamada global, tal como se muestra en la figura 4-5/Q.931 y **guid** en el campo **callIdentifier** (**identificador de llamada**) se fijará a todos ceros.

Una entidad que tiene la capacidad de tratar múltiples llamadas concurrentes en el canal de señalización de llamada puede indicar que no soportará llamadas adicionales en el canal de señalización mediante el envío del mensaje Liberación Completa con la causa **newConnectionNeeded** (**nueva conexión necesaria**). Una entidad que recibe liberación completa con la causa **newConnectionNeeded** puede intentar conectarse con un nuevo canal de señalización de llamada.

Una entidad puede transmitir un mensaje Indagación de Situación que no esté relacionado con una llamada específica. En tales casos, la entidad deberá poner a ceros el campo **callIdentifier**. Una entidad no deberá omitir el **Status-UUIE** en el mensaje de situación ni el **StatusInquiry-UUIE** en el mensaje Indagación de Situación cuando transmita dichos mensajes, aunque las entidades deberán estar preparadas para recibir mensajes que no contengan dichos elementos de mensaje a fin de mantener la compatibilidad ascendente.

El canal de señalización de llamada se puede establecer antes de la necesidad real de señalizar una llamada, pudiendo el canal permanecer conectado entre llamadas. Una entidad puede indicar esta capacidad fijando la bandera **maintainConnection** (**mantener conexión**) en VERDADERO en mensajes que envía en el canal de señalización de llamada. Además, un punto extremo que posee esta capacidad debe indicarlo cuando se registra con un controlador de acceso. Esto permitirá a un controlador de acceso que utilice encaminamiento de controlador de acceso conectarse al punto extremo en cualquier momento después del registro. Si esta conexión se pierde cuando ninguna llamada o señalización está activa, ningún extremo intentará establecer la conexión hasta que la señalización sea necesaria.

El valor de la bandera **maintainConnection** que una entidad envía sobre un canal de señalización de llamada, será la misma para todos los mensajes que contengan este campo mientras esté activo el canal de señalización de llamada. Ello no impide que una entidad fije este valor a VERDADERO para un canal de señalización de llamada y FALSO para otro canal de señalización de llamada.

La Rec. UIT-T H.225.0 especifica los mensajes Q.931 obligatorios que se utilizan para señalización de llamada en la presente Recomendación. La cláusula 8 especifica los procedimientos para usarlos.

7.3.1 Encaminamiento del canal de señalización de llamada

Los mensajes de señalización de llamada se pueden transferir según dos métodos. El primero de ellos es el de señalización de llamada encaminada por el controlador de acceso (véase la figura 25). En este método, los mensajes de señalización de llamada se encaminan a través del controlador de acceso entre los puntos extremos. El segundo método es el de señalización de llamada de puntos extremos directa (véase la figura 26). En este método, los mensajes de señalización de llamada se pasan directamente entre los puntos extremos. La elección del método a utilizar corre a cargo del controlador de acceso.

Ambos métodos utilizan las mismas clases de conexiones para los mismos fines y los mismos mensajes. Los mensajes de admisión son intercambiados en canales RAS con el controlador de acceso, seguidos de un intercambio de mensajes de señalización de llamada en un canal de señalización de llamada. Esto a su vez va seguido del establecimiento del canal de control H.245. Las acciones del controlador de acceso en respuesta a los mensajes de admisión determinan qué modelo de llamada se utiliza, lo cual no está sometido al control del punto extremo, aunque el punto extremo puede especificar una preferencia.

El procedimiento de señalización simétrica del anexo D/Q.931 se utilizará con todos los procedimientos de señalización de llamada obligatoria. No se trata aquí del cometido que una pasarela podría desempeñar en el lado RCC utilizando Q.931 u otros protocolos de señalización de llamada.

Las nubes de controladores de acceso de las figuras 25 a 28 contienen uno o más controladores de acceso que pueden comunicar, o no comunicar, entre sí. Los puntos extremos pueden estar conectados al mismo controlador de acceso o a diferentes controladores de acceso.

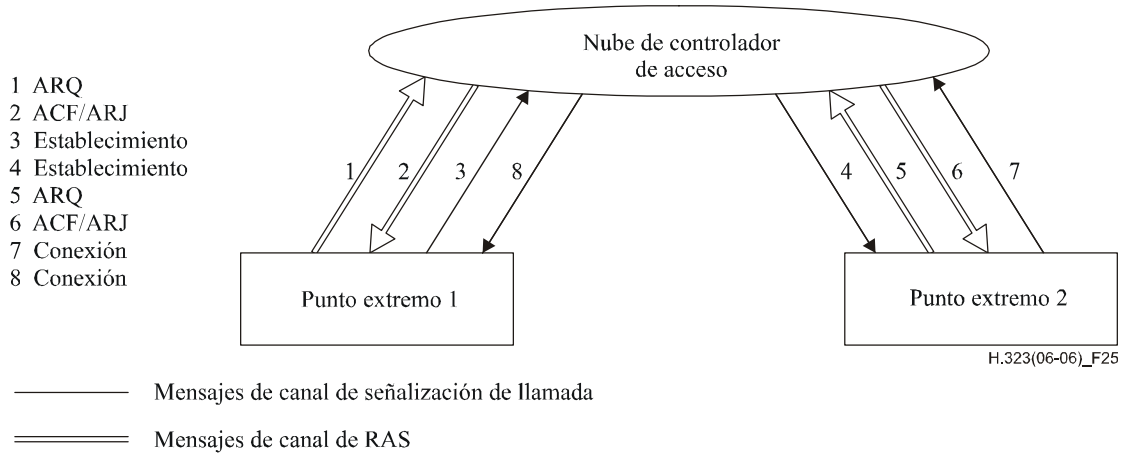


Figura 25/H.323 – Señalización de llamada encaminada por controlador de acceso

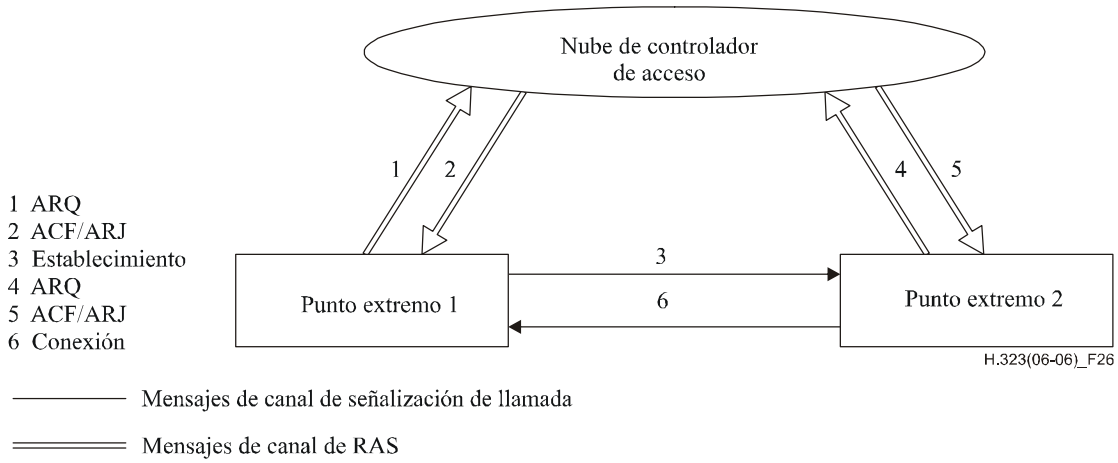


Figura 26/H.323 – Señalización de llamada de punto extremo directa

7.3.2 Encaminamiento del canal de control

Cuando se utiliza la señalización de llamada encaminada por controlador de acceso, se dispone de dos métodos para encaminar el canal de control H.245. En el primero de ellos, el canal de control H.245 se establece directamente entre los puntos extremos (véase la figura 27). Este método queda en estudio. En el segundo método, el canal de control H.245 es encaminado entre los puntos extremos a través del controlador de acceso (véase la figura 28). Este método permite al controlador de acceso reencaminar el canal de control H.245 a un MC cuando una conferencia multipunto ad hoc pasa de conferencia punto a punto a conferencia multipunto. El controlador de acceso realiza esta elección. Cuando se utiliza la señalización de llamada de punto extremo directa, el canal de control H.245 sólo puede ser conectado directamente entre los puntos extremos.

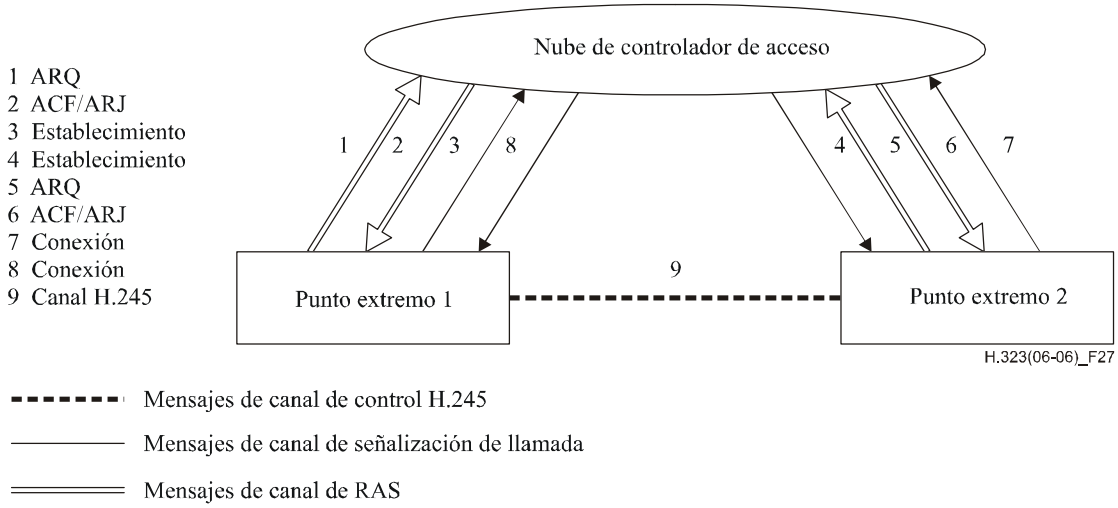


Figura 27/H.323 – Conexión de canal de control H.245 directa entre puntos extremos

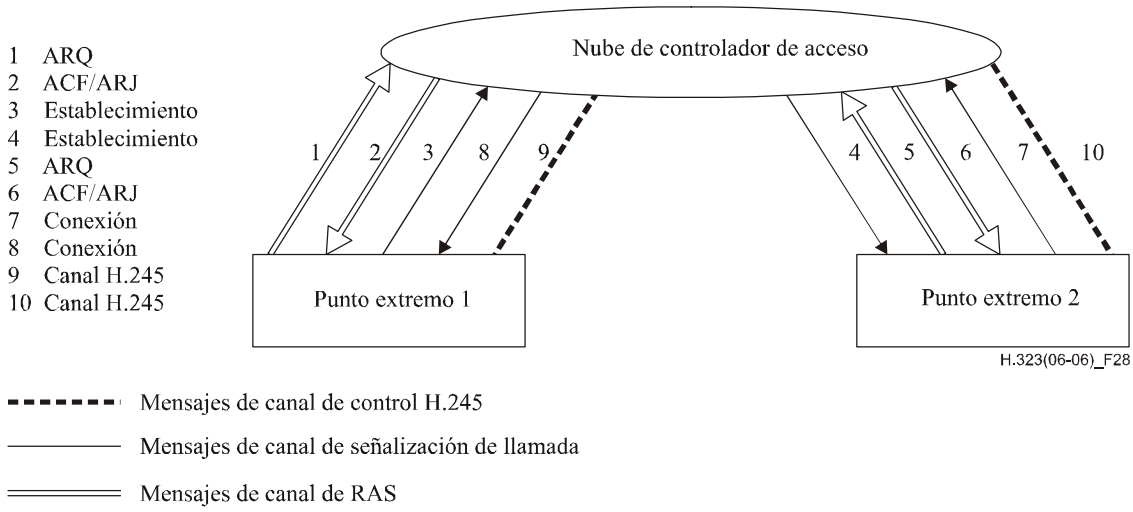


Figura 28/H.323 – Control H.245 encaminado por controlador de acceso

7.3.3 Revisiones del protocolo de señalización de llamada y control

Cuando una llamada se encamina a través de controladores de acceso, éstos utilizarán las siguientes reglas para determinar el número de versión H.225.0 o H.245 que será indicado en los mensajes originados por un punto extremo y encaminado o reenviado por el controlador de acceso:

a) Si el número de versión H.225.0 o H.245 del punto extremo de origen es menor o igual que el número de versión y el controlador de acceso decide representar las funciones de un número de versión igual o posterior en nombre del punto extremo de origen, los mensajes encaminados reflejarán el número de versión del controlador de acceso. En cualquier otro caso, éstos reflejarán el número de versión del punto extremo de origen.

b) Si el número de versión del punto extremo de origen es mayor que el del controlador de acceso, los mensajes encaminados reflejarán el número de versión del controlador de acceso.

En todos los casos, el controlador de acceso puede utilizar una sola codificación ASN.1 especificada en la versión H.225.0 o H.245 más reciente comprendida por el controlador de acceso conforme con esas reglas.

Puesto que algunas de las características de H.323, tales como la pausa y el reencaminamiento iniciados por terceras partes, requieren que las entidades de señalización conozcan exactamente qué versión del protocolo está siendo utilizada por otras entidades en una llamada, y puesto que el **protocolIdentifier** (**identificador de protocolo**) puede cambiar después de recibir el mensaje de señalización de la primera llamada y en otros momentos durante la llamada, por ejemplo, cuando se reencamina una llamada a una entidad diferente, las entidades que dependen de características específicas de la versión deberán determinar cuál es la versión de las demás entidades en una llamada examinando el **protocolIdentifier** en el mensaje Establecimiento y Conexión como mínimo. Una llamada se puede reencaminar, en el transcurso de la misma, hacia una entidad diferente que utiliza una versión distinta del protocolo. En tal caso, las entidades que dependen de características específicas de una versión deberán determinar de nuevo cuál es la versión de la entidad a la que la llamada puede haber sido conmutada. Si se tuneliza la señalización H.245, el punto extremo podrá utilizar el mensaje de señalización de llamada que contiene el mensaje tunelizado de conjunto de capacidades de terminal no vacío para determinar la versión del punto extremo distante. Si se utiliza un canal H.245 separado, una entidad podrá enviar un mensaje Indagación de Situación y determinar la versión del protocolo examinando el **protocolIdentifier** en el mensaje Situación resultante. En cualquier caso, la versión de H.245 utilizada por la otra entidad se señaliza en el mensaje de conjunto de capacidades no vacío.

Se señala que las entidades H.323 anteriores a la versión 4 quizás no puedan proporcionar el **protocolIdentifier** en el mensaje estado por lo que dichas entidades deberán suponer que la ausencia del **protocolIdentifier** sólo indica que la entidad es anterior a la versión 4.

NOTA – Un controlador de acceso puede señalizar su propia versión de protocolo cuando replique a un mensaje Establecimiento (por ejemplo, para enviar un mensaje llamada en curso antes del establecimiento de la comunicación con la parte llamada) o cuando inicie una conexión de salida independiente de una llamada existente. Es importante, por ello, que un punto extremo no dependa del mensaje o los mensajes iniciales para determinar la versión del protocolo del punto extremo distante.

7.4 Valor de referencia de llamada

Todos los mensajes de señalización de llamada y RAS contienen un valor de referencia de llamada (CRV, *call reference value*). Véase la Rec. UIT-T H.225.0. Hay un CRV para el canal de señalización de llamada y un CRV independiente para el canal RAS. Un CRV se utiliza para asociar los mensajes de señalización de llamada. Este CRV se utilizará en todos los mensajes de señalización de llamada entre dos entidades (punto extremo a controlador de acceso, punto extremo a punto extremo, etc.) relacionadas con la misma llamada. Un segundo CRV se utiliza para asociar los mensajes RAS. Este CRV se utilizará en todos los mensajes RAS entre dos entidades relacionadas con la misma llamada. Se utilizarán nuevos CRV para nuevas llamadas. Una segunda llamada procedente de un punto extremo para invitar a otro punto extremo a la misma conferencia utilizará nuevos CRV. El CRV no es lo mismo que el ID de llamada o el ID de conferencia (CID, *conference ID*). El CRV asocia mensajes de señalización de llamada o RAS entre dos entidades dentro de la misma llamada, el ID de llamada asocia todos los mensajes entre todas las entidades dentro de la misma llamada, y el CID asocia todos los mensajes entre todas las entidades dentro de todas las llamadas en la misma conferencia.

La referencia de llamada global, tal como se muestra en la figura 4-5/Q.931 y con el valor numérico 0, se utiliza para hacer referencia a todas las llamadas en el canal de señalización de llamada o en el canal RAS. Cuando se inician o se aceptan llamadas, las entidades H.323 deben seleccionar un valor de CRV distinto al valor de referencia de llamada global; la referencia de llamada global queda reservada para mensajes que no pertenezcan a una llamada en particular.

Cuando se inicia una nueva llamada, el punto extremo seleccionará un nuevo CRV para la llamada. El punto extremo llamante utilizará el mismo CRV en el canal RAS y en el canal de señalización de llamada H.225.0. Sin embargo, el punto extremo llamado no utilizará el CRV recibido en el establecimiento cuando se comunica en su canal RAS. En lugar de ello, el punto extremo llamado

seleccionará un nuevo CRV para utilizar el canal RAS que sea exclusivo en dicho canal sin tener en cuenta el CRV recibido en el establecimiento, aunque puede ocurrir que sean numéricamente equivalentes.

7.5 Identificador (ID) de llamada

El identificador de llamada es un valor distinto de cero globalmente único creado por el punto extremo llamante y que se intercambia en varios mensajes H.225.0. El ID de llamada identifica la llamada con la que está asociado el mensaje. Se utiliza para asociar todos los mensajes RAS y de señalización de llamada relacionados con la misma llamada. A diferencia del CRV, el ID de llamada no cambia dentro de una llamada. Todos los mensajes del punto extremo llamante a su controlador de acceso, del punto extremo llamante al punto extremo llamado, y del punto extremo llamado a su controlador de acceso relativos a la misma llamada contendrán el mismo ID de llamada. El ID de llamada se codifica como se indica en la Rec. UIT-T H.225.0. En la referencia a las figuras 29 a 39 de la cláusula 8, todos los mensajes dentro de una figura tendrán el mismo ID de llamada.

Cuando un punto extremo de la versión 1 llama a un punto extremo de la versión 2, corresponde al punto extremo de la versión 2 generar un ID de llamada antes de enviar ARQ a su controlador de acceso.

7.6 Identificador (ID) de conferencia y cometido de conferencia

El ID de conferencia (CID) es un valor único distinto de cero creado por el punto extremo llamante y que se intercambia en diversos mensajes H.225.0. El CID identifica la conferencia con la cual está asociado el mensaje. Por tanto, los mensajes procedentes de todos los puntos extremos dentro de la misma conferencia tendrán el mismo CID. El CID se codifica como se especifica en la Rec. UIT-T H.225.0.

El **conferenceGoal** (**cometido de conferencia**) indica el propósito de la llamada. Las opciones son: **create** (**crear**) – crear una nueva conferencia, **join** (**incorporarse**) – incorporarse a una conferencia existente, **invite** (**invitar**) – invitar a un nuevo punto extremo a una conferencia existente, **capability-negotiation** (**negociación de capacidad**) – negociar capacidades para una conferencia H.332 posterior, y **callIndependentSupplementaryService** (**servicio suplementario independiente de la llamada**) – transporte de APDU de servicios suplementarios.

7.7 Capacidad de llamada de un punto extremo

La capacidad de llamada indica la capacidad de aceptación que tiene un punto extremo para cada uno de los tipos de llamada que el punto extremo soporta (por ejemplo, voz, datos T.120, H.320, etc.). Si bien cualquier punto extremo puede comunicar capacidad de llamada a través de varios mensajes H.225.0, las pasarelas deben comunicar información de capacidad de llamada al controlador de acceso para ayudarle en el encaminamiento de las llamadas, en concreto, en el reparto de carga entre pasarelas y en la reducción del número de intentos de llamada fallidos.

La capacidad máxima y actual del punto extremo debe indicarse en el momento del registro. Además, la capacidad actual puede también indicarse en cada llamada. Para representar esta capacidad dinámica, se desea considerar los modelos de llamada siguientes:

- Modelo de llamada directa con admisión por llamada – En este caso, el punto extremo puede indicar capacidad remanente en los mensajes ARQ, DRQ o BRQ.
- Modelo de llamada directa con admisión previamente concedida – En este caso, el punto extremo puede indicar capacidad en los mensajes RRQ o RAI (si el punto extremo es una pasarela).

- Modelo de llamada encaminada por el controlador de acceso con admisión por llamada – El punto extremo puede proporcionar información de capacidad en los mensajes ARQ, DRQ, o BRQ.
- Modelo de llamada encaminada por el controlador de acceso con admisión concedida previamente – El punto extremo puede incluir información de capacidad en los mensajes de señalización de llamada, tales como Establecimiento y Liberación Completa. En este caso, el punto extremo origen puede proporcionar su información de capacidad en un mensaje Establecimiento, mientras que el punto extremo de terminación puede proporcionar su información de capacidad en los mensajes de aviso o conexión. Cada punto extremo puede proporcionar información de capacidad actualizada utilizando el mensaje Liberación Completa.

En cualquier caso, un controlador de acceso puede utilizar el intercambio IRQ/IRR para auditar un punto extremo a fin de descubrir potencialmente la capacidad de llamada del mismo. Obsérvese que cuando no se utilice el modelo de admisión previamente concedida o un mensaje Establecimiento en una llamada encaminada por el controlador de acceso, es preferible incluir información de capacidad en mensajes que necesariamente deban enviarse a un controlador de acceso, tal como un ARQ, en lugar de enviar mensajes adicionales para este propósito. Sin embargo, si un controlador de acceso recibe un mensaje Liberación Completa y está trabajando en el modo de admisión previamente concedida, debe enviar un IRR al controlador de acceso a fin de permitir que éste mantenga una información de capacidad más precisa.

Si un punto extremo proporciona información de capacidad de llamada, debe proporcionar información de capacidad en un mensaje RRQ y debe indicar sus capacidades de comunicación de capacidad de llamada en el mensaje RRQ. Un controlador de acceso puede solicitar a través de mensajes RCF y IRQ que un punto extremo proporcione información de capacidad de llamada. Un punto extremo que ha indicado que puede comunicar capacidad de llamada comunicará su capacidad según lo solicite el controlador de acceso. Excepto en el mensaje RRQ inicial, un punto extremo no debería comunicar capacidad máxima de llamada salvo que su controlador de acceso pida esa información en un mensaje IRQ. Un punto extremo puede utilizar información de capacidad en un mensaje BRQ, IRR o RAI para informar al controlador de acceso de cambios repentinos, tales como los causados por fallos del soporte físico.

Un punto extremo puede señalizar que tiene capacidades diferentes para los distintos protocolos que pueda soportar (por ejemplo, T.120, H.320, H.321, voz, etc.). No obstante, puesto que los fabricantes de equipos pueden utilizar los mismos recursos para múltiples protocolos, el controlador de acceso no debería hacer supuesto alguno sobre cómo puede cambiar la capacidad de llamada de un punto extremo para uno de los protocolos soportados cuando el punto extremo participa en una llamada utilizando un protocolo diferente.

Un controlador de acceso puede señalizar la capacidad de la llamada mediante **group** (**grupo**) donde **group** puede representar un conjunto de circuitos asociados con una interfaz concreta o con una portadora. Esta característica permite al controlador de acceso hacer un seguimiento de la capacidad de la llamada para cada grupo. El **grupo** puede ser el mismo que aquél del que se ha informado en el **circuitID** (**identificador de circuito**) para una llamada en concreto.

NOTA – La información de capacidad comunicada en cualquier mensaje es de naturaleza consultiva y puede no ser absolutamente exacta debido a situación de aceleración, de cambios repentinos en el punto extremo o la asignación local de recursos.

7.8 Servicios de identificación del llamador

7.8.1 Descripción de los servicios

En esta cláusula se describen los servicios de identificación del llamador, que incluyen:

- Presentación y restricción del número de la parte llamante.

- Presentación y restricción del número de la parte conectada.
- Presentación y restricción del número de la parte llamada (avisada).
- Presentación y restricción del número de la parte ocupada.

7.8.1.1 Presentación de la dirección de la parte llamante

La presentación de la dirección de la parte llamante es una característica que proporciona la dirección alias de la parte llamante a la parte llamada. La dirección de la parte llamante puede ser proporcionada por el punto extremo llamante o por el controlador de acceso en caso de llamada encaminadas por el controlador de acceso que se originan en la red de paquetes. Cuando la llamada se encamina a través del controlador de acceso al que está registrado el punto extremo llamante, el controlador de acceso puede proporcionar un servicio de supervisión que asegure que la dirección proporcionada es realmente la de la parte llamante. El controlador de acceso puede también proporcionar la dirección de la parte llamante cuando ésta no proporciona dirección alguna o cuando la parte llamante proporciona una dirección distinta de aquélla con la que dicha parte se registró.

Cuando una llamada se origina en la RCC y accede a la red de paquetes a través de una pasarela, ésta pasará a la red de paquetes la información del número de la parte llamante que se facilita desde la RCC.

7.8.1.2 Restricción de la dirección de la parte llamante

La restricción de la dirección de la parte llamante es una característica que permite al punto extremo llamante o al controlador de acceso del punto extremo llamante restringir a la parte llamada la presentación de la dirección alias de la parte llamante. Esta posibilidad puede residir en el punto extremo o en el controlador de acceso para llamadas encaminadas por el controlador de acceso.

Existen situaciones en las que a pesar de haberse indicado la restricción de la dirección de la parte llamante, dicha restricción puede verse anulada (por ejemplo, si la parte llamada proporciona algún servicio de emergencia).

7.8.1.3 Presentación de la dirección de la parte conectada

La presentación de la dirección de la parte conectada es una característica que proporciona a la parte llamante la dirección alias de la parte conectada o de la que contesta la llamada. La dirección de la parte conectada puede ser proporcionada por el punto extremo conectado o por el controlador de acceso en el caso de llamada encaminada por el controlador de acceso. Cuando la llamada se encamina a través del controlador de acceso al que está registrado el punto extremo conectado, el controlador de acceso puede proporcionar un servicio de supervisión que garantice que la dirección proporcionada es realmente la de la parte conectada. El controlador de acceso puede también proporcionar la dirección de la parte conectada cuando ésta no proporciona dirección alguna o cuando la parte conectada proporciona una dirección distinta de aquélla con la que dicha parte se registró.

Una pasarela pasará a la red de paquetes la información de la parte conectada recibida de la RCC.

7.8.1.4 Restricción de la dirección de la parte conectada

La restricción de la dirección de la parte conectada es una característica que permite al punto extremo conectado o al controlador de acceso del punto extremo conectado restringir a la parte llamante la presentación de la dirección alias de la parte conectada. Esta posibilidad puede residir en el punto extremo o en el controlador de acceso para llamadas encaminadas por el controlador de acceso.

Existen situaciones en las que a pesar de haberse indicado restricción de la dirección de la parte conectada, dicha restricción puede verse anulada (por ejemplo, si la parte llamada proporciona algún servicio de emergencia).

7.8.1.5 Presentación de la dirección de la parte llamada (avisada)

La presentación de la dirección de la parte avisada es una característica que proporciona a la parte llamante la dirección alias de la parte avisada. La dirección de la parte avisada puede ser proporcionada por el punto extremo avisado o por el controlador de acceso en el caso de llamadas encaminadas por el controlador de acceso. Cuando la llamada se encamina a través del controlador de acceso al que está registrado el punto extremo avisado, el controlador de acceso puede proporcionar un servicio de supervisión que garantice que la dirección proporcionada es realmente la de la parte avisada. El controlador de acceso puede también proporcionar la dirección de la parte avisada cuando ésta no proporciona dirección alguna o cuando la parte avisada proporciona una dirección distinta de aquélla con la que dicha parte se registró.

7.8.1.6 Restricción de la dirección de la parte llamada (avisada)

La restricción de la dirección de la parte avisada es una característica que permite al punto extremo avisado o al controlador de acceso del punto extremo avisado restringir la presentación de la dirección alias de la parte avisada a la parte llamante. Esta posibilidad puede residir en el punto extremo o en el controlador de acceso para llamadas encaminadas por el controlador de acceso.

7.8.1.7 Presentación de la dirección de la parte ocupada

La presentación de la dirección de la parte ocupada es una característica que proporciona a la parte llamante la dirección alias de la parte ocupada. La dirección de la parte ocupada puede ser proporcionada por el punto extremo ocupado o por el controlador de acceso en el caso de llamadas encaminadas por el controlador de acceso. Cuando la llamada se encamina a través del controlador de acceso al que está registrado el punto extremo ocupado, el controlador de acceso puede proporcionar un servicio de supervisión que garantice que la dirección proporcionada es realmente la de la parte ocupada. El controlador de acceso puede también proporcionar la dirección de la parte ocupada cuando ésta no proporciona dirección alguna o cuando la parte ocupada proporciona una dirección distinta de aquélla con la que dicha parte se registró.

7.8.1.8 Restricción de la dirección de la parte ocupada

La restricción de la dirección de la parte ocupada es una característica que permite al punto extremo ocupado o al controlador de acceso del punto extremo ocupado restringir la presentación de la dirección alias de la parte ocupada a la parte llamante. Esta posibilidad puede residir en el punto extremo o en el controlador de acceso para llamadas encaminadas por el controlador de acceso.

7.8.2 Mensajes y elementos de información

En esta cláusula se describen los diversos mensajes y elementos de información que permiten a los dispositivos H.323 proporcionar los servicios de presentación y restricción de dirección.

7.8.2.1 Información de dirección de la parte llamante

La información de dirección de la parte llamante aparece en el mensaje Establecimiento.

Cuando la información de dirección representa un número de teléfono, la información relevante puede aparecer en el elemento de información (IE, *information element*) número de la parte llamante. Este IE contiene el número del llamador, la información acerca del número y los indicadores de presentación y supervisión que se encuentran en el octeto 3a. Este es el modo de funcionamiento recomendado para el caso en el que una pasarela de la RTPC envíe un mensaje Establecimiento a la red de paquetes.

Alternativamente, la información de la parte llamante puede aparecer en los campos **sourceAddress** (**dirección de fuente**), **presentationIndicator** (**indicador de presentación**) y **screeningIndicator** (**indicador de supervisión**) del mensaje Establecimiento. Éste es el modo de funcionamiento requerido cuando **sourceAddress** no es un número de teléfono (es decir, cuando **sourceAddress** no es del tipo **dialledDigits** o **partyNumber**). También lo es, en virtud de 7.2.2.6/H.225.0, cuando la

información de dirección tiene la forma de un número de teléfono perteneciente a un plan de numeración privado.

El campo **presentationIndicator** del mensaje Establecimiento transporta información idéntica al indicador de presentación que se encuentra en el IE Número de la Parte Llamante. El significado y utilización del indicador de presentación se define en la Rec. UIT-T Q.951.

El campo **screeningIndicator** del mensaje Establecimiento transporta información idéntica al indicador de supervisión que se encuentra en el IE Número de la Parte Llamante. El significado y utilización del indicador de supervisión se define en la Rec. UIT-T Q.951.

7.8.2.2 Información de dirección de la parte conectada

La información de dirección de la parte conectada aparece en el mensaje Conexión.

Cuando la información de dirección representa un número de teléfono, la información relevante puede aparecer en el elemento de información (IE) número conectado, incluyendo el indicador de presentación y el indicador de supervisión. Éste es el modo de funcionamiento recomendado para el caso en el que una pasarela de la RTPC envía un mensaje Conexión a la red de paquetes.

Alternativamente, la información de la parte conectada puede aparecer en los campos **connectedAddress** (**dirección conectada**), **presentationIndicator** y **screeningIndicator** del mensaje Conexión. Éste es el modo de funcionamiento requerido cuando **connectedAddress** no es un número de teléfono (es decir, **connectedAddress** no es del tipo **dialledDigits** o **partyNumber**).

El campo **presentationIndicator** del mensaje Conexión transporta información idéntica al indicador de presentación que se encuentra en el IE Número Conectado. El significado y utilización del indicador de presentación se define en la Rec. UIT-T Q.951.

El campo **screeningIndicator** del mensaje Conexión transporta información idéntica al indicador de supervisión que se encuentra en el IE Número Conectado. El significado y utilización del indicador de supervisión se define en la Rec. UIT-T Q.951.

7.8.2.3 Información de dirección de la parte llamada (avisada)

La información de dirección de la parte avisada aparece en el mensaje aviso.

La información de la parte avisada puede aparecer en los campos **alertingAddress**, **presentationIndicator** y **screeningIndicator** del mensaje aviso.

El campo **presentationIndicator** del mensaje aviso transporta información idéntica al indicador de presentación que se encuentra en el IE Número Conectado. El significado y utilización del indicador de presentación se define en la Rec. UIT-T Q.951.

El campo **screeningIndicator** del mensaje aviso transporta información idéntica al indicador de supervisión que se encuentra en el IE Número Conectado. El significado y utilización del indicador de supervisión se define en la Rec. UIT-T Q.951.

7.8.2.4 Información de dirección de la parte ocupada

La información de dirección de la parte ocupada aparece en el mensaje Liberación Completa.

La información de la parte ocupada puede aparecer en los campos **busyAddress** (**dirección ocupada**), **presentationIndicator** y **screeningIndicator** del mensaje Liberación Completa.

El campo **presentationIndicator** del mensaje Liberación Completa transporta información idéntica al indicador de presentación que se encuentra en el IE Número Conectado. El significado y utilización del indicador de presentación se define en la Rec. UIT-T Q.951.

El campo **screeningIndicator** del mensaje Liberación Completa transporta información idéntica al indicador de supervisión que se encuentra en el IE Número Conectado. El significado y utilización del indicador de supervisión se define en la Rec. UIT-T Q.951.

7.8.3 Acciones en el punto extremo origen

Esta cláusula describe los aspectos de procedimiento necesarios para proporcionar servicios de identificación del llamador en el punto extremo origen.

7.8.3.1 La pasarela como punto extremo origen

En el caso de un mensaje Establecimiento procedente de la RDSI que se recibe en una pasarela, el número del llamador y la información de presentación residen en el IE Número de la Parte Llamante. La pasarela enviará un mensaje Establecimiento a la red de paquetes cuyo IE Número de la Parte Llamante contenga la misma información que haya en el mensaje Establecimiento procedente de la RCC con la siguiente excepción. Si el campo Identificación del Plan de Numeración contiene el valor Plan de Numeración Privado, deberán omitirse las cifras del IE Número de la Parte Llamante de conformidad con 7.2.2.6/H.225.0. En este caso excepcional la pasarela colocará la información de identificación del llamador recibida en los campos **sourceAddress**, **presentationIndicator** y **screeningIndicator** del mensaje Establecimiento. Cuando la pasarela disponga de la información necesaria para poder enviar tanto un número PNP como un número E.164, el IE Número de la Parte Llamante transportará el número E.164 (y no el número PNP "vacío").

Cuando una pasarela reciba un mensaje Conexión, copiará el IE Número Conectado del mismo procedente de la red de paquetes al mensaje Conexión que se envía a la RDSI. Si el IE Número Conectado no está presente en el mensaje Conexión, la pasarela convertirá **connectedAddress**, **presentationIndicator** y **screeningIndicator** en un IE Número Conectado, si dicha **connectedAddress** representa un número de teléfono. Si **connectedAddress** no representa un número de teléfono o si el IE Número Conectado no está presente, la pasarela omitirá el IE Número Conectado del mensaje Conexión que envía a la RDSI.

Cuando una pasarela reciba un mensaje aviso con información de la parte avisada o un mensaje Liberación Completa con información de la parte ocupada, convertirá la información de la parte al formato de señalización de lado de circuito de la pasarela si el formato de señalización soporta esta información de la parte.

7.8.3.2 El terminal o la MCU como punto extremo origen

En el caso de llamadas originadas en la red de paquetes, el terminal origen o el MCU puede enviar un mensaje Establecimiento con el IE Número de la Parte Llamante incluyendo indicadores de presentación y supervisión o los campos **sourceAddress**, **presentationIndicator** y **screeningIndicator**. En cualquier caso, el indicador de supervisión indicará "usuario no supervisado". A título de ejemplo, si el llamador desea bloquear la identificación a la parte llamada, el indicador de presentación se pondría a "presentación restringida", pero el número del llamador seguiría apareciendo en el IE Número de la Parte Llamante. En caso de encaminamiento por el controlador de acceso, el controlador de acceso de la parte llamante puede añadir dicha información si no está presente o si es incorrecta y el controlador de acceso de la parte llamada puede suprimir la información de identificación del llamador si ello es pertinente. El controlador de acceso de la parte llamante o de la parte llamada también puede añadir o suprimir información de dirección de acuerdo con una política local.

Cuando un terminal o una MCU recibe un mensaje Conexión, aviso o liberación completa debe respetar el indicador de presentación cuando presente la información de dirección al usuario.

7.8.4 Acciones en el punto extremo de terminación

En esta cláusula se describen los aspectos de procedimiento necesarios para proporcionar servicios de identificación del llamador en el punto extremo de terminación.

7.8.4.1 La pasarela como punto extremo de terminación

Cuando una pasarela RTPC recibe un mensaje Establecimiento de la red de paquetes, copiará la información del IE Número de la Parte Llamante del mensaje Establecimiento al formato de señalización soportado en la RTPC. Por ejemplo, esa información debería copiarse en el IE Número de la Parte Llamante del mensaje Establecimiento Q.931 de la RDSI. Si el IE Número de la Parte Llamante no está presente en el mensaje Establecimiento, o si el campo Identificación del Plan de Numeración contiene el valor Plan de Numeración Privado, la pasarela formará dicho IE utilizando **sourceAddress** (considerando que es uno de los tipos de alias de número de teléfono), **presentationIndicator** y **screeningIndicator** del mensaje Establecimiento.

La pasarela enviará un mensaje Conexión a la red de paquetes en el que el IE Número Conectado tiene la misma información que existía en el formato de señalización soportado en la red telefónica. En el caso de que en la pasarela se reciba un mensaje Conexión Q.931 procedente de la RDSI, la información de la parte conectada reside en el IE numero conectado.

7.8.4.2 El terminal o la MCU como punto extremo de terminación

Un terminal o una MCU que reciba un mensaje Establecimiento debe respetar el indicador de presentación cuando se presente al usuario la información del llamador.

En el caso de llamadas respondidas en la red de paquetes, el terminal o la MCU que responde puede incluir en el mensaje Conexión el IE Número Conectado o los campos **connectedAddress**, **presentationIndicator** y **screeningIndicator**. En cualquier caso, el terminal o la MCU fijarán el **screeningIndicator** en "usuario no supervisado". En caso de encaminamiento por el controlador de acceso, el controlador de acceso de la parte que responde puede añadir esta información si no está presente o si es incorrecta y el controlador de acceso de la parte llamante puede suprimir la información de dirección de la parte que responde si ello es pertinente.

Un terminal o una MCU puede proporcionar información de dirección en el mensaje aviso utilizando los campos **alertingAddress**, **presentationIndicator** y **screeningIndicator** del mensaje Aviso. Si se proporciona la dirección, el terminal o la MCU fijarán el **screeningIndicator** a "usuario no supervisado". En caso de encaminamiento por el controlador de acceso, el controlador de acceso de la parte que responde puede añadir esta información si no está presente o si es incorrecta y el controlador de acceso de la parte llamante puede suprimir la información de dirección de la parte que responde, si ello es pertinente. El controlador de acceso de la parte que responde o el controlador de acceso de la parte llamante pueden también añadir o suprimir información de dirección de acuerdo con una política local.

Un terminal o una MCU ocupada pueden proporcionar información de dirección en el mensaje Liberación Completa utilizando los campos **busyAddress**, **presentationIndicator** y **screeningIndicator** del mensaje Liberación Completa. Si se proporciona la dirección, el terminal o la MCU fijará el **screeningIndicator** a "usuario no supervisado". En caso de encaminamiento por el controlador de acceso, el controlador de acceso de la parte que responde puede añadir esta información si no está presente o si es incorrecta y el controlador de acceso de la parte llamante puede suprimir la información de dirección de la parte que responde, si ello es pertinente.

7.8.5 Acciones en un controlador de acceso

En los casos de encaminamiento por el controlador de acceso, éste puede proporcionar información de identificación o puede proporcionar un servicio de supervisión. Los servicios que puede proporcionar un controlador de acceso dependen del tipo de punto extremo servido. En esta cláusula se describen los aspectos de procedimiento necesarios para proporcionar servicios de identificación del llamador cuando el controlador de acceso encamina la señalización de llamada.

7.8.5.1 La pasarela como punto extremo de origen

En los casos de encaminamiento por el controlador de acceso, éste no debe modificar la información del mensaje Establecimiento enviado desde una pasarela. Se considera que la red telefónica ha proporcionado información correcta.

7.8.5.2 El terminal o la MCU como punto extremo de origen

En los casos de encaminamiento por el controlador de acceso, éste puede proporcionar información de la parte llamante cuando ésta no es una pasarela. El controlador de acceso puede proporcionar la dirección de la parte llamante si ésta no la proporcionó o si el controlador de acceso determina que la dirección no es correcta. Si el controlador de acceso proporciona una dirección distinta a la enviada en el mensaje Establecimiento, fijará el indicador de supervisión en "proporcionado por la red". Si el controlador de acceso verifica la dirección enviada en el mensaje Establecimiento, pero no modifica la información de dirección, el controlador de acceso fijará el indicador de supervisión en "proporcionada por el usuario, verificada y pasada". Si el controlador de acceso determina que la información de dirección enviada en el mensaje Establecimiento es incorrecta, pero no modifica la información de dirección, fijará el indicador de supervisión en "proporcionado por el usuario, verificado y fallido". El controlador de acceso puede fijar el indicador de presentación para proporcionar servicio al punto extremo. El controlador de acceso puede permitir que el punto extremo obvie el servicio del punto extremo especificando una presentación distinta (por ejemplo, restringiendo la presentación para la llamada en curso cuando el servicio del punto extremo es permitir la presentación).

7.8.5.3 La pasarela como punto extremo de terminación

En los casos de encaminamiento por el controlador de acceso, un controlador de acceso no debería modificar la información del mensaje Conexión enviada desde una pasarela. Se considera que la red telefónica ha proporcionado información correcta.

7.8.5.4 El terminal o la MCU como punto extremo de terminación

En los casos de encaminamiento por el controlador de acceso, éste puede proporcionar información de la parte conectada, avisada u ocupada cuando la parte conectada, avisada u ocupada no es de una pasarela. El controlador de acceso puede proporcionar la dirección de la parte conectada (la parte avisada u ocupada) si la parte conectada (la parte avisada u ocupada) no proporcionó una o si el controlador de acceso determina que la dirección no es correcta. Si el controlador de acceso proporciona una dirección distinta a la enviada en el mensaje Conexión, aviso o liberación completa, el controlador de acceso fijará el indicador de supervisión en "proporcionado por la red ". Si el controlador de acceso verifica la información de dirección enviada en el mensaje Conexión, aviso o liberación completa, pero no modifica la información de dirección, el controlador de acceso fijará el indicador de supervisión en "proporcionado por el usuario, verificado y pasado". Si el controlador de acceso determina que la información de dirección enviada en el mensaje Conexión, aviso o liberación completa es incorrecta pero no modifica la información de dirección, fijará el indicador de supervisión en "proporcionado por el usuario, verificado y fallido". El controlador de acceso puede fijar el indicador de presentación para proporcionar servicio al punto extremo. El controlador de acceso puede permitir que el punto extremo obvie el servicio del punto extremo especificando una presentación distinta (por ejemplo, restringiendo la presentación para la llamada en curso cuando el servicio del punto extremo es permitir la presentación).

7.9 Marco ampliable genérico

El marco ampliable genérico permite añadir rápidamente al protocolo nuevas características sin afectar a la especificación nuclear H.225.0 subyacente. El marco ampliable consta de dos partes:

- Transporte de datos opacos en mensajes H.225.0.
- Negociación de las características soportadas.

El soporte del **marco extensible genérico** es facultativo.

7.9.1 Formato de una estructura datos genéricos

Los mensajes de señalización de llamada H.225.0 y un subconjunto de mensajes RAS pueden transportar datos opacos en el campo **datos genéricos** (**GenericData**).

La estructura **GenericData** consta básicamente de un identificador y de cero o más parámetros que permiten la definición flexible de datos opacos y de características. La estructura **GenericData** consta de un **id** para identificar los datos genéricos y el campo **parameters** para el transporte de los datos.

Cada parámetro también contiene un **id** identificador y un campo **content**. El campo **content** soporta diversos tipos de datos, incluyendo **raw**, **text**, **unicode**, **bool**, **number8**, **number16**, **number32**, **id**, **compound** y **nested**. Ello permite la definición flexible de datos genéricos y facilita la implementación. Sin embargo, es previsible que para datos genéricos que contengan un gran número de parámetros, se utilice la forma **raw** de **content**, que contendrá datos ASN.1.

7.9.2 Negociación utilizando el marco ampliable – Generalidades

El marco ampliable proporciona un método común para la negociación de características que opera sobre múltiples dominios y que puede ser gestionado y configurado por distintas entidades operacionales. Por tanto, las entidades no requieren un conocimiento *a priori* de otros conjuntos de características de las entidades para operar con éxito.

El mecanismo utilizado para negociar características en RAS y en la señalización de llamada utiliza el **FeatureDescriptor** (**descriptor de características**), que es un alias de una estructura **GenericData** anteriormente descrita. Ello permite identificar una característica y que se asocien parámetros a la misma.

Las entidades de señalización intermedias pueden – sujetas a consideraciones de seguridad – añadir a los mensajes que pasan a través de ellas las características que les sean necesarias, que deseen y que soporten. Las entidades intermedias pueden suprimir características deseadas y soportadas especificadas en los mensajes antes de pasarlos. Las entidades intermedias no suprimirán campos de características necesarias salvo que éstos tengan por objeto soportar las características que están suprimiendo. Si la entidad intermedia no desea permitir una característica necesaria, rechazará la transacción.

Si una entidad intermedia decide soportar una característica solicitada señalizada en un mensaje, debe suprimir del mensaje, antes de pasarlo, la petición de la característica. La entidad intermedia debe señalizar hacia atrás a la entidad que hace la petición que se soporta la característica. Esto puede conseguirse modificando la respuesta de la entidad distante o generando su propio mensaje.

7.9.3 Negociación utilizando el marco ampliable – RAS

La negociación de las características RAS se aplica a la fase de descubrimiento, registro y establecimiento de la comunicación. En particular, se aplica al intercambio de mensajes de descubrimiento (GRQ, GCF, GRJ), mensajes de registro (RRQ, RCF, RRJ), mensajes de petición de admisión (ARQ, ACF, ARJ), mensajes de petición de localización (LRQ, LCF, LRJ), mensajes de control de servicio (SCI/SCR) y el mensaje no normalizado.

En la negociación RAS, las entidades pueden especificar el conjunto de características que necesitan para que una transacción tenga éxito, el conjunto de características que desean y el conjunto de características que soportan.

7.9.3.1 Procesamiento por la entidad solicitante

Una entidad solicitante (normalmente un punto extremo) utiliza los elementos de la estructura **FeatureSet** (**conjunto de características**) para especificar los diversos tipos de características que requiere. Especifica el conjunto de características que necesita mediante el campo **neededFeatures**

(**características necesarias**), el conjunto de características que desea mediante el campo **desiredFeatures** (**características deseadas**) y el conjunto de características que soporta con el campo **supportedFeatures** (**características soportadas**). Estos tres tipos de campos están en la estructura **FeatureSet**.

En respuesta a su petición, la entidad peticionaria recibe un mensaje de confirmación o de rechazo.

Si la petición se rechaza, la entidad respondedora puede haber incluido un conjunto de **neededFeatures** que la entidad solicitante debe soportar para que la petición tenga éxito. Si así ocurre y la entidad solicitante soporta las características necesarias, dicha entidad puede reenviar una petición especificando que soporta las características necesarias por parte de la entidad respondedora.

Si se acepta la petición, es necesario aplicar procedimientos especiales para asegurar que la negociación es compatible con una vuelta atrás en el proceso. Para ello, la entidad solicitante verifica que las características especificadas como necesarias están enumeradas en la respuesta como **supportedFeatures**. Si una entidad solicitante no observa las características que necesita en el campo **supportedFeatures** del mensaje de respuesta, asumirá que la entidad respondedora no soporta dichas características. Si la entidad solicitante determina que no puede continuar en estas circunstancias, cancelará la operación que estaba intentando realizar (es decir, enviará un mensaje DRQ si inicialmente envió un ARQ, y así sucesivamente), de forma que el estado de la entidad respondedora vuelve a su situación anterior.

7.9.3.2 Procesamiento por la entidad respondedora

La entidad respondedora (típicamente un controlador de acceso) analiza las características especificadas en el campo **neededFeatures** de la petición para determinar si puede aceptar la petición. También analiza los campos **neededFeatures**, **desiredFeatures** y **supportedFeatures** para determinar si la entidad solicitante soporta las características que necesita.

Si la entidad respondedora es un controlador de acceso que envía un mensaje LRQ en respuesta a la recepción de un mensaje ARQ, el controlador de acceso copiará todas las características que no ha proporcionado en el LRQ. Al tratar de determinar si el conjunto de características necesarias es soportado, el controlador de acceso examinará las características soportadas del punto extremo que pueden resolver el ARQ localmente o bien en respuesta a un mensaje LCF, y las características soportadas por el controlador de acceso.

Si la entidad respondedora determina que el conjunto necesario de características es soportado por ambas entidades, la entidad respondedora puede acusar recibo de la petición. La entidad respondedora enumera el conjunto de características que ha decidido soportar en el campo **supportedFeatures** de su respuesta. Si se acepta la petición, todas las **neededFeatures** de la petición deben estar incluidas en el campo **supportedFeatures** de la respuesta. La entidad respondedora puede también incluir **desiredFeatures**.

Si la entidad respondedora necesita que se soporten características adicionales, rechazará la petición. Si desea declarar las características que se deben soportar para que la petición tenga éxito, lo hace en el campo **neededFeatures** del mensaje de rechazo. La entidad respondedora puede también incluir cualesquiera otras **desiredFeatures** y **supportedFeatures** en el mensaje de rechazo.

7.9.4 Negociación utilizando el marco ampliable – Señalización de llamada

A continuación se describe el proceso de negociación para el canal de señalización de llamada.

7.9.4.1 Procesamiento por el punto extremo iniciador

Un punto extremo iniciador puede especificar las características que necesita para una llamada, las características que desea y las características que soporta. El conjunto de características que necesita lo especifica mediante el campo **neededFeatures** del mensaje Establecimiento. También especifica

el conjunto de características que desea utilizando el campo **desiredFeatures** y el conjunto de características que soporta mediante el campo **supportedFeatures**.

Si la llamada se rechaza, una o más entidades respondedoras pueden haber incluido un conjunto de **neededFeatures** que el punto extremo iniciador debe soportar para que la llamada tenga éxito. Si ese es el caso, y el punto extremo iniciador soporta las características necesarias, el punto extremo iniciador puede iniciar de nuevo la llamada especificando que las diversas entidades a lo largo del trayecto de señalización soportan las características necesarias.

Si la llamada se acepta, el punto extremo iniciador verificará que las características que él especifica como necesarias se enumeran como **supportedFeatures** en el mensaje Aviso o Conexión. Si un punto extremo iniciador observa que las características que necesita no están en el campo **supportedFeatures** del mensaje, considerará que las entidades del trayecto de señalización de llamada no soportan las características que necesita. Si la entidad iniciadora determina que no puede continuar en esas circunstancias, liberará la llamada utilizando un mensaje Liberación Completa.

Cuando un punto extremo iniciador recibe un conjunto de capacidades vacío como resultado de una pausa y reencaminamiento de una tercera parte, suprimirá todo el conocimiento que tenga sobre las capacidades de las entidades distantes. Cuando el punto extremo reciba un conjunto de capacidades no vacío, enviará su conjunto de características utilizando el campo **featureSet** del mensaje facilidad con el campo **reason** puesto a **featureSetUpdate** (**actualización de conjunto de características**). El campo **replacementFeatureSet** (**conjunto de características de sustitución**) de este mensaje se pone a VERDADERO. Cuando se recibe el conjunto de características del punto extremo distante en un mensaje facilidad, el contenido puede interpretarse tal como se ha expuesto anteriormente.

7.9.4.2 Procesamiento por entidades intermedias

Las entidades intermedias que se encuentran a lo largo del trayecto de señalización de la llamada, tales como controlador de acceso y elementos de frontera pueden también interactuar en el proceso de negociación.

Las entidades de señalización intermedia tales como controladores de acceso y elementos de frontera pueden – sujetos a consideraciones de seguridad – añadir las características que les sean necesarias, que deseen y que soporten, a los mensajes que pasan a través de ellas. Las entidades intermedias pueden suprimir características deseadas y soportadas especificadas en los mensajes (incluidos los mensajes de Establecimiento, Aviso y Conexión) antes de pasarlos. Las entidades intermedias no suprimirán campos de características necesarias de un mensaje Establecimiento o de un mensaje Facilidad, salvo que éstos tengan por objeto soportar las características que aquéllas están suprimiendo. Si la entidad intermedia no desea permitir una característica necesaria, rechazará o terminará la llamada.

Si una entidad intermedia decide soportar una característica solicitada señalizada en un mensaje Establecimiento, debería suprimir del mensaje Establecimiento la petición de la característica antes de pasarlo. La entidad intermedia debe señalizar las características que soporta en los mensajes Aviso (si se envía) o Conexión junto con el conjunto de características soportadas por los destinos.

Cuando una entidad intermedia recibe un parámetro **featureSet** en un mensaje Facilidad con el campo **replacementFeatureSet** puesto a VERDADERO, debe modificar las características indicadas de acuerdo con sus requisitos de forma similar a como modifica las características señalizadas en los mensajes Establecimiento, Aviso o Conexión. Entonces pasa el mensaje.

7.9.4.3 Procesamiento por el punto extremo llamado

El punto extremo llamado analiza las características especificadas en el campo **neededFeatures** del mensaje Establecimiento para determinar si puede aceptar la llamada. También analiza los campos **neededFeatures**, **desiredFeatures** y **supportedFeatures** para determinar si las características que

necesita son soportadas por las diversas entidades a lo largo del trayecto de señalización de la llamada.

Si el punto extremo llamado determina que las entidades apropiadas soportan el conjunto necesario de características, puede aceptar la llamada. El punto extremo llamado enumera el conjunto de características que ha decidido soportar en el campo **supportedFeatures** de los mensajes Aviso (si se envía) y Conexión. Si se acepta la llamada, todas las **neededFeatures** del mensaje Establecimiento deben declararse en el campo **supportedFeatures** de los mensajes de señalización de llamada Aviso (si se envía) y Conexión. El punto extremo llamado puede asimismo incluir en el mensaje el campo **desiredFeatures**.

Si el punto extremo llamado necesita que las entidades del trayecto de señalización de la llamada soporten características adicionales, rechazará la llamada enviando un mensaje Liberación Completa. Si desea declarar las características que se deben soportar para que la llamada tenga éxito, lo especifica utilizando el campo **neededFeatures** del mensaje Liberación Completa. El punto extremo llamado puede también incluir cualquier **desiredFeatures** y **supportedFeatures** en el mensaje Liberación Completa.

Cuando un punto extremo llamado recibe un conjunto de capacidades vacío como resultado de una pausa y reencaminamiento de una tercera parte, actuará exactamente igual que si hubiese iniciado la llamada. Es decir, suprimirá todo el conocimiento que tenga sobre capacidades de las entidades distantes. Cuando el punto extremo reciba un conjunto de capacidades no vacío, enviará su conjunto de características utilizando el campo **featureSet** del mensaje Facilidad con el campo **reason** puesto a **featureSetUpdate**. El campo **replacementFeatureSet** de este mensaje se pone a VERDADERO. Cuando se recibe el conjunto de características del punto extremo distante en un mensaje Facilidad, el contenido puede interpretarse tal como se ha expuesto anteriormente.

8 Procedimientos de señalización de la llamada

La provisión de la comunicación se efectúa siguiendo los pasos que a continuación se indican:

– Fase A: Establecimiento de la comunicación (véase 8.1).
– Fase B: Comunicación inicial e intercambio de capacidad (véase 8.2).
– Fase C: Establecimiento de comunicación audiovisual (véase 8.3).
– Fase D: Servicios de la llamada (véase 8.4).
– Fase E: Terminación de la llamada (véase 8.5).

8.1 Fase A – Establecimiento de la comunicación

El establecimiento de la comunicación se efectúa utilizando los mensajes de control de llamada definidos en la Rec. UIT-T H.225.0, de acuerdo con los procedimientos de control de llamada definidos más abajo. Las peticiones de reserva de anchura de banda deberán efectuarse lo antes posible.

Si se especifican la dirección alias y la dirección de transporte, se preferirá la dirección alias.

No hay ninguna sincronización explícita ni enganche entre dos puntos extremos durante el procedimiento de establecimiento de la comunicación. Esto significa que el punto extremo A puede enviar un mensaje Establecimiento al punto extremo B exactamente al mismo tiempo que el punto extremo B envía un mensaje Establecimiento al punto extremo A. Corresponde a la aplicación de terminal determinar si sólo se desea una llamada y ejercer la acción apropiada. Esta acción puede ser para un punto extremo indicar que está ocupado siempre que tiene un mensaje Establecimiento pendiente. Si un punto extremo puede soportar más de una llamada simultánea, debe indicar que está ocupado siempre que recibe un mensaje Establecimiento del mismo punto extremo con el cual tiene un mensaje Establecimiento pendiente.

Un punto extremo será capaz de enviar el mensaje Aviso. Aviso tiene el significado de que la parte llamada (usuario) ha sido avisada de una llamada entrante. Aviso será sólo originado por el último punto extremo llamado y por tanto sólo cuando ha sido avisado el usuario. En el caso de interfuncionamiento a través de una pasarela, la pasarela enviará Aviso cuando reciba una indicación de llamada de la RCC. Si un punto extremo puede responder a un mensaje Establecimiento con un mensaje Conexión, Llamada en Curso, o Liberación Completa en el plazo de 4 segundos, no es necesario enviar el mensaje Aviso. Un punto extremo que envía el mensaje Establecimiento puede esperar recibir un mensaje Aviso, Conexión, Llamada en Curso o Liberación Completa en un plazo de 4 segundos después de su transmisión con éxito.

El mensaje Conexión debe enviarse sólo si se está seguro de que el intercambio de capacidades H.245 concluirá con éxito y puede existir un nivel mínimo de comunicaciones, con el objeto de mantener la coherencia del significado del mensaje Conexión entre redes de paquetes y redes con conmutación de circuitos.

8.1.1 Establecimiento de comunicación básica – Ninguno de los puntos extremos está registrado

En el escenario mostrado en la figura 29, ninguno de los puntos extremos está registrado en un controlador de acceso. Los dos puntos extremos comunican directamente. El punto extremo 1 (punto extremo llamante) envía el mensaje Establecimiento (1) al identificador TSAP de canal de señalización de llamada conocido del punto extremo 2. El punto extremo 2 responde con el mensaje Conexión (4) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.

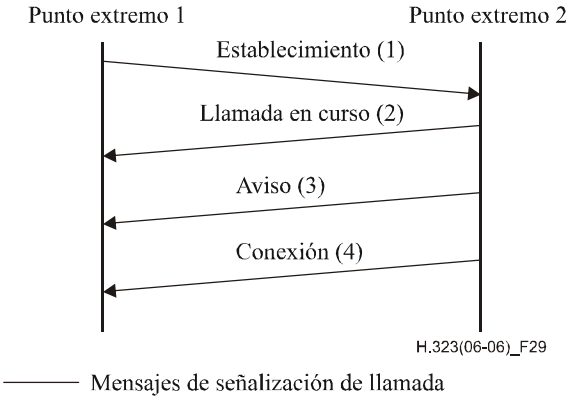


Figura 29/H.323 – Establecimiento de comunicación básica, sin controladores de acceso

8.1.2 Ambos puntos extremos registrados en el mismo controlador de acceso

En el escenario mostrado en la figura 30, ambos puntos extremos están registrados en el mismo controlador de acceso y el controlador de acceso ha optado por señalización de llamada directa. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con ese controlador de acceso. El controlador de acceso devolverá la dirección de transporte de canal de señalización de llamada del punto extremo 2 (punto extremo llamado) en la ACF. El punto extremo 1 envía entonces el mensaje Establecimiento (3) al punto extremo 2 utilizando esa dirección de transporte. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (5)/ACF (6) con el controlador de acceso. Es posible que el punto extremo 2 reciba un ARJ (6) en cuyo caso envía el mensaje Liberación Completa al punto extremo 1. El punto extremo 2 responde con el mensaje Conexión (8) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.

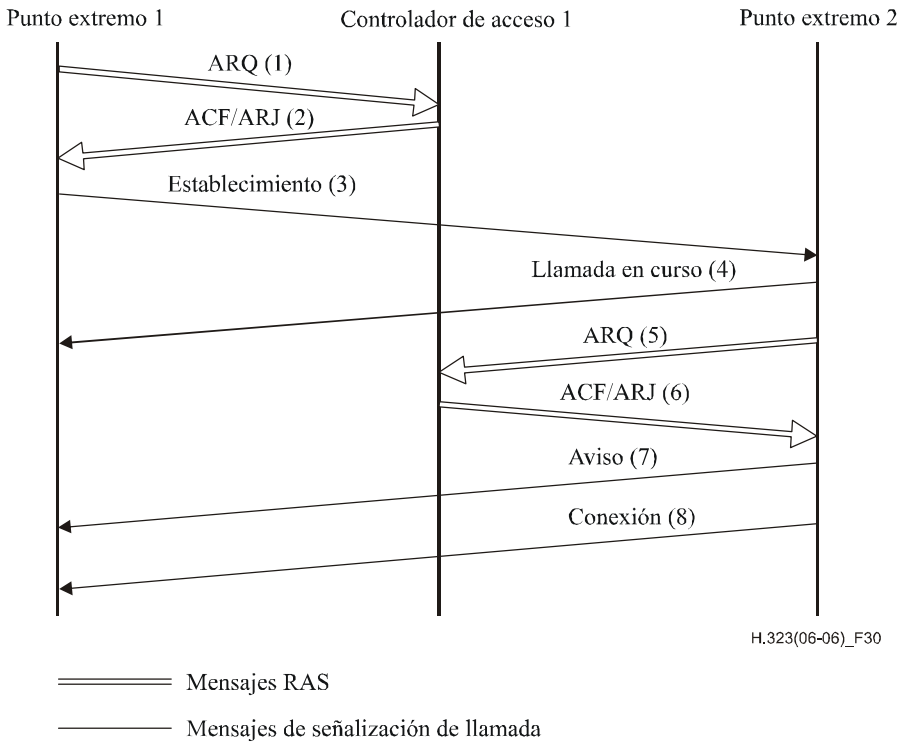


Figura 30/H.323 – Ambos puntos extremos registrados, el mismo controlador de acceso – Señalización de llamada directa

En el escenario mostrado en la figura 31, ambos puntos extremos están registrados en el mismo controlador de acceso y el controlador de acceso ha optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el controlador de acceso. El controlador de acceso devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF. El punto extremo 1 envía entonces el mensaje Establecimiento (3) utilizando esa dirección de transporte. El controlador de acceso envía a continuación el mensaje Establecimiento (4) al punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (6)/ACF (7) con el controlador de acceso. Es posible que el punto extremo 2 reciba un ARJ (7), en cuyo caso envía el mensaje Liberación Completa al controlador de acceso. El punto extremo 2 responde con el mensaje Conexión (9) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El controlador de acceso envía al punto extremo 1 el mensaje Conexión (10) que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 de controlador de acceso, dependiendo de si el controlador de acceso decide encaminar o no el canal de control H.245.

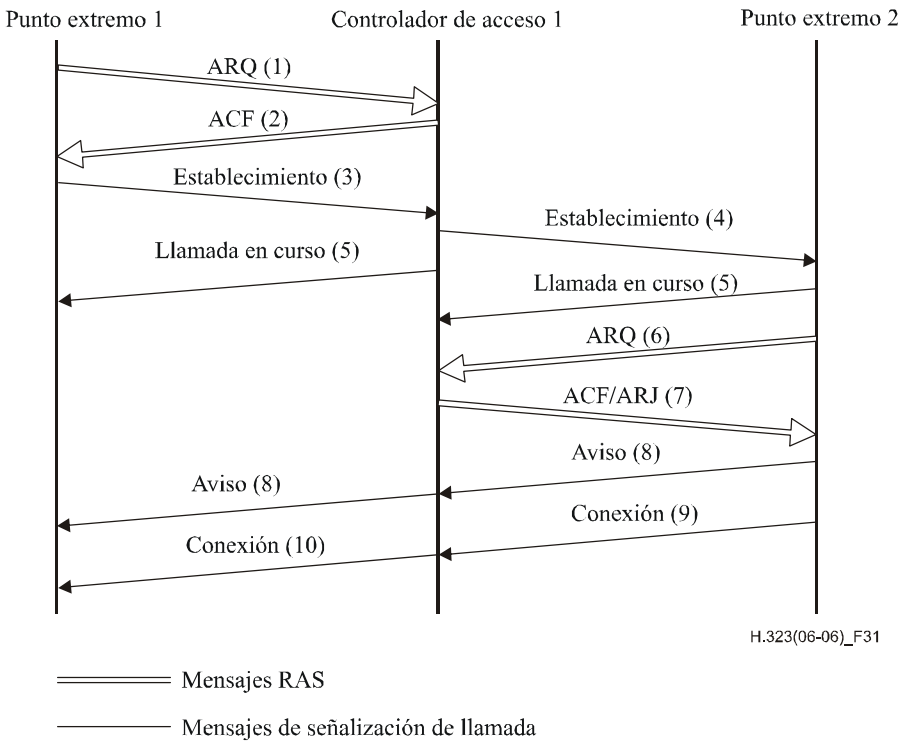


Figura 31/H.323 – Ambos puntos extremos registrados, el mismo controlador de acceso – Señalización de llamada encaminada por el controlador de acceso

8.1.3 Sólo el punto extremo llamante tiene controlador de acceso

En el escenario mostrado en la figura 32, el punto extremo 1 (punto extremo llamante) está registrado en un controlador de acceso, el punto extremo 2 (punto extremo llamado) no está registrado en un controlador de acceso y el controlador de acceso ha optado por señalización de llamada directa. El punto extremo 1 inicia el intercambio ARQ (1)/ACF (2) con el controlador de acceso. El punto extremo 1 envía entonces el mensaje Establecimiento (3) al punto extremo 2 utilizando la dirección de transporte de canal de señalización de llamada conocida. Si el punto extremo 2 desea aceptar la llamada, responde con el mensaje Conexión (6) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.

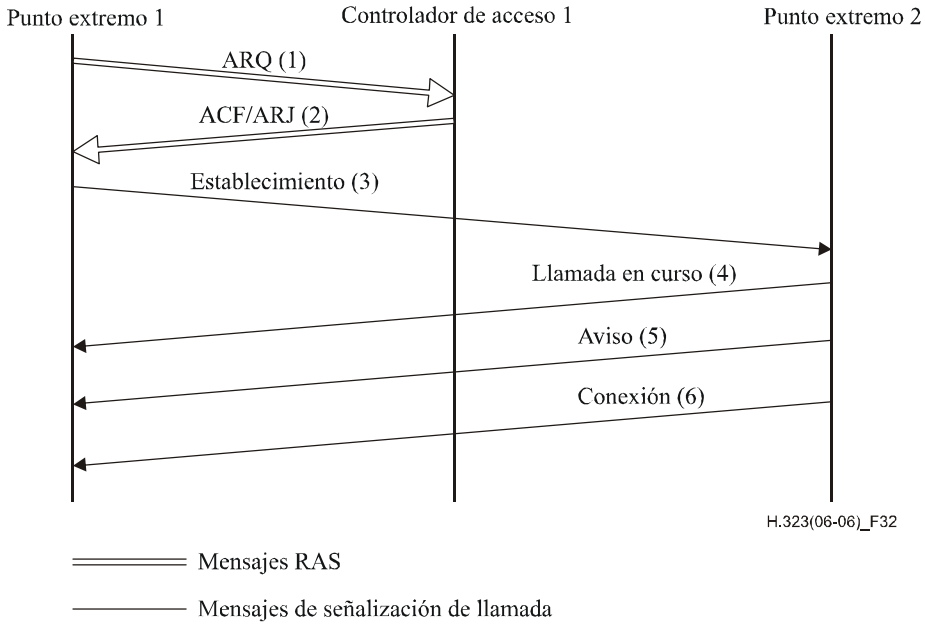


Figura 32/H.323 – Sólo el punto extremo llamante está registrado – Señalización de llamada directa

En el escenario mostrado en la figura 33, el punto extremo 1 (punto extremo llamante) está registrado en un controlador de acceso, el punto extremo 2 (punto extremo llamado) no está registrado en un controlador de acceso y el controlador de acceso ha optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con ese controlador de acceso. El controlador de acceso devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF (2). El punto extremo 1 envía entonces el mensaje Establecimiento (3) utilizando esa dirección de transporte. El controlador de acceso envía a continuación el mensaje Establecimiento (4) a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, responde con el mensaje Conexión (7) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El controlador de acceso envía el mensaje Conexión (8) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 de controlador de acceso, dependiendo de si el controlador de acceso decida encaminar o no el canal de control H.245.

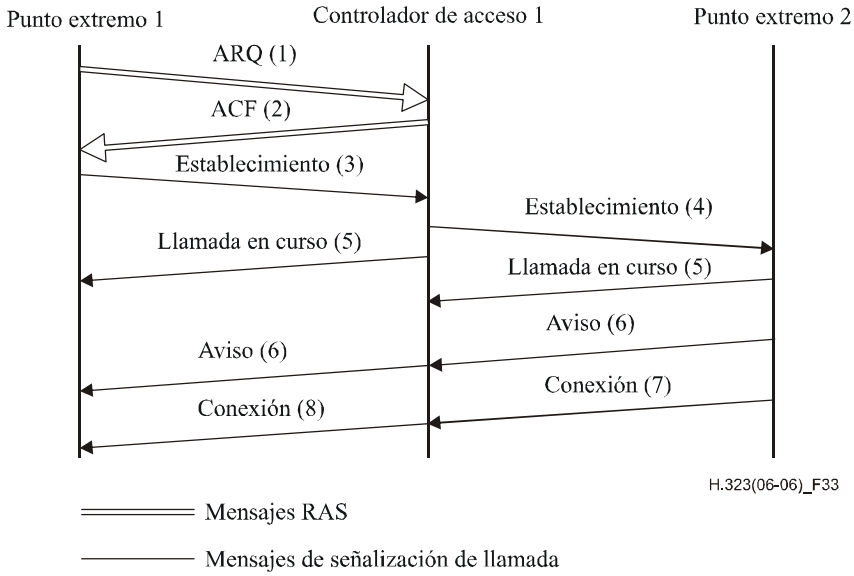


Figura 33/H.323 – Sólo el punto extremo llamante está registrado – Señalización de llamada encaminada por el controlador de acceso

8.1.4 Sólo el punto extremo llamado tiene controlador de acceso

En el escenario mostrado en la figura 34, el punto extremo 1 (punto extremo llamante) no está registrado en un controlador de acceso, el punto extremo 2 (punto extremo llamado) está registrado en un controlador de acceso y el controlador de acceso ha optado por la señalización de llamada directo. El punto extremo 1 envía el mensaje Establecimiento (1) al punto extremo 2 utilizando la dirección de transporte de canal de señalización de llamada conocida. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (3)/ACF (4) con el controlador de acceso. Es posible que el punto extremo 2 reciba un ARJ (4), en cuyo caso envía un mensaje Liberación Completa al punto extremo 1. El punto extremo 2 responde con el mensaje Conexión (6) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.

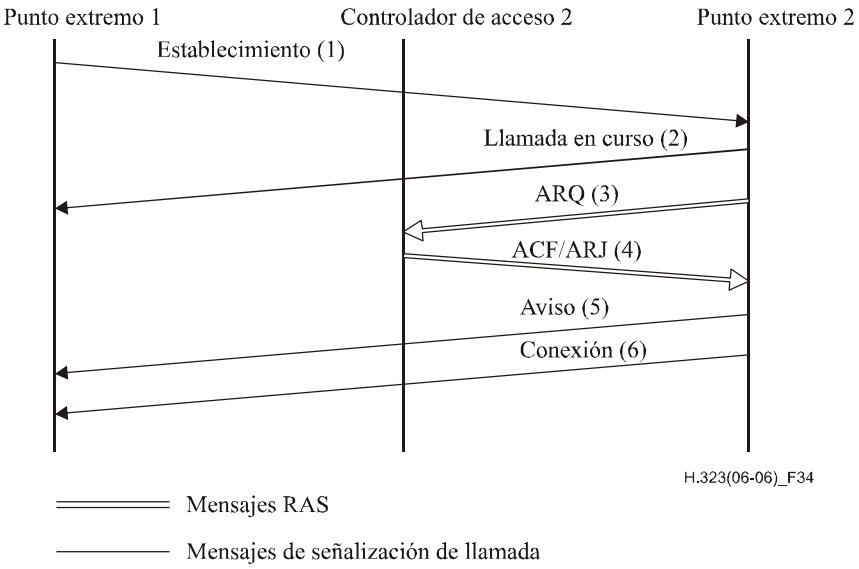


Figura 34/H.323 – Sólo el punto extremo llamado está registrado – Señalización de llamada directa

En el escenario mostrado en la figura 35, el punto extremo 1 (punto extremo llamante) no está registrado en un controlador de acceso, el punto extremo 2 (punto extremo llamado) está registrado en un controlador de acceso y el controlador de acceso ha optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) envía un mensaje Establecimiento (1) a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (3)/ACF (4) con el controlador de acceso. Si es aceptable, el controlador de acceso devolverá una dirección de transporte de canal de señalización de llamada de él mismo en ARJ (4) con un código de causa de **routeCallToGatekeeper** (**encaminamiento de llamada a controlador de acceso**). El punto extremo 2 responde al punto extremo 1 con un mensaje Facilidad (5) que contiene la dirección de transporte de señalización de llamada de su controlador de acceso. El punto extremo 1 envía entonces el mensaje Liberación Completa (6) al punto extremo 2. El punto extremo 1 responde con un mensaje Establecimiento (7) a la dirección de transporte de canal de señalización de llamada del controlador de acceso. El controlador de acceso envía el mensaje Establecimiento (8) al punto extremo 2. El punto extremo 2 inicia el intercambio de ARQ (9)/ACF (10) con ese controlador de acceso. El punto extremo 2 responde después con el mensaje Conexión (12) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El controlador de acceso envía el mensaje Conexión (13) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 de controlador de acceso dependiendo de si el controlador de acceso decide encaminar o no el canal de control H.245.

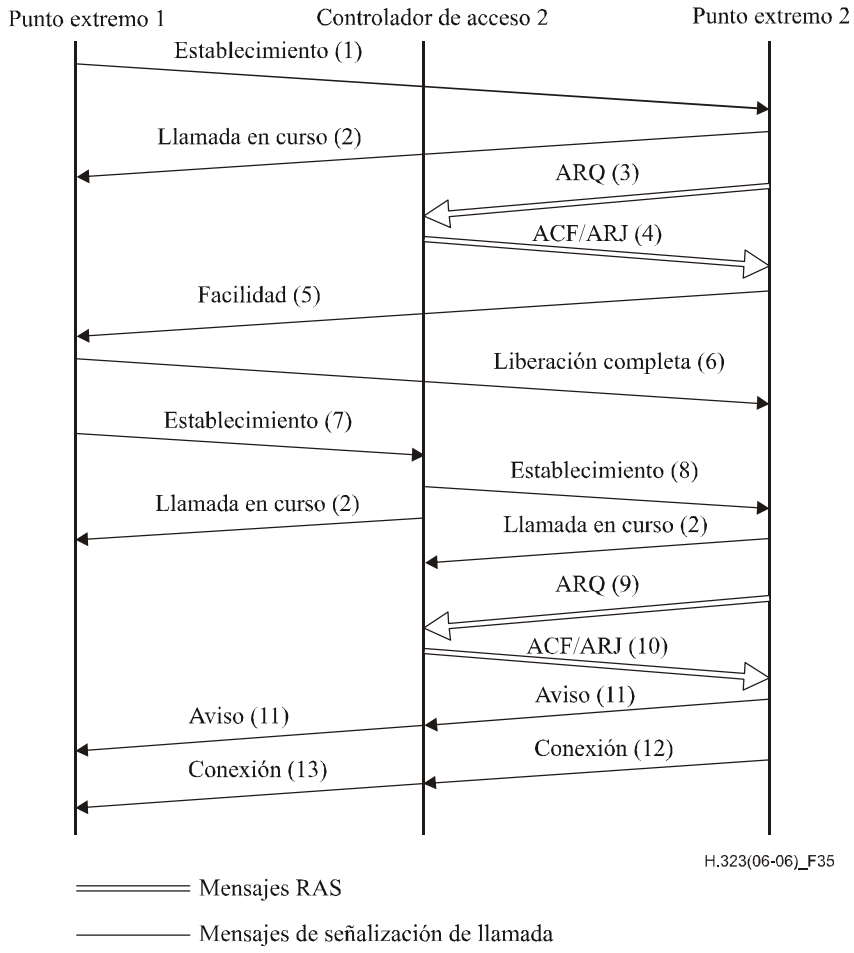


Figura 35/H.323 – Sólo el punto extremo llamado está registrado – Señalización de llamada encaminada por el controlador de acceso

8.1.5 Ambos puntos extremos registrados en controladores de acceso diferentes

En el escenario mostrado en la figura 36, ambos puntos extremos están registrados en controladores de acceso diferentes y ambos controladores de acceso han optado por la señalización de llamada directa. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el controlador de acceso 1. El controlador de acceso 1 puede devolver la dirección de transporte de canal de señalización de llamada del punto extremo 2 (punto extremo llamado) en la ACF si el controlador de acceso 1 tiene una manera de comunicar con el controlador de acceso 2. El punto extremo 1 envía entonces el mensaje Establecimiento (3) bien a la dirección de transporte devuelta por el controlador de acceso (si está disponible) o bien a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (5)/ACF (6) con el controlador de acceso 2. Es posible que el punto extremo 2 reciba un ARJ (6), en cuyo caso envía un mensaje Liberación Completa al punto extremo 1. El punto extremo 2 responde con el mensaje Conexión (8) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.

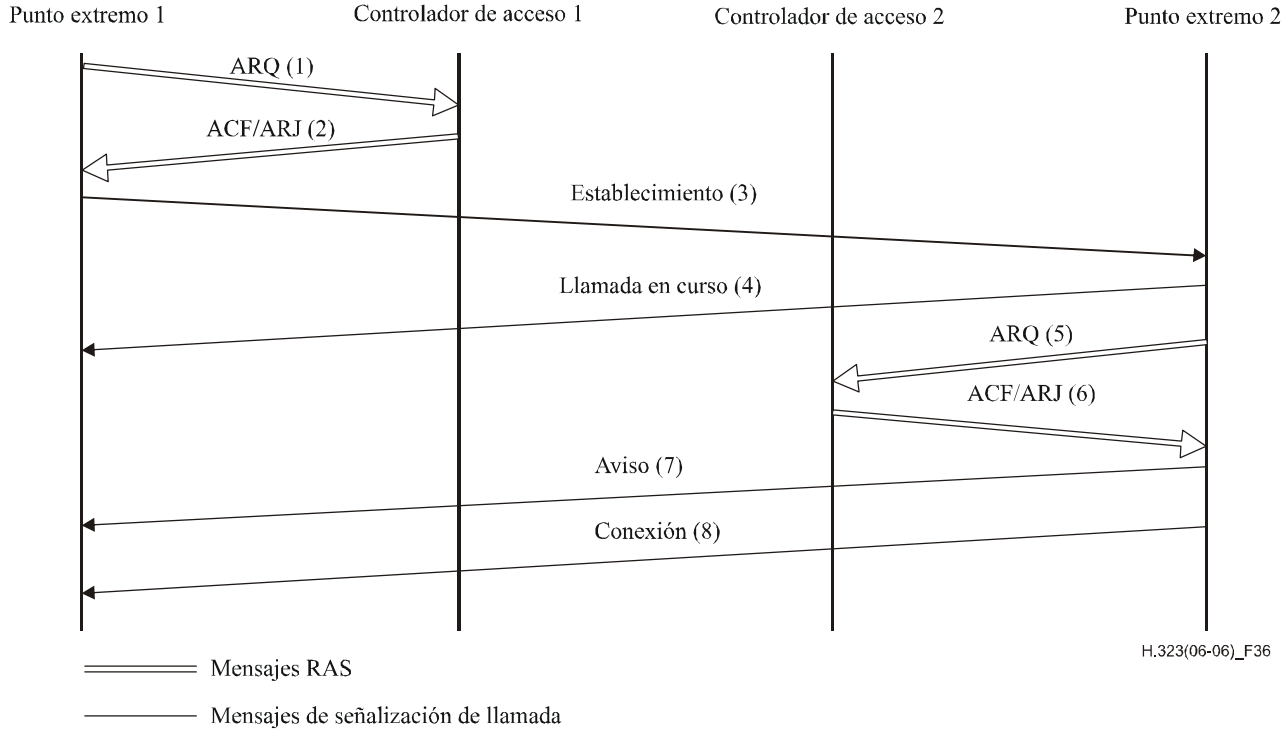


Figura 36/H.323 – Ambos puntos extremos registrados – Señalización de llamada directa de ambos controladores de acceso

En el escenario mostrado en la figura 37, ambos puntos extremos están registrados en diferentes controladores de acceso, el controlador de acceso del punto extremo llamante ha optado por la señalización de llamada directa y el controlador de acceso del punto extremo llamado ha optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el controlador de acceso 1. El controlador de acceso 1 puede devolver la dirección de transporte de canal de señalización de llamada del punto extremo 2 (punto extremo llamado) en la ACF (2) si el controlador de acceso 1 tiene una manera de comunicar con el controlador de acceso 2. El punto extremo 1 envía entonces el mensaje Establecimiento (3) bien a la dirección de transporte devuelta por el controlador de acceso (si está disponible) o bien a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia el intercambio ARQ (5)/ACF (6) con el controlador de acceso 2. Si es aceptable, el controlador de acceso 2 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en ARJ (6) con un código de causa de

routeCallToGatekeeper. El punto extremo 2 responde al punto extremo 1 con un mensaje Facilidad (7) que contiene la dirección de transporte de señalización de llamada del controlador de acceso 2. El punto extremo 1 envía entonces el mensaje Liberación Completa (8) al punto extremo 2. El punto extremo 1 enviará DRQ (9) al controlador de acceso 1 que responde con DCF (10). El punto extremo 1 inicia después un nuevo intercambio de ARQ (11)/ACF (12) con el controlador de acceso 1. El punto extremo 1 envía un mensaje Establecimiento (13) a la dirección de transporte de canal de señalización de llamada del controlador de acceso. El controlador de acceso 2 envía el mensaje Establecimiento (14) al punto extremo 2. El punto extremo 2 inicia el intercambio de ARQ (15)/ACF (16) con el controlador de acceso 2. El punto extremo 2 responde después con el mensaje Conexión (18) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El controlador de acceso 2 envía el mensaje Conexión (19) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 del controlador de acceso 2, dependiendo de si el controlador de acceso decide encaminar o no el canal de control H.245.

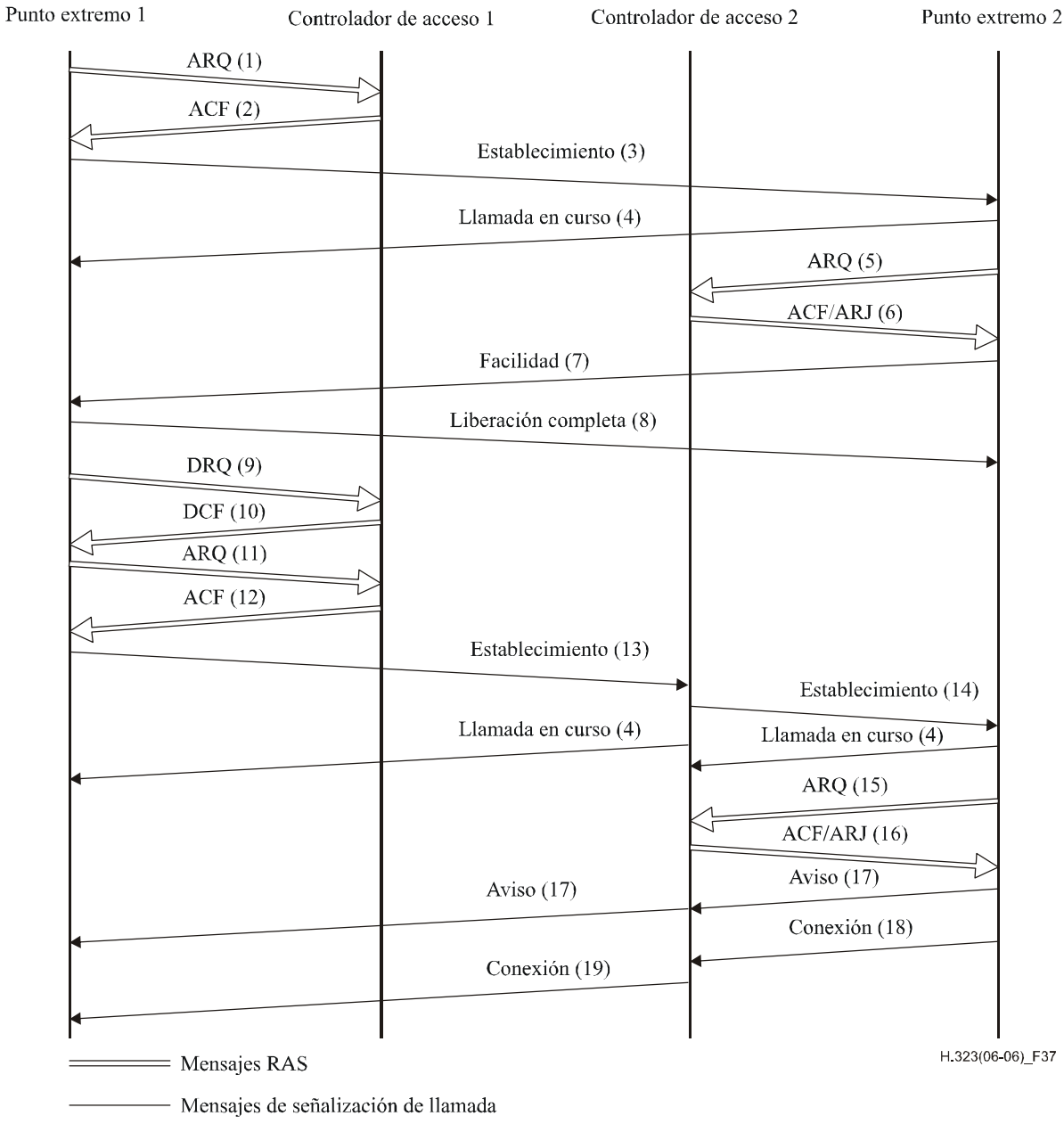


Figura 37/H.323 – Ambos puntos extremos registrados – Señalización de llamada directa/encaminada

En el escenario mostrado en la figura 38, ambos puntos extremos están registrados en controladores de acceso diferentes, el controlador de acceso del punto extremo llamante ha optado por encaminar la señalización de la llamada y el controlador de acceso del punto extremo llamado ha optado por la señalización de llamada directa. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el controlador de acceso 1. El controlador de acceso 1 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF (2). El punto extremo 1 envía entonces el mensaje Establecimiento (3) utilizando esa dirección de transporte. El controlador de acceso 1 envía entonces el mensaje Establecimiento (4) que contiene su dirección de transporte de canal de señalización de llamada a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia el intercambio ARQ (6)/ACF (7) con el controlador de acceso 2. Es posible que el punto extremo 2 reciba un ARJ (7), en cuyo caso envía un mensaje Liberación Completa al punto extremo 1. El punto extremo 2 responde al controlador de acceso 1 con el mensaje Conexión (9) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El controlador de acceso 1 envía el mensaje Conexión (10) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 del controlador de acceso 1, dependiendo de si el controlador de acceso decide encaminar o no el canal de control H.245.

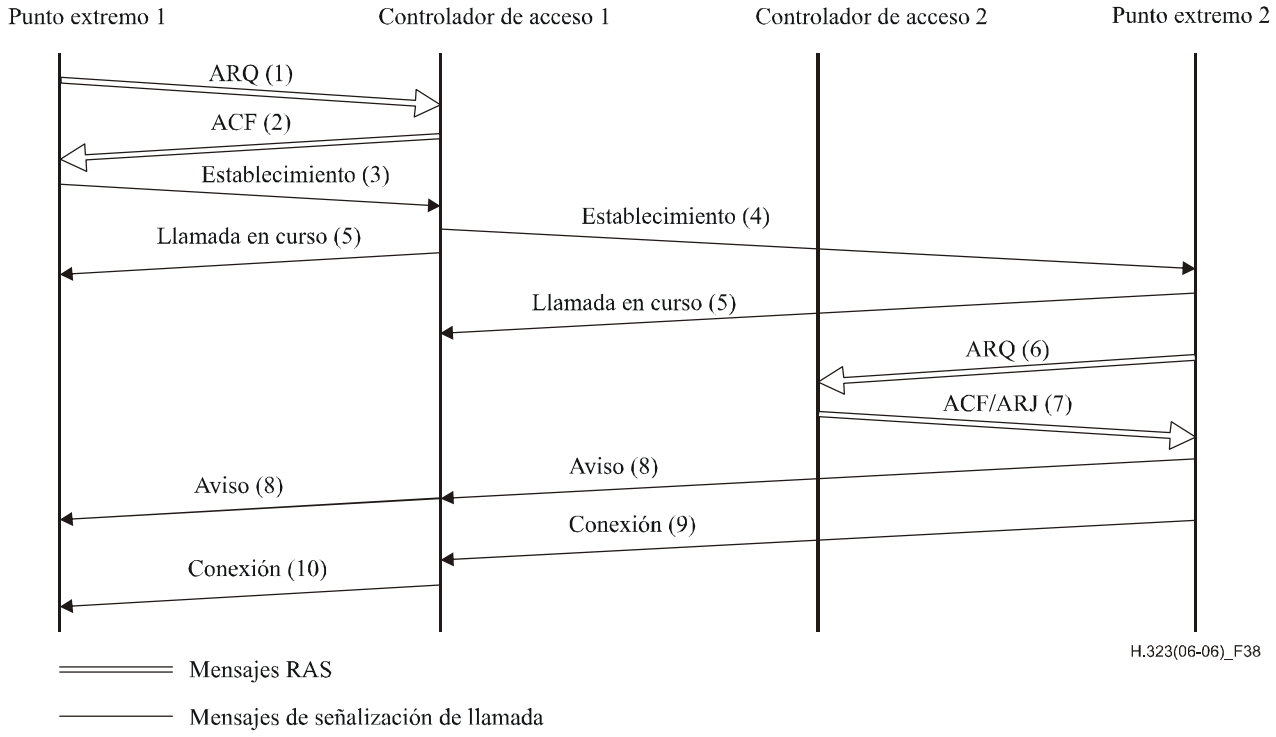


Figura 38/H.323 – Ambos puntos extremos registrados – Señalización de llamada encaminada/directa

En el escenario mostrado en la figura 39, ambos puntos extremos están registrados en controladores de acceso diferentes y ambos controladores de acceso han optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el controlador de acceso 1. El controlador de acceso 1 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF (2). El punto extremo 1 envía entonces el mensaje Establecimiento (3) utilizando esa dirección de transporte. El controlador de acceso 1 envía a continuación el mensaje Establecimiento (4) a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia el intercambio ARQ (6)/ACF (7) con el controlador de acceso 2. Si es aceptable, el controlador de

acceso 2 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en ARJ (7) con un código de causa de **routeCallToGatekeeper**. El punto extremo 2 responde al controlador de acceso 1 con un mensaje Facilidad (8) que contiene la dirección de transporte de señalización de llamada del controlador de acceso 2. El controlador de acceso 1 envía después el mensaje Liberación Completa (9) al punto extremo 2. El controlador de acceso 1 envía un mensaje Establecimiento (10) a la dirección de transporte de canal de señalización de llamada del controlador de acceso 2. El controlador de acceso 2 envía el mensaje Establecimiento (11) al punto extremo 2. El punto extremo 2 inicia el intercambio de ARQ (12)/ACF (13) con el controlador de acceso 2. El punto extremo 2 responde después al controlador de acceso 2 con el mensaje Conexión (15) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El controlador de acceso 2 envía el mensaje Conexión (16) al controlador de acceso 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 del controlador de acceso 2, dependiendo de si el controlador de acceso decide encaminar o no el canal de control H.245. El controlador de acceso 1 envía el mensaje Conexión (17) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 enviada por el controlador de acceso 2 o una dirección de transporte de canal de control H.245 del controlador de acceso 1, dependiendo de si el controlador de acceso 1 decide encaminar o no el canal de control H.245.

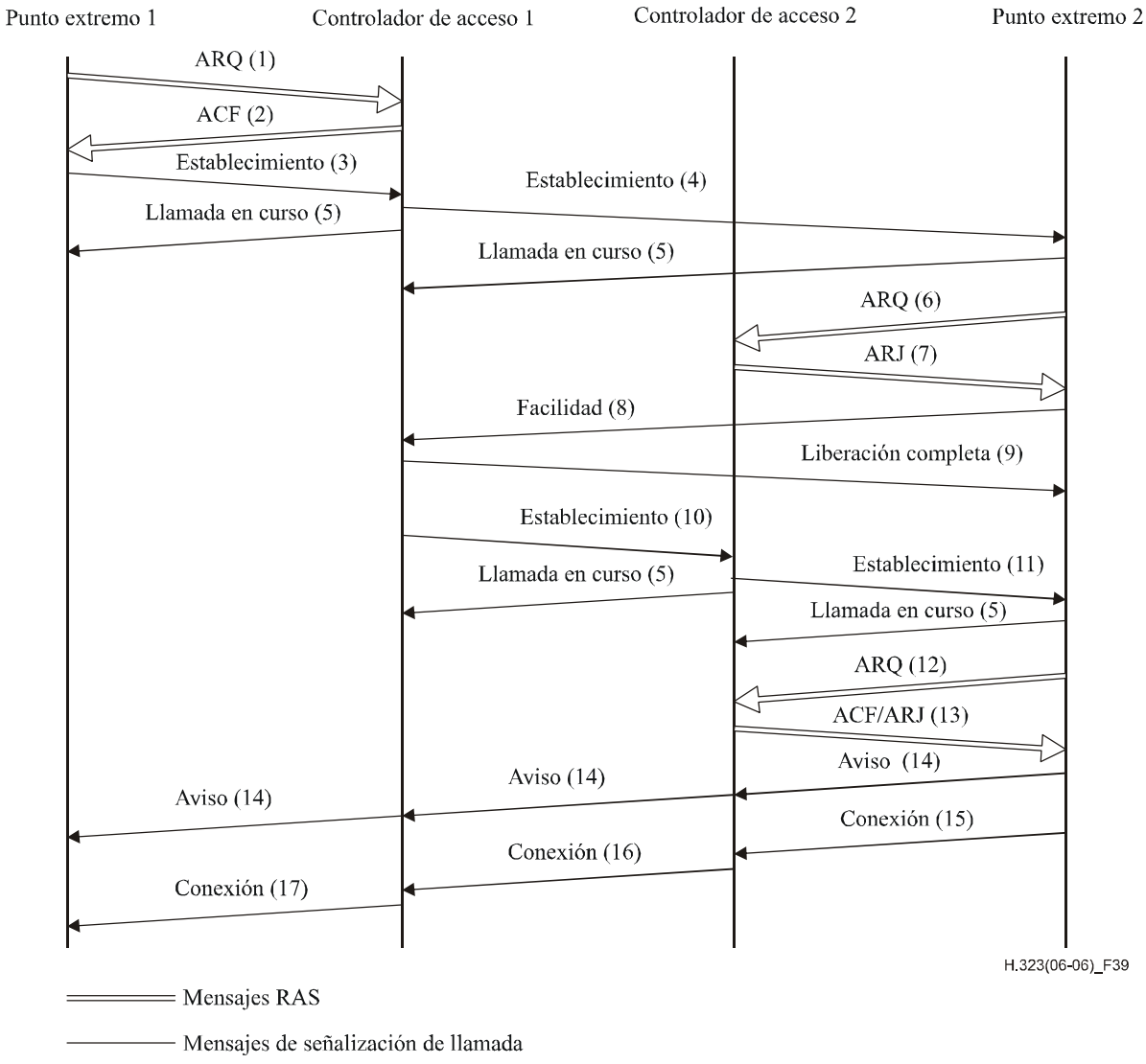


Figura 39/H.323 – Ambos puntos extremos registrados – Ambos controladores de acceso encaminan la señalización de llamada

8.1.6 Señalización opcional del punto extremo llamado

Los procedimientos definidos en 8.1.4 y 8.1.5 demuestran que cuando se registra un punto extremo llamado en un controlador de acceso, se envía inicialmente un mensaje Establecimiento al punto extremo llamado desde el punto extremo llamante o el controlador de acceso del punto extremo llamante. Si el controlador de acceso del punto extremo llamado desea usar el modelo de llamada encaminada por el controlador de acceso, retorna su propia dirección de transporte de canal de señalización de llamada en el ARJ. El punto extremo llamado utiliza entonces el mensaje Facilidad para redireccionar la llamada a la dirección de transporte de señalización de llamada del controlador de acceso del punto extremo llamado. Estos procedimientos suponen que el punto extremo llamante o el controlador de acceso del punto extremo llamante sólo conoce la dirección de transporte del canal de señalización del punto extremo llamado. Esta dirección puede haber sido recibida en un LCF enviado en respuesta a un LRQ que solicita la dirección del punto extremo llamado o puede ser conocida por métodos fuera de banda.

Si el controlador de acceso del punto extremo llamado desea un modelo de llamada encaminada por el controlador de acceso, puede retornar su propia dirección de transporte de señalización de llamada en el LCF. Esto permitirá al punto extremo llamante o al controlador de acceso del punto extremo llamante enviar el mensaje Establecimiento directamente al controlador de acceso del punto extremo llamado, eliminando así el proceso de redireccionamiento.

En la figura 40 se muestra un ejemplo de este escenario, ejemplo en el que ambos puntos extremos están registrados en controladores de acceso diferentes, y ambos controladores de acceso deciden encaminar la señalización de llamada (similar al caso de la figura 39). El punto extremo 1 (punto extremo llamante) envía un ARQ (1) al controlador de acceso 1. El controlador de acceso 1 multidifunde un LRQ (2) para localizar el punto extremo llamado 2. El controlador de acceso 2 retorna un LCF (3) con su propia dirección de transporte de canal de señalización de llamada. Así, el controlador de acceso 1 enviará posteriormente un mensaje Establecimiento (6) a la dirección de transporte de canal de señalización de llamada del controlador de acceso 2, y el controlador de acceso 2 enviará un mensaje Establecimiento (8) al punto extremo 2. El punto extremo 2 inicia el intercambio ARQ (9)/ACF (10) con el controlador de acceso 2. El punto extremo 2 responde entonces al controlador de acceso 2 con el mensaje Conexión (12), que contiene su propia dirección de transporte de canal de control H.245 para uso en la señalización H.245. El controlador de acceso 2 envía el mensaje Conexión (13) al controlador de acceso 1, que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2, o una dirección de transporte de canal de control H.245 del controlador de acceso 2, según que el controlador de acceso 2 decida o no encaminar el canal de control H.245. El controlador de acceso 1 envía el mensaje Conexión (14) al punto extremo 1, que puede contener la dirección de transporte de canal de control H.245 enviada por el controlador de acceso 2, o una dirección de transporte de canal de control H.245 del controlador de acceso 1, según que el controlador de acceso 1 decida o no encaminar el canal de control H.245.

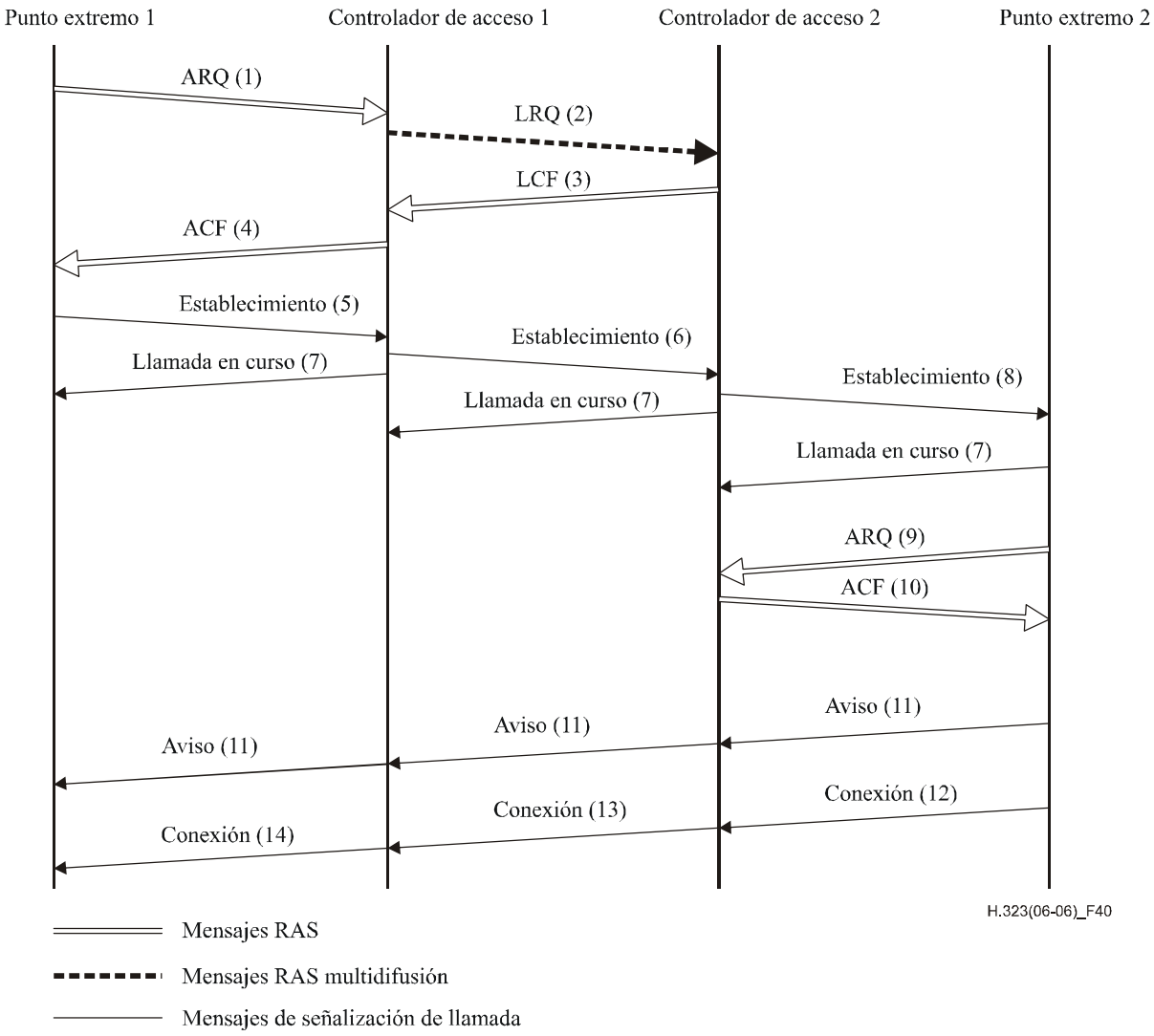


Figura 40/H.323 – Señalización opcional de punto extremo llamado

8.1.7 Procedimiento de conexión rápida

Los puntos extremos H.323 pueden establecer canales de medios en una llamada utilizando los procedimientos definidos en la Rec. UIT-T H.245 o el procedimiento "de conexión rápida" descrito en esta cláusula. Con el procedimiento de conexión rápida los puntos extremos pueden establecer una comunicación punto a punto básica con apenas un sólo intercambio de mensajes de ida y vuelta, lo que permite una entrega inmediata de trenes de medios al efectuar la conexión de la llamada.

El punto extremo llamante inicia el procedimiento de conexión rápida enviando un mensaje Establecimiento que contiene el elemento **arranque rápido** (**fastStart**) al punto extremo llamado. El elemento **fastStart** consiste en una secuencia de estructuras **OpenLogicalChannel** que describen los canales de medios que el punto extremo llamante propone enviar y recibir, incluidos todos los de los parámetros necesarios para abrir inmediatamente e iniciar la transferencia de medios por los canales. A continuación se examinan algunos detalles del contenido y la utilización del elemento **fastStart**.

El punto extremo llamado puede rechazar la utilización del procedimiento de conexión rápida porque no lo implementa o bien porque desea invocar características que requieren la utilización de los procedimientos definidos en la Rec. UIT-T H.245. El rechazo del procedimiento de conexión rápida se lleva a cabo bien mediante la no devolución del elemento **fastStart** o incluyendo el elemento **fastConnectRefuse** en ningún mensaje de señalización de llamada H.225.0 hasta el

mensaje Conexión incluido. Se debe señalar que un punto extremo puede omitir elementos **fastStart** en un mensaje previo a conexión, sino posteriormente devolver el elemento **fastStart** en el mensaje Conexión aceptando por tanto el procedimiento de conexión rápida. Rechazar el procedimiento de conexión rápida (o no iniciarlo) requiere que se utilicen los procedimientos H.245 para intercambiar capacidades y abrir canales de medios.

Cuando el punto extremo llamado desea aplicar el procedimiento de conexión rápida, envía un mensaje de señalización de llamada H.225.0 (Llamada en Curso, Progreso, Aviso o Conexión) que contiene un elemento **fastStart** seleccionando entre las propuestas **openLogicalChannel** ofrecidas por el punto extremo llamante. El punto extremo procesará cada uno de estos mensajes hasta que determine que la conexión rápida es aceptada o rehusada. Aunque el punto extremo llamante puede recibir el elemento **fastStart** en un mensaje Facilidad enviado por un controlador de acceso, el punto extremo llamado no utilizará el mensaje Facilidad para enviar **fastStart**. Los canales así aceptados se consideran abiertos como si se hubieran seguido los procedimientos **openLogicalChannel** y **openLogicalChannelAck** H.245 habituales. El punto extremo llamado no incluirá un elemento **fastStart** en ningún mensaje de señalización de llamada H.225.0 enviado después del mensaje Conexión, y no incluirá **fastStart** en ningún mensaje de señalización de llamada H.225.0 a menos que el mensaje Establecimiento contenga un elemento **fastStart**.

El punto extremo llamado puede empezar la transmisión de medios (según los canales abiertos) inmediatamente después de enviar un mensaje de señalización de llamada H.225.0 que contiene **fastStart**. Por consiguiente, el punto extremo llamante debe estar preparado para recibir medios en *cualquiera* de los canales de recepción que se propone en el mensaje Establecimiento, ya que es posible que los medios se reciban antes del mensaje de señalización de llamada H.225.0 indicando precisamente qué canales se han de utilizar. Una vez que el punto extremo llamante recibe un mensaje de señalización de llamada H.225.0 que contiene **fastStart**, el punto extremo llamante puede dejar de intentar la recepción de medios por los canales para los que no fueron aceptadas las propuestas por el punto extremo llamado. Obsérvese que los requisitos nacionales pueden prohibir a los puntos extremos llamados que transmitan medios, o limitar la naturaleza del contenido de los trenes de medios, antes de la transmisión de un mensaje Conexión; corresponde al punto extremo cumplir los requisitos aplicables. Si el punto extremo llamante coloca el elemento **espera para conexión de medios** (**mediaWaitForConnect**) en VERDADERO en el mensaje Establecimiento, el punto extremo llamado no enviará ningún medio hasta después de que se envíe el mensaje Conexión.

El punto extremo llamante puede empezar inmediatamente la transmisión de medios (según los canales abiertos) al recibir un mensaje de señalización de llamada H.225.0 que contiene **fastStart**. Por consiguiente, el punto extremo llamado debe estar preparado para recibir inmediatamente medios en los canales que aceptó en el mensaje de señalización de llamada H.225.0 con **fastStart**. Obsérvese que los requisitos nacionales pueden prohibir a los puntos extremos llamantes que transmitan medios antes de recibir un mensaje Conexión; corresponde al punto extremo cumplir los requisitos aplicables.

NOTA 1 – Una entidad no enviará un elemento **fastStart** vacío en ningún mensaje (es decir, un elemento **fastStart** contendrá al menos una propuesta **OpenLogicalChannel**). Si un punto extremo recibe un elemento **fastStart** que no tiene ninguna propuesta **OpenLogicalChannel**, ignorará el elemento **fastStart**.

NOTA 2 – Cuando un punto extremo o un controlador de acceso que interviene en la señalización de llamada recibe un elemento **fastStart** en un mensaje Llamada en Curso, no podrá retransmitir el procedimiento de llamada si el mensaje Llamada en Curso ha sido ya enviado al lado de origen. En tal caso, se establecerá una correspondencia entre el elemento **fastStart** del mensaje Llamada en Curso y elemento **fastStart** de un mensaje Facilidad.

8.1.7.1 Propuesta, selección y apertura de canales de medios

El punto extremo llamante puede proponer múltiples canales de medios, o varios conjuntos de características alternativas para cada canal de medios, codificando múltiples estructuras **OpenLogicalChannel** dentro del elemento **fastStart** del mensaje Establecimiento. Cada estructura **OpenLogicalChannel** dentro del elemento **fastStart** describe exactamente un canal de medios unidireccional o un canal de medios bidireccional.

En el mensaje Establecimiento, cada **OpenLogicalChannel** es una propuesta para establecer un canal de medios. Las propuestas **OpenLogicalChannel** están incluidas en el elemento **fastStart** por orden de preferencia: las alternativas preferidas se enumeran primero en la secuencia **fastStart**; las propuestas para abrir canales audio se enumerarán antes que los canales para cualquier otro tipo de medios. En el mensaje de señalización de llamada H.225.0 con **fastStart** enviado como respuesta al mensaje Establecimiento, cada **OpenLogicalChannel** es una aceptación de un canal de medios propuesto e indica los canales que están establecidos y que pueden ser utilizados inmediatamente para la transmisión de medios.

Si un elemento ofrecido **dataType** especifica criptación mediante la opción **h235Media**, el elemento **encryptionAuthenticationAndIntegrity** incluido puede tener un elemento **encryptionCapability** con varios algoritmos de criptación (entre ellos el algoritmo NULL). Se adoptará esta construcción para ofrecer una selección de alguno de los algoritmos especificados para la criptación de la capacidad de medios asociada.

En una estructura **openLogicalChannel** que propone un canal para transmisión del punto extremo llamante al punto extremo llamado, el elemento **forwardLogicalChannelParameters** contendrá parámetros que especifican las características del canal propuesto, y se omitirá el elemento **reverseLogicalChannelParameters**. Cada estructura **OpenLogicalChannel** tendrá un valor **forwardLogicalChannelNumber** único. Las propuestas alternativas para el mismo canal de transmisión contendrán el mismo valor **sessionID** en **H2250LogicalChannelParameters**. El elemento **mediaChannel** se omitirá en la propuesta y será proporcionado por el punto extremo llamado si la propuesta es aceptada. Se colocarán los otros elementos **H2250LogicalChannelParameters** y **dataType** para describir correctamente las capacidades de transmisión del punto extremo llamante asociado con este canal propuesto. El punto extremo llamante puede elegir no proponer ningún canal para transmisión del punto extremo llamante al punto extremo llamado porque desea utilizar más adelante los procedimientos H.245 para establecer esos canales.

En el mensaje Establecimiento, cada **OpenLogicalChannel** que propone un canal unidireccional para la transmisión desde el punto extremo llamante al punto extremo llamado y que transporte medios utilizando RTP contendrá el elemento **mediaControlChannel** (que indica el canal RTPC inverso) en el elemento **H2250LogicalChannelParameters** de la estructura **forwardLogicalChannelParameters**.

En un **openLogicalChannel** que propone un canal para transmisión del punto extremo llamado al punto extremo llamante, se incluirá el elemento **reverseLogicalChannelParameters** que contendrá parámetros que especifican las características del canal propuesto. Debe incluirse también el elemento **forwardLogicalChannelParameters** (porque no es opcional), con el elemento **dataType** colocado en **nullData** (**datos nulos**), **multiplexParameters** colocado en **none** (**ninguno**), y todos los elementos opcionales omitidos. Las propuestas alternativas para el mismo canal de recepción contendrán el mismo valor **sessionID** en **H2250LogicalChannelParameters**. Todas las estructuras **OpenLogicalChannel** alternativas que proponen un canal para transmisión desde el punto extremo llamado al punto extremo llamante contendrán el mismo valor **sessionID** y el mismo valor **mediaChannel**. Se colocarán los otros elementos **H2250LogicalChannelParameters** y **dataType** dentro de **reverseLogicalChannelParameters** para describir correctamente las capacidades de recepción del punto extremo llamante asociado con este canal propuesto. El punto extremo llamante puede elegir no proponer ningún canal para transmisión del punto extremo llamado al punto

extremo llamante porque desea utilizar más adelante los procedimientos H.245 para establecer esos canales.

En el mensaje Establecimiento, cada **OpenLogicalChannel** que propone un canal unidireccional para transmisión desde el punto extremo llamado al punto extremo llamante y que transporte medios utilizando RTP contendrá el elemento **mediaControlChannel** (indicando el canal RTCP que va en el mismo sentido) en el elemento **H2250LogicalChannelParameters** de la estructura **reverseLogicalChannelParameters**.

En un **OpenLogicalChannel** que proponga un canal bidireccional entre el punto extremo llamante y el punto extremo llamado, los elementos **forwardLogicalChannelParameters** y **reverseLogicalChannelParameters** contendrán parámetros que especifiquen las características del canal propuesto. Cada una de dichas estructuras **OpenLogicalChannel** tendrá un valor exclusivo de **forwardLogicalChannelNumber**. Las propuestas alternativas para el mismo canal bidireccional contendrán el mismo valor de **sessionID** en **H2250LogicalChannelParameters**. El elemento **mediaChannel** se omitirá de la propuesta; el punto extremo llamado lo proporcionará en el elemento **reverseLogicalChannelParameters** si la propuesta es aceptada. El orden de **H2250LogicalChannelParameters** y de **dataType** se fijará para describir correctamente las capacidades de transmisión del punto extremo llamante con su canal propuesto.

Todos los elementos **mediaControlChannel** insertados por el punto extremo llamante para el mismo valor de **sessionID** en ambos sentidos tendrán el mismo valor.

Al recibir un mensaje Establecimiento que contiene el elemento **fastStart**, que determina que está dispuesto a continuar el procedimiento de conexión rápida y alcanzar el punto de la conexión en el cual está preparado para iniciar la transmisión de medios, el punto extremo llamado elegirá entre las estructuras **OpenLogicalChannel** propuestas que contienen elementos **reverseLogicalChannelParameters** para cada tipo de medio que desea transmitir, y entre las estructuras **OpenLogicalChannel** propuestas que especifican **forwardLogicalChannelParameters** (y que omiten **reverseLogicalChannelParameters**) para cada tipo de medio que desea recibir, y de entre las estructuras **OpenLogicalChannel** propuestas que contienen los elementos **forwardLogicalChannelParameters** y **reverseLogicalChannelParameters** para cada canal bidireccional que desea transmitir y/o recibir. Si se presentan propuestas alternativas, se seleccionará únicamente una estructura **OpenLogicalChannel** entre cada conjunto de alternativas; las alternativas dentro de un conjunto tienen el mismo **sessionID**. Si se ofrecen varios algoritmos de criptación para un canal, el punto extremo llamado debe seleccionar uno y modificar el **OpenLogicalChannel** para suprimir los otros. El punto extremo llamado acepta un canal propuesto devolviendo la estructura **OpenLogicalChannel** correspondiente en cualquier mensaje de señalización de llamada H.225.0 enviado como respuesta al mensaje Establecimiento hasta el mensaje Conexión incluido. Un punto extremo llamado puede optar por repetir el elemento **fastStart** en todos los mensajes subsiguientes hasta el mensaje Conexión incluido: el contenido del elemento **fastStart** será el mismo. Los puntos extremos llamantes reaccionarán al primer elemento **fastStart** recibido en un mensaje de respuesta al mensaje Establecimiento e ignorarán cualesquiera elementos **fastStart** subsiguientes. El punto extremo llamado puede elegir no abrir un flujo de medios en un sentido determinado o un tipo de medios determinado no incluyendo una estructura **OpenLogicalChannel** correspondiente en el elemento **fastStart** de la respuesta de señalización de llamada H.225.0.

Al aceptar un canal para transmisión propuesto del punto extremo llamado al punto extremo llamante, el punto extremo llamado devolverá la estructura **OpenLogicalChannel** correspondiente al punto extremo llamante, insertando un solo elemento **forwardLogicalChannelNumber** en la estructura **OpenLogicalChannel** y, para canales que transportan medios utilizando RTP, un elemento **mediaControlChannel** (que indica el canal RTCP inverso) en el elemento **H2250LogicalChannelParameters** de la estructura **reverseLogicalChannelParameters**. El punto extremo llamado puede comenzar la transmisión de medios por el canal aceptado según los

parámetros especificados en el elemento **reverseLogicalChannelParameters** inmediatamente después de enviar la respuesta de señalización de llamada H.225.0 que contiene **fastStart**, a menos que el elemento **mediaWaitForConnect** estuviera colocado en VERDADERO, en cuyo caso debe esperar hasta que se envíe el mensaje Conexión.

Al aceptar un canal para transmisión propuesto del punto extremo llamante al punto extremo llamado, el punto extremo llamado devolverá la estructura **OpenLogicalChannel** correspondiente al punto extremo llamante. El punto extremo llamado insertará un **mediaChannel** válido y, para canales que transporten medios utilizando RTP, un campo **mediaControlChannel** (que indica que el canal RTCP tiene el mismo sentido) en el elemento **h2250LogicalChannelParameters** de la estructura **forwardLogicalChannelParameters**. Todos los elementos **mediaControlChannel** insertados por el punto extremo llamado para el mismo **sessionID** en ambos sentidos tendrán el mismo valor. El punto extremo llamado se preparará entonces para recibir inmediatamente el flujo de medios conforme a los parámetros especificados en **forwardLogicalChannelParameters**. El punto extremo llamante puede iniciar la transmisión de los medios por los canales aceptados y abiertos al recibir la respuesta de señalización de llamada H.225.0 que contiene **fastStart**, y puede liberar todos los recursos asignados a la recepción por los canales propuestos que no fueron aceptados.

Al aceptar un canal bidireccional propuesto para la transmisión entre el punto extremo llamante y el punto extremo llamado, el punto extremo llamado devolverá la correspondiente estructura **OpenLogicalChannel** al punto extremo llamante. Los puntos extremos llamado y llamante utilizarán el valor en el elemento **forwardLogicalChannelNumber** como el número de canal lógico de los trayectos de transmisión hacia adelante y de retorno del canal bidireccional. El punto extremo llamado insertará un elemento **mediaChannel** válido en el elemento **h2250LogicalChannelParameters** de la estructura **reverseLogicalChannelParameters**. Los puntos extremos llamante y llamado recibirán flujos de medios de acuerdo con los parámetros especificados en **forwardLogicalChannelParameters** y **reverseLogicalChannelParameters**, respectivamente. El punto extremo llamado estará preparado para aceptar una conexión en el canal bidireccional antes de devolver el elemento **fastStart**. El punto extremo llamante puede comenzarla transmisión de medios en los canales aceptados cuando recibe la respuesta de señalización de llamada H.225.0 que contiene **fastStart** y puede liberar recursos atribuidos a los canales propuestos y que no fueron aceptados.

NOTA – Sólo se permite al punto extremo llamado alterar campos de una estructura **OpenLogicalChannel** propuesta ajustándose a las especificaciones de esta cláusula. No se permite, por ejemplo, que un punto extremo altere el número de tramas por paquete ni otras características del canal propuesto que no estén declaradas específicamente en esta cláusula. Si el punto extremo llamante quisiese aumentar la probabilidad de aceptación de la Conexión Rápida, debería incluir varias propuestas con distintos parámetros alternativos. Esta regla no impide que un punto extremo incluya el **encryptionSync** en el **OpenLogicalChannel** devuelto.

8.1.7.2 Cambio a los procedimientos H.245

Después del establecimiento de una comunicación utilizando el procedimiento de conexión rápida, cada punto extremo puede determinar si es necesario invocar características de llamada que requieren la utilización de procedimientos H.245. Cualquier punto extremo puede iniciar la utilización de estos procedimientos en cualquier punto durante la llamada, utilizando la tunelización descrita en 8.2.1 (si **h245Tunnelling** permanece activa). Una entidad H.323 de la versión 4 o superior que utilice la conexión rápida en una llamada utilizará la tunelización H.245 cuando sea necesario un canal de control H.245, y siempre fijará el campo **h245Tunnelling** a VERDADERO. En 8.2.3 se describe el proceso de cambio a una conexión H.245 separada, que puede ser utilizado por entidades de la versión 3 y posteriores o por las nuevas entidades H.323 cuando se comunican con entidades de la versión 3 o anteriores con el objetivo de mantener la retrocompatibilidad.

Cuando se establece una comunicación utilizando el procedimiento de conexión rápida, ambos puntos extremos conservarán abierto el canal de señalización de llamada H.225.0 hasta que la llamada se termine o bien, por compatibilidad con puntos extremos más antiguos, hasta que se establezca una conexión H.245 separada.

Cuando los procedimientos H.245 están activos, todos los procedimientos H.245 obligatorios que normalmente se producen al iniciar una conexión H.245 se completarán antes de la iniciación de cualquier procedimiento H.245 adicional. Los canales de medios que fueron establecidos en el procedimiento de conexión rápida son "heredados" como si se hubieran abierto utilizando los procedimientos **openLogicalChannel** y **openLogicalChannelAck** H.245 normales.

Si el punto extremo llamante utiliza el procedimiento de conexión rápida para iniciar una llamada, no abrirá el canal de control H.245 utilizando la tunelización H.245 normal ni por medio de una conexión H.245 separada hasta que el punto extremo llamado devuelva **fastStart**, **fastConnectRefused**, **h245Address**, o el mensaje Conexión. Se señala que los puntos extremos H.323 más antiguos pueden abrir el canal de control H.245 incluso antes de recibir uno de esos elementos de mensaje o el mensaje, a pesar de que haya iniciado una llamada de conexión rápida. Aunque en publicaciones anteriores se insistía mucho en desaconsejar ese comportamiento, que ahora está prohibido, los puntos extremos necesitan estar al corriente de ese comportamiento anticuado. Si un punto extremo abre el canal de control H.245 antes de recibir los elementos de mensaje o el mensaje antes mencionados, supondrá que se ha terminado la conexión rápida y no enviará un elemento **fastStart**.

Ahora bien, un punto extremo puede intercambiar el mensaje **terminalCapabilitySet** y el mensaje **masterSlaveDetermination** en el mensaje Establecimiento como se describe en 8.2.4. Ese intercambio de mensajes constituye la apertura del canal de control H.245, pero no impide a ningún punto extremo aplicar la conexión rápida.

El punto extremo llamado no iniciará los procedimientos H.245 antes de devolver **fastConnectRefused**, **fastStart** o el mensaje Conexión. Un punto extremo llamado que devuelva el elemento **h245Address** en cualquier mensaje hasta el mensaje Conexión (incluido) y que todavía no haya aceptado o rechazado explícitamente la conexión rápida, devolverá también **fastStart** o **fastConnectRefused** en el mismo mensaje. Se señala que los puntos extremos más antiguos quizás no devuelvan **fastStart** o **fastConnectRefused**. Para compatibilidad hacia atrás con los puntos extremos más antiguos, los puntos extremos H.323 pueden suponer que se rechaza el procedimiento de conexión rápida si el punto de extremo llamado envía el elemento **h245Address** o abre el canal de control H.245 sin enviar simultáneamente o previamente **fastStart** o **fastConnectRefused**.

Se señala que en el caso en que se abra una conexión H.245 separada desde el punto extremo llamado hasta el punto extremo llamante que suministró su **h245Address** en el mensaje Establecimiento, se produce una condición de competencia: el punto extremo llamante puede detectar la apertura del canal de control H.245 desde el punto extremo llamado antes de recibir el elemento **fastStart**. Por este motivo, se recomienda que si un punto extremo acepta el procedimiento de conexión rápida e inicia una conexión separada para H.245, deberá introducir un retardo entre el envío del mensaje H.225.0 que contiene el elemento de **fastStart** y la iniciación de la conexión H.245 separada. Si el punto extremo llamado no introduce un retardo, el punto extremo llamante deberá estar preparado de todos modos para una posible llegada tardía del elemento **fastStart** en este escenario. Los puntos extremos más antiguos pueden suponer que se ha rechazado el procedimiento de conexión rápida si se abre el canal de control H.245 antes de recibir el elemento **fastStart**.

8.1.7.3 Terminación de una llamada

Si una llamada conectada que utiliza el procedimiento de conexión rápida continúa su compleción sin iniciar los procedimientos H.245, la llamada puede ser terminada por cualquier punto extremo enviando un mensaje Liberación Completa de señalización de llamada H.225.0. Si los procedimientos H.245 se inician durante la llamada, ésta se termina tal como se describe en 8.5.

Si no se ha establecido una conexión H.245 separada y el canal de señalización de llamada H.225.0 está terminado, se terminará también la llamada.

8.1.7.4 Tonos y anuncios dentro de banda y fuera de banda

Los tonos y los anuncios pueden ser generados localmente o bien ser pasados dentro de banda desde el punto extremo de terminación.

Cuando se completa el establecimiento de la comunicación, el punto extremo del lado de terminación decidirá si proporciona tonos dentro de banda o si se utilizarán tonos generados localmente en el lado de origen. Obsérvese que en algunos sistemas otros tipos de indicaciones pueden sustituir a los tonos y anuncios generados localmente (por ejemplo, indicaciones visuales en una pantalla). Para los objetivos de esta cláusula, se hará referencia a ellos como tonos y anuncios generados localmente. Los tonos generados localmente en el lado origen constituyen la opción por defecto. El lado de terminación puede desear proporcionar tonos y anuncios dentro de banda, por ejemplo, cuando el punto extremo de terminación es una pasarela a una red analógica. Para dar instrucciones al lado origen a fin de que no genere tonos locales, tales como señal de devolución de llamada o de ocupado, el lado de terminación abrirá el canal de medios respondiendo a la petición de conexión rápida y enviado un elemento de información indicador de progreso con el descriptor de progreso #1, *La llamada no es RDSI extremo a extremo; puede existir más información de progreso de llamada dentro de banda*, o el #8, *Existe disponible en este momento información dentro de banda o un esquema adecuado* en un mensaje de Llamada en Curso, Progreso o Aviso, o en un mensaje Conexión si no se envió un mensaje Aviso. La respuesta al mensaje de Conexión rápida se hará antes o al mismo tiempo que se envía el indicador de progreso (es decir, hasta el mismo mensaje, incluido éste, en el que se envía el indicador de progreso). El lado de terminación puede proporcionar tonos y anuncios dentro de banda (tales como señal de devolución de llamada o de ocupado) tan pronto como se haya enviado el descriptor de progreso y se haya abierto el canal de medios. Obsérvese que el indicador de progreso sólo debe figurar en un mensaje Aviso en caso de que sólo se avise al punto extremo. Si se proporciona otro tono dentro de banda, tal como ocupado o reorden, el indicador de progreso no debe figurar en un mensaje Aviso. Cuando no hay disponible un mensaje de establecimiento de comunicación adecuado, puede utilizarse un mensaje Progreso para transportar el indicador de progreso.

NOTA – Cuando un punto extremo o un controlador de acceso que interviene en la señalización de una llamada recibe un elemento de información indicador de progreso en un mensaje Llamada en Curso, no podrá retransmitir la llamada en curso si el mensaje llamada en curso ha sido ya enviado al lado de origen. En ese caso, se establecerá una correspondencia entre el elemento de información indicador de progreso del mensaje Llamada en Curso con el elemento de información indicador de progreso de un mensaje Progreso.

Si el lado de terminación no desea proporcionar tonos y anuncios desde el extremo lejano, no enviará un elemento de información indicador de progreso con el descriptor #1 o #8. Para ordenar al lado origen que se aplican avisos generados localmente, se envía el mensaje Aviso.

Al recibir un mensaje Aviso, al lado origen proporcionará tonos y anuncios generados localmente salvo que se cumplan las dos condiciones siguientes:

1) Hay disponible un canal de medios para "escucha". El elemento **fastStart** podría haber sido recibido en cualquier mensaje hasta, e incluido, el mensaje Aviso.

2) Se ha recibido un elemento de información indicador de progreso con el descriptor de progreso #1, *La llamada no es RDSI extremo a extremo; puede existir más información de progreso de llamada dentro de banda*, o el #8, *Existe disponible en este momento información dentro de banda o un esquema adecuado* se ha recibido en cualquier mensaje hasta, e incluido, el mensaje Aviso.

Al recibir un mensaje Liberación Completa que incluya un elemento de información causa, el lado origen generará un tono o proporcionará una indicación adecuada al valor de causa recibido. Por ejemplo, si se recibe el valor de la causa #17, *Usuario ocupado*, el lado origen generará un tono de ocupado o proporcionará una indicación de usuario ocupado.

Cuando se utilizan tonos y anuncios generados localmente, es facultativo que el elemento de información señal esté presente para incluir más información acerca del tipo de señal que se debe proporcionar.

8.1.8 Establecimiento de una comunicación a través de pasarelas

8.1.8.1 Establecimiento de comunicación entrante a través de pasarela

Cuando un terminal externo llama a un punto extremo de red a través de la pasarela, el establecimiento de la comunicación entre la pasarela y el punto extremo de red se produce de la misma manera que el establecimiento de comunicación de punto extremo a punto extremo. Es posible que la pasarela tenga que emitir mensajes llamada en curso al terminal externo mientras establece la comunicación en la red.

Una pasarela que no pueda encaminar directamente una llamada RCC entrante a un punto extremo H.323 deberá ser capaz de aceptar la marcación en dos etapas. En el caso de pasarelas hacia redes H.320 (también H.321, H.322 y H.310 en el modo H.321), la pasarela aceptará números SBE del terminal H.320. Opcionalmente las pasarelas para redes H.320 pueden soportar los códigos TCS-4 e IIS BAS para extraer información sobre marcación H.323 después que se haya establecido la llamada H.320. En el caso de pasarelas hacia modo nativo H.310 y redes H.324, la pasarela aceptará mensajes de **userInputIndication** H.245 provenientes del terminal H.324. En estos dos casos, el soporte de la multifrecuencia bitono (DTMF) es opcional. En el caso de pasarelas hacia terminales sólo vocales, la pasarela aceptará números DTMF del terminal sólo vocal. Estos números indicarán un número de marcación de segunda etapa para acceder al punto extremo individual en la red.

8.1.8.2 Establecimiento de comunicación saliente a través de pasarela

Cuando un punto extremo de red llama a un terminal externo a través de la pasarela, el establecimiento de la comunicación entre el punto extremo de red y la pasarela se produce de la misma manera que el establecimiento de comunicación de punto extremo a punto extremo. La pasarela recibirá **dialledDigits** o **partyNumber** (**e164Number** o **privateNumber**) de destino en el mensaje Establecimiento. A continuación utilizará esa dirección para efectuar la llamada saliente. La pasarela puede devolver mensajes llamada en curso al punto extremo de red mientras establece la comunicación saliente.

Una pasarela debe enviar un mensaje Llamada en Curso después de que reciba el mensaje Establecimiento (o después de que reciba ACF) si espera que transcurran más de cuatro segundos antes de que pueda responder con Aviso, Conexión o Liberación completa.

El elemento de información indicador de progreso se utiliza para indicar que se está produciendo el interfuncionamiento entre redes. La pasarela emitirá un elemento de información indicador de progreso dentro de los mensajes Aviso, Llamada en Curso o Conexión. Esta información también puede ser enviada en un mensaje Progreso.

El punto extremo de red enviará todas las direcciones **dialledDigits** o **partyNumber** que está llamando en el mensaje Establecimiento. Por ejemplo, una llamada de seis canales B en la RDSI requerirá seis direcciones **dialledDigits** o **partyNumber** en el mensaje Establecimiento. La pasarela responderá al mensaje Establecimiento con un mensaje Conexión o Liberación Completa, así como con los mensajes opcionales Aviso, Llamada en curso o Progreso. El fallo de la llamada RCC se notificará al punto extremo de red en el mensaje Liberación Completa. La utilización de múltiples valores de CRV y múltiples mensajes Establecimiento queda en estudio. La adición de canales en la RCC durante una comunicación queda también en estudio.

Un punto extremo de red que esté registrado en un controlador de acceso deberá pedir en el mensaje ARQ anchura de banda de llamada suficiente para la suma de todas las llamadas RCC. Si no se solicitara anchura de banda de llamada suficiente en el mensaje ARQ, se seguirán los procedimientos de 8.4.1, Cambios de anchura de banda, para obtener anchura de banda de llamada adicional.

La pasarela puede pasar a la fase B después de efectuar la primera llamada por la RCC. Se pueden efectuar nuevas llamadas para números **dialledDigits** o **partyNumber** de RCC adicionales después del intercambio de capacidad con la pasarela y el establecimiento de las comunicaciones audio con el punto extremo de RCC.

8.1.9 Establecimiento de comunicación con una MCU

En las conferencias multipunto centralizadas, todos los puntos extremos intercambian señalización de llamada con la MCU. El establecimiento de la comunicación entre un punto extremo y la MCU se produce del mismo modo que el establecimiento de comunicación de punto extremo a punto extremo de los escenarios de 8.1.1 a 8.1.5. La MCU puede ser el punto extremo llamado o el punto extremo llamante.

En una conferencia multipunto centralizada, el canal de control H.245 se abre entre los puntos extremos y el MC dentro de la MCU. Los canales de audio, vídeo y datos se abren entre los puntos extremos y el MP dentro de la MCU. En una conferencia multipunto descentralizada, el canal de control H.245 se abre entre los puntos extremos y el MC (puede haber muchos canales de control H.245 como ése, uno por cada llamada). Los canales de audio y vídeo deben ser de multidifusión con todos los puntos extremos de la conferencia. El canal de datos se abrirá con el MP de datos.

En una conferencia multipunto ad hoc en la que los puntos extremos no contengan un MC y el controlador de acceso desease proporcionar un servicio multipunto ad hoc para los puntos extremos, el canal de control H.245 será encaminado a través del controlador de acceso. Inicialmente, el canal de control H.245 puede ser encaminado entre los puntos extremos a través del controlador de acceso. Cuando la conferencia pase a ser multipunto, el controlador de acceso puede conectar los puntos extremos a MC asociado con el controlador de acceso.

En una conferencia multipunto ad hoc en la que uno o ambos puntos extremos contienen un MC, se utilizan los procedimientos de establecimiento de comunicación normal definidos en 8.1.1 a 8.1.5. Estos procedimientos pueden aplicarse aun si un punto extremo que contiene un MC es realmente un MCU. El procedimiento de determinación principal-subordinado se utiliza para determinar qué MC será el MC activo en la conferencia.

8.1.10 Reenvío de llamada

Un punto extremo que desea reenviar una llamada a otro punto extremo puede utilizar un mensaje facilidad indicando la dirección de transporte del nuevo punto extremo. El punto extremo receptor de esa indicación de facilidad debe enviar un mensaje Liberación Completa y recomenzar después los procedimientos de la fase A con el nuevo punto extremo.

8.1.11 Establecimiento de comunicación de difusión

El establecimiento de comunicación para conferencias de difusión y de panel de difusión con bajo grado de control seguirá los procedimientos definidos en la Rec. UIT-T H.332.

8.1.12 Envío superpuesto

Las entidades H.323 pueden opcionalmente soportar envío superpuesto. Si existe un controlador de acceso, y se utiliza envío superpuesto, los puntos extremos deben enviar un mensaje ARQ al controlador de acceso cada vez que se introduce alguna nueva información de direccionamiento. El punto extremo colocará la información de direccionamiento acumulativa total en el campo **destinationInfo** cada vez que se envía un mensaje ARQ. Si existe información de direccionamiento insuficiente en el ARQ, el controlador de acceso debe responder con un ARJ con el **motivo** puesto a **incompleteAddress** (**dirección incompleta**). Esto indica que el punto extremo debe enviar otro ARQ cuando haya disponible más información de direccionamiento. Cuando un controlador de acceso tiene suficiente información de direccionamiento para asignar una **destCallSignalAddress** (**dirección de señal de llamada de destino**) adecuada, retornará una ACF. Obsérvese que esto no necesariamente significa que la información de dirección está completa. Si el controlador de acceso envía un ARJ con **AdmissionRejectReason** puesto a otra cosa que **incompleteAddress**, se abortará el proceso de establecimiento de comunicación.

Cuando un punto extremo tiene una **destCallSignalAddress** adecuada, enviará un mensaje Establecimiento con el campo **canOverlapSend** (**envío superpuesto posible**) asignado según sea o no capaz de soportar los procedimientos de envío superpuesto. Si una entidad distante recibe un mensaje Establecimiento con una dirección incompleta y el campo **canOverlapSend** puesto a VERDADERO, debe iniciar los procedimientos de envío superpuesto retornando el mensaje Acuse de Establecimiento. La información de direccionamiento adicional debe enviarse utilizando mensajes de información. Si la dirección está incompleta y el campo **canOverlapSend** puesto a FALSO, la entidad distante debe enviar Liberación Completa. Obsérvese que las pasarelas no deben transferir mensajes Acuse de Establecimiento de la RCC a puntos extremos H.323 que no han indicado que pueden soportar procedimientos de envío superpuesto cuando no puede obtenerse el resultado deseado.

8.1.13 Establecimiento de comunicación a alias de conferencia

Pueden utilizarse direcciones alias (véase 7.1.3) para representar una conferencia en un MC. Se aplican los procedimientos de las subcláusulas precedentes, con las excepciones aquí indicadas.

8.1.13.1 Incorporación a un alias de conferencia, sin controlador de acceso

El punto extremo 1 (punto extremo llamante) envía el mensaje Establecimiento (1) (véase la figura 29) al identificador de TSAP de canal de señalización de llamada conocido del punto extremo 2 (el MC). El mensaje Establecimiento incluye los campos siguientes:

```
destinationAddress          = conferenceAlias
destCallSignalAddress       = MC(U) transport address
conferenceID                = 0 (since the CID is unknown)
conferenceGoal              = join
```

El punto extremo 2 responde con el mensaje Conexión (4), que contiene:

```
h245Address                 = Transport Address for H.245 signalling
conferenceID                = CID for the conference
```

8.1.13.2 Incorporación a un alias de la conferencia, con controlador de acceso

El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) (véase la figura 30) con el controlador de acceso. El ARQ contiene:

```
destinationInfo             = conferenceAlias
callIdentifier              = some value N
conferenceID                = 0 (since the CID is unknown)
```

El controlador de acceso retornará la dirección de transporte del canal de señalización de llamada del punto extremo 2 (denominado punto extremo, que contiene el MC) en la ACF. El punto extremo 1 envía entonces el mensaje Establecimiento (3) al punto extremo 2 utilizando esa dirección de transporte y los campos siguientes:

```
destinationAddress          = conferenceAlias
destCallSignalAddress       = address supplied by ACF
conferenceID                = 0
conferenceGoal              = join
```

Por último, el punto extremo 2 retorna un mensaje Conexión con los campos siguientes:

```
h245Address                 = Transport Address for H.245 signalling
conferenceID                = CID for the conference
```

El punto extremo 1 completa la llamada informando a su controlador de acceso del CID correcto. El punto extremo 1 envía un IRR al controlador de acceso con los campos siguientes:

```
callIdentifier              = same value N as used in the first ARQ
conferenceID                = original CID from endpoint 1
substituteConferenceIDs     = CID from endpoint 2
```

8.1.13.3 Creación o invitación con un alias de conferencia

El punto extremo 1 (punto extremo llamante) puede enviar un mensaje Establecimiento al punto extremo 2. El mensaje Establecimiento incluye los campos siguientes:

```
destinationAddress          = conferenceAlias
destCallSignalAddress       = MC(U) transport address
conferenceID                = CID of the conference
conferenceGoal              = create or invite
```

El punto extremo 2 responde con el mensaje Conexión, que contiene:

```
h245Address                 = Transport Address for H.245 signalling
conferenceID                = CID for the conference
```

8.1.13.4 Consideración sobre los puntos extremos de la versión 1

Cuando una entidad H.323 (punto extremo o MCU) recibe un mensaje Establecimiento de una entidad de la versión 1 y la **destinationAddress** (**dirección de destino**) concuerda con uno de sus alias de conferencia, ignorará entonces el **conferenceGoal** y tratará la petición establecimiento como una petición de incorporación.

Cuando un controlador de acceso recibe un ARQ de una entidad de la versión 1 y la **destinationInfo** concuerda con uno de sus alias de conferencia, ignorará entonces el campo **conferenceID** (**ID de la conferencia**). Análogamente, cuando una entidad H.323 recibe un mensaje Establecimiento de una entidad de la versión 1 y la **destinationAddress** concuerda con uno de sus alias de conferencia, ignorará entonces el **conferenceID**.

Estas disposiciones permiten a un punto extremo de la versión 1 llamar a un alias de conferencia.

8.1.14 Modificación de las direcciones de destino en el controlador de acceso

Un punto extremo fijará el campo **canMapAlias** (**posibilidad de correspondencia de alias**) al valor VERDADERO para indicar que puede aceptar información de destino modificada procedente de un controlador de acceso. El punto extremo utilizará la información de destino devuelta en los mensajes ACF o LCF en lugar de la información de destino que se pasa en ARQ o LRQ. En una pasarela de entrada, la información de destino que aparece en la ACF se utilizará en el mensaje Establecimiento que se envía a la red de paquetes. En una pasarela de salida, la información de destino que aparece en la ACF se utilizará para direccionar un destino en la RTGC (por ejemplo, la que figura en el mensaje Establecimiento enviado a la RDSI).

En casos de encaminamiento por el controlador de acceso, éste puede modificar las direcciones de destino del mensaje Establecimiento que recibe antes de enviar el correspondiente mensaje Establecimiento.

NOTA – En los sistemas H.323 anteriores a la versión 4 no era necesario fijar el campo **canMapAlias** a VERDADERO.

8.1.15 Indicación de los protocolos deseados

Cuando un punto extremo realiza una llamada, puede indicar en varios mensajes H.225.0 los protocolos que desea utilizar en dicha llamada, tales como facsímil, H.320, T.120, etc., utilizando el campo **desiredProtocols**. Si el punto extremo proporciona a su controlador de acceso una lista con los protocolos que desea, o si una entidad envía un mensaje LRQ a un controlador de acceso con una lista de los protocolos deseados, el controlador de acceso debería intentar localizar un punto extremo que soporte dichos protocolos deseados. Si el controlador de acceso no encuentra punto extremo alguno que soporte cualquiera de los protocolos deseados, el controlador de acceso resolverá la dirección para que la llamada pueda continuar.

El punto extremo llamante puede examinar el **EndpointType** (**tipo de punto extremo**) del punto extremo de destino para determinar exactamente los protocolos que puede manejar el punto extremo distante.

8.1.16 Tonos y anuncios solicitados por el controlador de acceso

Un controlador de acceso puede solicitar a una pasarela que reproduzca un tono o un anuncio si ocurren una serie de eventos de llamada. Estos eventos de llamada pueden ser eventos "previos a la llamada" (algo que ocurre antes de que la pasarela de terminación sea señalizada, como por ejemplo, solicitar al llamante un número de destino o un código de cuenta), eventos que ocurren "en plena llamada " (algo que ocurre a mitad de una llamada, como por ejemplo, proporcionar un anuncio que avise a las partes de la llamada que ésta terminará en unos pocos minutos) o eventos de "final de llamada " (algo que ocurre al final de una llamada, como por ejemplo, un mensaje de despedida). En todos los casos, el controlador de acceso puede utilizar el **descriptor de señales H248** (**H248SignalsDescriptor**) para describir la forma de sugerencia o requerimiento que debería utilizar la pasarela.

Se soportan los eventos previos a la llamada siguientes:

- Requerimiento de un destino – En lo que a menudo se denomina marcación en dos etapas, el llamador marca un número para alcanzar la pasarela y entonces se le requiere que marque el número del destino verdadero. Aunque una pasarela puede tener una política general para realizar siempre dicho requerimiento, en algunas circunstancias puede tener sentido permitir que la pasarela consulte al controlador de acceso. Esta operación de "consulta" es simplemente una ARQ en la que el número llamado es la **destinationInfo**. Si el controlador de acceso decide que es necesario el número de destino verdadero, puede ordenar a la pasarela que se dirija al llamante, recopile los dígitos adicionales y consulte al controlador de acceso sobre el destino. El controlador de acceso utiliza el ARJ con un elemento **serviceControl** (**control de servicio**) y **AdmissionRejectReason** (**razón de rechazo de admisión**) de **collectDestination** (**recopilación de destino**). El elemento **serviceControl** tiene un **ServiceControlDescriptor** del tipo **signal** (**señal**) (que contiene el **H248SignalsDescriptor**) y cuyo **reason** (**motivo**) sea **open** (**abierta**). La **AdmissionRejectReason** de **collectDestination** ordena a la pasarela que sitúe el destino verdadero que ha recopilado en el **destinationInfo** de una nueva ARQ.
- Requerimiento de un código de autorización, código de cuenta o PIN – En este caso, el controlador de acceso responde a la ARQ con un ARJ que contiene un elemento **serviceControl** y una **AdmissionRejectReason** que es **collectPIN** (**recopilar PIN**). El elemento **serviceControl** tiene un **ServiceControlDescriptor** del tipo **signal** (que contiene el **H248SignalsDescriptor**) y su **reason** es **open**. La **AdmissionRejectReason** de **collectPIN** ordena a la pasarela que coloque el PIN recopilado (o código de autorización o código de cuenta) en un testigo o **cryptoToken** (**testigo de criptación**) de una nueva ARQ.
- Requerimiento de un destino y de un PIN – Se trata de la aplicación en serie de los dos casos anteriores.
- Rechazo de una llamada – Un controlador de acceso puede rechazar una llamada, pero debe proporcionar alguna realimentación al usuario (por ejemplo, proporcionando un anuncio o tono de red ocupado en caso de que no existieran facilidades disponibles para un destino). En este caso, el ARJ debe contener una **AdmissionRejectReason** que refleje dicha situación, pero no **collectPIN** o **collectDestination**.

Un controlador de acceso puede iniciar una señal a mitad de la llamada utilizando el mensaje SCI. El elemento **serviceControl** tiene un **ServiceControlDescriptor** del tipo **signal** (que contiene el **H248SignalsDescriptor** de H.248) y cuya **reason** sea **open**. La señal puede detenerse enviando el mensaje **ServiceControlIndication**, pero con un **ServiceControlDescriptor** cuya **reason** sea **close**. Una pasarela debería responder al mensaje SCI con un SCR con el **result** adecuado.

Un controlador de acceso puede iniciar una señal al final de la llamada en un mensaje DRQ (para el caso de encaminamiento de punto extremo) o en un mensaje Liberación Completa (para el caso de encaminamiento por el controlador de acceso) con un elemento **serviceControl**. El elemento **serviceControl** tiene un **ServiceControlDescriptor** del tipo **signal** (que contiene el **H248SignalsDescriptor** de H.248) y cuya **reason** es **open**. La señal puede detenerse enviando el mensaje **ServiceControlIndication**, pero con un **ServiceControlDescriptor** cuya **reason** sea **close**.

8.2 Fase B – Comunicación inicial e intercambio de capacidad

Una vez que ambos lados han intercambiado los mensajes de establecimiento de comunicación de la fase A, los puntos extremos, si proyectan emplear H.245, establecerán el canal de control H.245. Se utilizan los procedimientos de la Rec. UIT-T H.245 en el canal de control H.245 para el intercambio de capacidad y la apertura de canales de medios.

NOTA – Opcionalmente, el canal de control H.245 puede ser establecido por el punto extremo llamado al recibir el mensaje Establecimiento, y por el punto extremo llamante al recibir Aviso o Llamada en Curso. En el caso de que no llegue un mensaje Conexión, o un punto extremo envíe Liberación Completa, el canal de control H.245 será cerrado.

Los puntos extremos soportarán el procedimiento de intercambio de capacidades H.245, como se describe en 6.2.8.1.

Las capacidades de los sistemas de punto extremo se intercambian mediante la transmisión del mensaje **terminalCapabilitySet** H.245. Este mensaje de capacidad será el primer mensaje H.245 enviado a menos que el punto extremo indique que comprende el campo **parallelH245Control** (véase 8.2.4). Si antes de la terminación satisfactoria de intercambio de capacidad terminal, cualquier otro procedimiento presenta un fallo (es decir, rechazado, no comprendido, no soportado) el punto extremo de origen se ha de iniciar y completar satisfactoriamente el intercambio de capacidad terminal antes de intentar cualquier otro procedimiento. Un punto extremo que recibe un mensaje **terminalCapabilitySet** de una entidad par antes de iniciar el intercambio de capacidades responderá conforme a lo requerido en 6.2.8.1, e iniciará y completará satisfactoriamente el intercambio de capacidades con esa entidad par antes de iniciar cualquier otro procedimiento.

Los puntos extremos soportarán el procedimiento de determinación principal-subordinado de H.245, como se describe en 6.2.8.4. En los casos en que ambos puntos extremos de una llamada tengan capacidad MC, la determinación principal-subordinado se utilizará para determinar qué MC será el MC activo de la conferencia. El MC activo puede enviar entonces el mensaje **mcLocationIndication**. El procedimiento permite también la determinación principal-subordinado para la apertura de canales bidireccionales de datos.

La determinación principal-subordinado avanzará (enviando **MasterSlaveDetermination** o bien **MasterSlaveDeterminationAck**, según corresponda) en el primer mensaje H.245 después que se haya iniciado el intercambio de capacidad terminal.

Si el intercambio de capacidad inicial o los procedimientos de determinación principal-subordinado fallan, deberían intentarse al menos otras dos veces antes de que el punto extremo abandone el intento de conexión y pase a la fase E.

Tras la compleción satisfactoria de los requisitos de la fase B, los puntos extremos pasarán directamente al modo de funcionamiento deseado, normalmente a la fase C.

8.2.1 Encapsulado de mensajes H.245 dentro de mensajes de señalización de llamada H.225.0

Para conservar recursos, sincronizar la señalización y control de llamada y reducir el tiempo de establecimiento de la comunicación, puede ser conveniente transmitir mensajes H.245 dentro de mensajes de señalización de llamada H.225.0 dentro del canal de señalización de llamada en vez de establecer un canal H.245 separado. Este proceso, conocido como "encapsulado" o "tunelización" de mensajes H.245, se efectúa utilizando el elemento **h245Control** de **h323-uu-pdu** por el canal de señalización de llamada, copiando un mensaje H.245 codificado como una cadena de octetos.

Cuando la tunelización está activa, pueden encapsularse uno o más mensajes H.245 en cualquier mensaje de señalización de llamada H.225.0. Si se está utilizando la tunelización y no es necesaria la transmisión de un mensaje de señalización de llamada H.225.0 en el instante en que debe transmitirse un mensaje H.245, se enviará entonces un mensaje facilidad con **reason** colocado en **transportedInformation** (**información transportada**). (Se señala que los sistemas anteriores a la versión 4 utilizaban un mensaje facilidad con el **h323-message-body** (**cuerpo de mensaje h323**) colocado en **empty** (**vacío**).)

Una entidad llamante que puede y está dispuesta a utilizar el encapsulado H.245 dará el valor VERDADERO al elemento **h245Tunnelling** en el mensaje Establecimiento y en todos los mensajes subsiguientes de señalización de llamada H.225.0 que envía mientras desea mantener activa la tunelización. Una entidad llamada que puede y está dispuesta a utilizar el encapsulado H.245 colocará el elemento **h245Tunnelling** en VERDADERO en el primer mensaje enviado de señalización de llamada H.225.0 en respuesta al mensaje Establecimiento y en cada mensaje subsiguiente de señalización de llamada H.225.0 que envía mientras desea mantener activa la tunelización. La entidad llamada no dará el valor VERDADERO al elemento **H245Tunnelling** en ninguna respuesta de señalización de llamada H.225.0 (y la tunelización sigue estando desactivada) a menos que fuera VERDADERO en el mensaje Establecimiento al que está respondiendo. Si la entidad llamada no conoce aún si se soporta la tunelización H.245, incluirá la bandera **provisionalRespToh245Tunnelling** (**respuesta provisional a tunelización H245**). Esto puede ocurrir, por ejemplo, cuando un controlador de acceso responda a una entidad llamante con un mensaje llamada en curso antes de que el punto extremo llamado responda a la bandera **h245Tunnelling**. La bandera **provisionalRespToH245Tunnelling** elimina efectivamente el significado de la bandera **h245Tunnelling** en un mensaje, siendo la bandera ignorada por el punto extremo de recepción.

Si **h245Tunnelling** no se coloca en VERDADERO en ningún mensaje de señalización de llamada H.225.0, que no incluya la bandera **provisionalRespToH245Tunnelling** la tunelización está desactivada desde ese punto mientras dura la llamada y se establecerá una conexión H.245 separada cuando y si se invocan los procedimientos H.245.

La entidad llamante puede incluir mensajes H.245 tunelizados en el mensaje Establecimiento; el elemento **h245Tunnelling** debe colocarse también en VERDADERO. Si la entidad llamada no coloca el elemento **h245Tunnelling** en VERDADERO y está ausente la bandera **provisionalRespToH245Tunnelling** del primer mensaje enviado de señalización de llamada H.225.0 como respuesta a establecimiento, la entidad llamante supondrá que los mensajes H.245 que había encapsulado en establecimiento fueron ignorados por la entidad llamada y los repetirá, en caso necesario, después que se establezca el canal H.245 separado. El punto extremo llamado, si coloca el elemento **h245Tunnelling** en VERDADERO, puede incluir también los mensajes H.245 encapsulados en el primer mensaje de señalización de llamada H.225.0 y en los mensajes subsiguientes.

El punto extremo llamante no incluirá el elemento **fastStart** ni los mensajes H.245 encapsulados en **h245Control** en el mismo mensaje Establecimiento, dado que la presencia de los mensajes H.245 encapsulados podría no tener en cuenta el procedimiento de conexión rápida. No obstante, un punto extremo llamante puede incluir un elemento **fastStart** y colocar el elemento **h245Tunnelling** en VERDADERO dentro del mismo mensaje Establecimiento; del mismo modo, un punto extremo llamado puede incluir **fastStart** y colocar **h245Tunnelling** en VERDADERO dentro de la misma respuesta de señalización de llamada H.225.0. En este caso, se siguen los procedimientos de conexión rápida y la conexión H.245 permanece "no establecida" hasta la transmisión real del primer mensaje H.245 tunelizado o hasta la apertura de la conexión H.245 separada.

Cuando se está utilizando el encapsulado H.245, ambos puntos extremos conservarán abierto el canal de señalización de llamada H.225.0 hasta que se termine la llamada o bien hasta que se establezca una conexión H.245 separada.

Cuando un punto extremo recibe un elemento **h245control** que encapsula más de una PDU H.245, las PDU H.245 encapsuladas serán tratadas (es decir, establecidas en capas superiores) secuencialmente por orden de desplazamiento creciente desde el comienzo del mensaje H.225.0.

Las entidades de la versión 4 y superiores H.323 indicarán soporte de la tunelización H.245 como se describe en está cláusula colocando el campo **h245Tunnelling** en VERDADERO en todos los mensajes que contengan ese campo.

8.2.2 Tunelización a través de entidades de señalización intermedias

Ciertas entidades del trayecto de señalización como, por ejemplo, los controladores de acceso, pueden desempeñar funciones tales como desvío en caso de no respuesta u otro control de llamada especializado que da lugar a representar ante un punto extremo una situación de llamada que es distinta de la situación de la llamada real en el otro punto extremo. Estas entidades intermedias garantizarán que los mensajes H.245 encapsulados en mensajes de señalización de llamada H.225.0 se dirijan a otro punto extremo incluso si el mensaje de señalización de llamada H.225.0 en el cual se encapsuló el mensaje H.245 estuviera consumido y no se hubiera enviado al otro punto extremo. Esto se efectúa mediante la transferencia del mensaje H.245 encapsulado en un mensaje facilidad con el **reason** colocado en **transportedInformation**. (Se señala que los sistemas anteriores a la versión 4 utilizaban un mensaje Facilidad con el **h323-message-body** puesto en **empty**.) Por ejemplo, si un controlador de acceso ya ha enviado un mensaje Conexión a un punto extremo llamante y recibe más tarde un mensaje Conexión de un punto extremo llamado que contiene un mensaje H.245 encapsulado, debe enviar el mensaje H.245 utilizando un mensaje facilidad.

Determinadas entidades del trayecto de señalización también utilizarán el mensaje Facilidad o el mensaje Progreso para transportar cualquier nueva información (tal como elementos de información Q.931, campos de los elementos de información UU llamada en curso, protocolos H.323 no tunelizados y mensajes H.245 encapsulados) que se reciban en un mensaje Llamada en Curso dirigido al otro punto extremo, en caso de que la entidad ya haya enviado un mensaje Llamada en Curso. Ello permitirá que la entidad transmita, por ejemplo, el elemento **fastStart** para facilitar el correcto establecimiento de una comunicación con comienzo rápido y/o un indicador de progreso para indicar la presencia de tonos y anuncios dentro de banda. Cuando se utiliza el mensaje Facilidad para transportar dicha información extraída del mensaje llamada en curso, el **motivo** de facilidad toma el valor **forwardedElements** (**elementos enviados**).

8.2.3 Cambio a una conexión H.245 separada

Cuando se está utilizando el encapsulado H.245 o el procedimiento de conexión rápida, cualquier punto extremo puede elegir efectuar un cambio utilizando la conexión H.245 separada en cualquier momento. Para facilitar la iniciación de la conexión H.245 separada por cualquier punto extremo, cualquiera de los puntos extremos, cada uno de ellos puede incluir **h245Address** en cualquier mensaje de señalización de llamada H.225.0 que envía durante la llamada. Si en el momento en que un punto extremo considera necesario iniciar la conexión H.245 separada, descubre que todavía no ha recibido el elemento **h245Address** del otro punto extremo, el punto extremo transmitirá un mensaje facilidad cuyo **FacilityReason** (**motivo de facilidad**) es **startH245** y proporcionará su dirección H.245 en el elemento **h245Address**. Un punto extremo que recibe un mensaje Facilidad cuyo **facilityReason** sea **startH245** y que no ha iniciado ya independientemente el canal H.245 separado, abrirá el canal H.245 utilizando la **h245Address** especificada. La utilización de la conexión H.245 separada es iniciada abriendo la conexión TCP H.245, y aceptada mediante acuse de recibo de la conexión TCP H.245.

Si se estaba utilizando tunelización, el punto extremo que inicia la conexión H.245 separada no enviará ningún otro mensaje H.245 tunelizado por el canal de señalización de llamada, ni enviará ningún mensaje H.245 por la conexión H.245 separada hasta que se acuse recibo del establecimiento de la conexión TCP. El punto extremo que acusa recibo de la apertura de la conexión H.245 separada no enviará ningún otro mensaje H.245 tunelizado por el canal de señalización de llamada después del acuse recibo de la apertura de la conexión H.245 separada. Como cabe la posibilidad de que los mensajes H.245 ya se hayan enviado y estén en tránsito cuando se inicia el canal H.245 separado, los puntos extremos seguirán recibiendo y procesando correctamente los mensajes H.245 tunelizados hasta que se reciba un mensaje de señalización de llamada H.225.0 con la bandera **h245Tunnelling** colocada en FALSO; las respuestas a esos mensajes H.245 tunelizados "tardíos" o el acuse de recibo de los mismos se enviarán por la

conexión H.245 separada después de que se establezca. Una vez establecida dicha conexión, no es posible volver atrás y utilizar la tunelización.

Cuando ambos puntos extremos inician simultáneamente la conexión H.245 separada, el punto extremo con el elemento **h245Address** numéricamente más pequeño cerrará la conexión TCP que abrió y utilizará la conexión abierta por el otro punto extremo. A fin de comparar los valores numéricos de **h245Address**, cada octeto de la dirección será comparado individualmente empezando por el primer octeto de la CADENA DE OCTETOS y siguiendo por la CADENA DE OCTETOS de izquierda a derecha hasta que se hallen valores de octetos numéricos desiguales. La comparación se efectúa primero por el elemento de la dirección de capa de red **h245Address**, y luego, si se halla que es igual, por el elemento dirección de transporte (puerto).

8.2.4 Iniciación de la tunelización H.245 en paralelo con conexión rápida

Tal como se muestra con detalle en 8.2, los primeros dos mensajes H.245 que envía un punto extremo en el canal de control H.245 son el mensaje **terminalCapabilitySet** y los mensajes **masterSlaveDetermination**. Incluso cuando se utiliza la conexión rápida resulta ventajoso intercambiar estos mensajes tan rápidamente como sea posible. En particular, una entidad puede necesitar conocer cuanto antes si la otra entidad soporta DTMF en **UserInputIndication** o con tipos de cabida útil RTP (descritos en 10.5). Además, si se rechaza la conexión rápida, resultan obvias las ventajas de haber transmitido estos mensajes, ya que es necesario intercambiar menos mensajes para la apertura de canales lógicos.

Por lo tanto, para acelerar el intercambio de capacidades y el establecimiento de la comunicación en general, una entidad puede incluir el mensaje H.245 **terminalCapabilitySet** y los mensajes **masterSlaveDetermination** en el mensaje Establecimiento, incluyendo estos mensajes en el campo **control H245 en paralelo** (**parallelH245Control**) del mensaje Establecimiento. A diferencia del campo **h245Control**, la entidad llamante puede enviar estos mensajes en el mensaje Establecimiento junto con el elemento **fastStart**. La entidad llamante fijará el campo **h245Tunnelling** a VERDADERO cuando se incluya el campo **parallelH245Control**.

NOTA – Una entidad llamante no debería incluir el campo **parallelH245Control** sin incluir también el campo **fastStart**, puesto que la tunelización H.245 en el contexto de una llamada que no utiliza los procedimientos de conexión rápida debería ser manejada conforme a lo indicado en 8.2.1.

Para indicar que la entidad llamada entiende el campo **parallelH245Control**, el primer mensaje H.245 que la entidad llamada envía será el mensaje **terminalCapabilitySetAck** tunelizado en el canal de señalización de llamada H.225.0. La entidad llamada debería enviar este mensaje de respuesta al mismo tiempo que se envía **fastConnectRefused** o **fastStart** a la entidad llamante. Se señala que si un punto extremo no indica que entiende el campo **parallelH245Control**, deberá cumplir lo indicado en 8.2 y enviar **terminalCapabilitySet** y no **terminalCapabilitySetAck** como primer mensaje H.245. La entidad llamada fijará el campo **h245Tunnelling** a VERDADERO si entiende el campo **parallelH245Control**. En la figura 41 se muestra el intercambio de mensajes de una llamada con conexión rápida entre dos puntos extremos que han entendido el campo **parallelH245Control**.

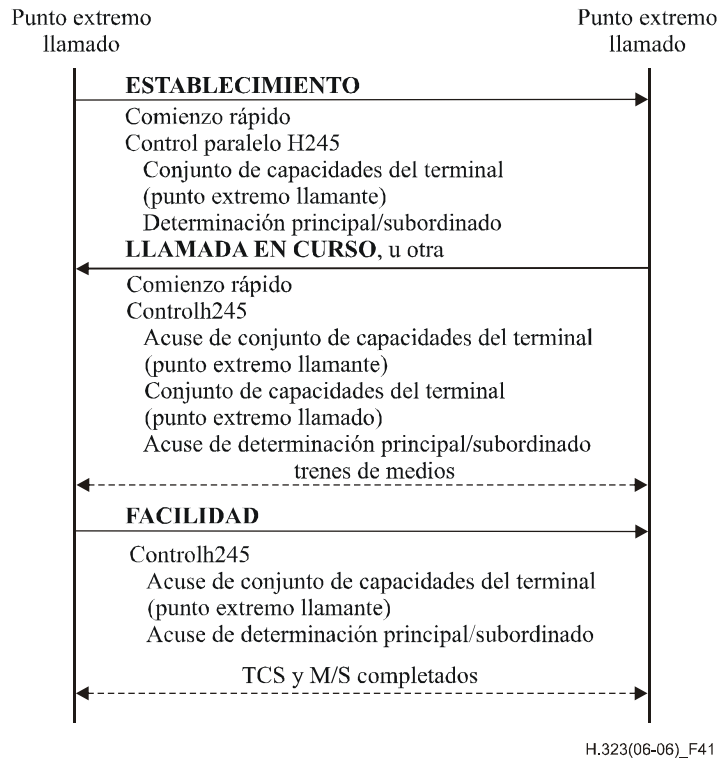


Figura 41/H.323 – Iniciación H.245 en paralelo con conexión rápida exitoso

La entidad llamante detectará que el campo **parallelH245Control** no ha sido entendido cuando reciba un mensaje Conexión y aún no haya recibido una respuesta al mensaje **terminalCapabilitySet** inicial, el primer mensaje H.245 recibido de la entidad llamada no sea un mensaje **terminalCapabilitySetAck** tunelizado, o bien cuando recibe **fastStart** o **fastConnectRefused** y aún no haya recibido respuesta al mensaje **terminalCapabilitySet**. La figura 42 muestra un intercambio de mensajes entre un punto extremo que envía el campo **parallelH245Control** y un punto extremo llamado que no entiende el campo.

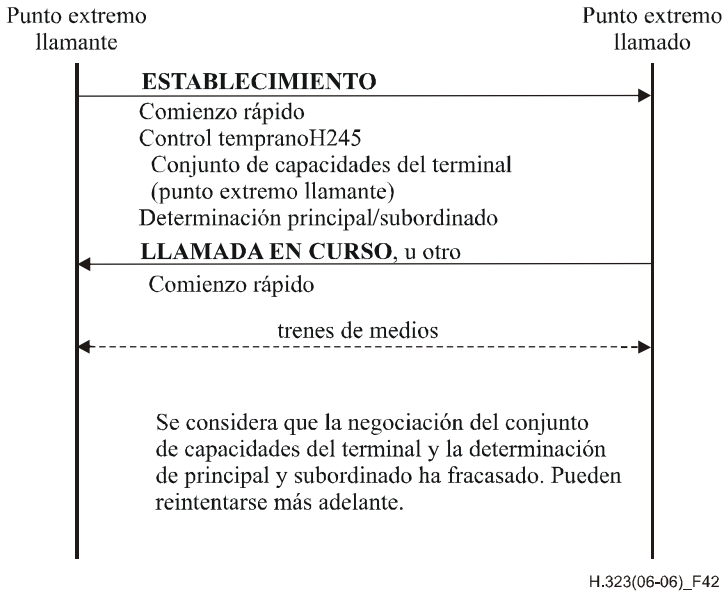


Figura 42/H.323 – Iniciación H.245 en paralelo con conexión rápida sin éxito

8.3 Fase C – Establecimiento de comunicación audiovisual

Después del intercambio de capacidades y la determinación de principal-subordinado, se utilizarán los procedimientos de la Rec. UIT-T H.245 para abrir canales lógicos para los diversos trenes de información. Los trenes de audio y vídeo, que se transmiten por los canales lógicos establecidos en H.245, se transportan en identificadores TSAP dinámicos utilizando un protocolo no fiable (véase la Rec. UIT-T H.225.0). Las comunicaciones de datos, que se transmiten por los canales lógicos establecidos en H.245, se transportan utilizando un protocolo fiable (véase la Rec. UIT-T H.225.0).

El mensaje **openLogicalChannelAck** devuelve, o los parámetros **reverseLogicalChannelParameters** de la petición **openLogicalChannel** contienen, la dirección de transporte que el punto extremo receptor ha asignado a ese canal lógico. El canal transmisor deberá enviar a continuación el tren de información asociado con el canal lógico a esa dirección de transporte.

Después de la apertura de canales lógicos para audio y vídeo, el transmisor enviará un mensaje **h2250MaximumSkewIndication** para cada par de audio y vídeo asociado.

8.3.1 Cambios de modo

Durante una sesión, los procedimientos de cambio de estructura de canal, capacidad, modo de recepción, etc., se llevarán a cabo tal como se define en la Rec. UIT-T H.245. El apéndice V/H.245 contiene un procedimiento para cambiar modos en un canal lógico que pueden minimizar la interrupción del audio.

8.3.2 Intercambio de vídeo por mutuo acuerdo

La **videoIndicateReadyToActivate** (**indicación de vídeo preparado para activación**) se define en la Rec. UIT-T H.245. Su empleo es opcional, pero cuando se utilice, deberá seguirse el siguiente procedimiento.

Se fija el punto extremo 1 de tal manera que no se transmita vídeo a menos que, y hasta que, el punto extremo 2 indique también que está preparado para transmitir vídeo. El punto extremo 1 enviará la indicación **videoIndicateReadyToActivate** cuando se haya completado el intercambio de capacidad inicial, pero no transmitirá una señal de vídeo hasta que haya recibido **videoIndicateReadyToActivate** o vídeo entrante procedente del punto extremo 2.

Un punto extremo que no haya sido fijado de esta manera opcional no está obligado a esperar hasta la recepción de **videoIndicateReadyToActivate** o vídeo antes de iniciar su transmisión de vídeo.

8.3.3 Distribución de direcciones de tren de medios

En unidifusión, el punto extremo abrirá canales lógicos a la MCU o a otro punto extremo. Las direcciones se pasan en **openLogicalChannel** y **openLogicalChannelAck**.

En multidifusión, las direcciones multidifundidas son asignadas por el MC y distribuidas a los puntos extremos en la **communicationModeCommand** (**instrucción de modo de comunicación**). Es responsabilidad del MC atribuir y asignar direcciones de multidifusión únicas. El punto extremo señalizará un **openLogicalChannel** al MC con la dirección multidifusión asignada. El MC enviará **openLogicalChannel** a cada punto extremo receptor. En los casos en los que medios procedentes de múltiples puntos extremos son transmitidos en una única sesión (por ejemplo, dirección multidifusión simple), el MC abrirá un canal lógico con cada punto extremo que reciba medios de un punto extremo en la conferencia.

En los casos en los que un punto extremo se incorpora a una conferencia después de que se ha transmitido la **communicationModeCommand** inicial, es responsabilidad del MC enviar una **communicationModeCommand** actualizada al nuevo punto extremo y abrir los canales lógicos apropiados para medios originarios del nuevo punto extremo. En los casos en los que los puntos extremos abandonan la conferencia después de que se ha transmitido la

communicationModeCommand, es responsabilidad del MC cerrar los canales lógicos apropiados para medios originarios del nuevo punto.

En multiunidifusión, el punto extremo debe abrir canales lógicos a cada uno de los otros puntos extremos. Se envía **openLogicalChannel** al MC y contendrá el número de terminal del punto extremo para el cual está destinado el canal. El punto extremo puede comparar **openLogicalChannelAck** mediante el **forwardLogicalChannelNumber** (**número de canal lógico directo**).

8.3.4 Correlación de trenes de medios en conferencias multipunto

El siguiente método se utilizará para asociar un canal lógico con un tren RTP dentro de una conferencia multipunto. El punto extremo de origen del tren de medios envía el mensaje **openLogicalChannel** al MC. En los casos en que el origen desearía indicar un destino para el **openLogicalChannel**, el punto extremo del origen debe colocar la **terminalLabel** (**etiqueta de terminal**) del punto extremo de destino en el campo **destination** (**destino**) de los **h2250LogicalChannelParameters**. El punto extremo de origen debe también colocar su propia **terminalLabel** en el campo **source** (**fuente**) de **h2250LogicalChannelParameters**. Téngase en cuenta que en el modelo multidifusión, la ausencia de un **destination** indica que el tren es aplicable a todos los puntos extremos.

Si a un punto extremo de origen le ha sido asignada una **terminalLabel** por un MC, el punto extremo de origen utilizará un SSRC que contenga el octeto más bajo de su **terminalLabel** como el octeto más bajo de su SSRC.

En el punto extremo de destino se puede asociar el número de canal lógico con el origen del tren RTP comparando el campo **openLogicalChannel.h2250LogicalChannelParameters.source** con el octeto más bajo del SSRC en el encabezamiento RTP.

Es posible para las colisiones del SSRC cuando un punto extremo H.323 está en una conferencia H.332. El punto extremo que detecta la colisión seguirá los procedimientos en RTP para la resolución de colisiones del SSRC.

8.3.5 Procedimientos de instrucción de modo de comunicación

La **communicationModeCommand** H.245 es enviada por un MC H.323 para especificar el modo de comunicación para cada tipo de medios: unidifusión o multidifusión. Esta instrucción puede causar una conmutación entre una conferencia centralizada y una descentralizada, por lo que puede exigir el cierre de todos los canales lógicos existentes y la apertura de otros nuevos.

La **communicationModeCommand** especifica todas las sesiones de la conferencia. Para cada sesión se especifican los siguientes datos: el identificador de sesión RTP, el ID de sesión RTP asociado si es aplicable, una etiqueta de terminal si es aplicable, una descripción de la sesión, el **dataType** de las sesiones (por ejemplo, G.711), y una dirección unidifusión o multidifusión para los canales de medios y de control de medios apropiados para la configuración y el tipo de conferencia.

La **communicationModeCommand** transporta los modos de transmisión que los puntos extremos de la conferencia deben utilizar en una conferencia. La instrucción no transporta los modos de recepción, ya que son especificados por instrucciones **openLogicalChannel** enviadas desde el MC a los puntos extremos.

Se presume que la **communicationModeCommand** está definiendo los modos de una conferencia y, por tanto, se envía después de la indicación **multipointConference** (**conferencia multipunto**) que notifica a un punto extremo que debe cumplir las instrucciones del MC. Los puntos extremos deben esperar una **communicationModeCommand** antes de abrir canales lógicos cuando han recibido una indicación **multipointConference**.

Los puntos extremos que reciben una **communicationModeCommand** utilizan el campo **terminalLabel** de cada entrada de la tabla para determinar si la entrada es aplicable para su propio procesamiento. Las entradas que no contienen una **terminalLabel** se aplican a todos los puntos extremos de la conferencia. Las entradas que contienen **terminalLabels** son instrucciones a puntos extremos específicos que hacen corresponder la **terminalLabel** con la entrada. Por ejemplo, cuando se colocan trenes de audio procedentes de todos los puntos extremos en una dirección multidifusión (una sesión), la entrada de la tabla para el modo audio, la dirección de medios, y la dirección de control de medios no contendrán una **terminalLabel**. Cuando la entrada de la tabla manda a un punto extremo que envíe su vídeo a una dirección multidifusión, el MC incluirá esa **terminalLabel** de punto extremo.

La **communicationModeCommand** puede utilizarse para ordenar a puntos extremos de una conferencia (o de una llamada punto a punto) que cambien los modos indicando un nuevo modo para un **mediaChannel** que ya está en uso. Puede también utilizarse para decir a un punto extremo que transmita el tren de medios a una nueva dirección indicando el modo actualmente en uso, pero con un nuevo **mediaChannel**. Análogamente, un punto extremo que recibe una **communicationModeCommand** que indique el modo actualmente en uso y ningún **mediaChannel** debe cerrar el canal apropiado y el intento de reabrir utilizando la secuencia **openLogicalChannel-openLogicalChannelAck**, donde el **openLogicalChannelAck** contiene la dirección a la que el punto extremo enviará los medios.

El apéndice I contiene ejemplos de las entradas de la **communicationModeTable** (**tabla de modos de comunicación**) para diversos casos.

8.4 Fase D – Servicios de la llamada

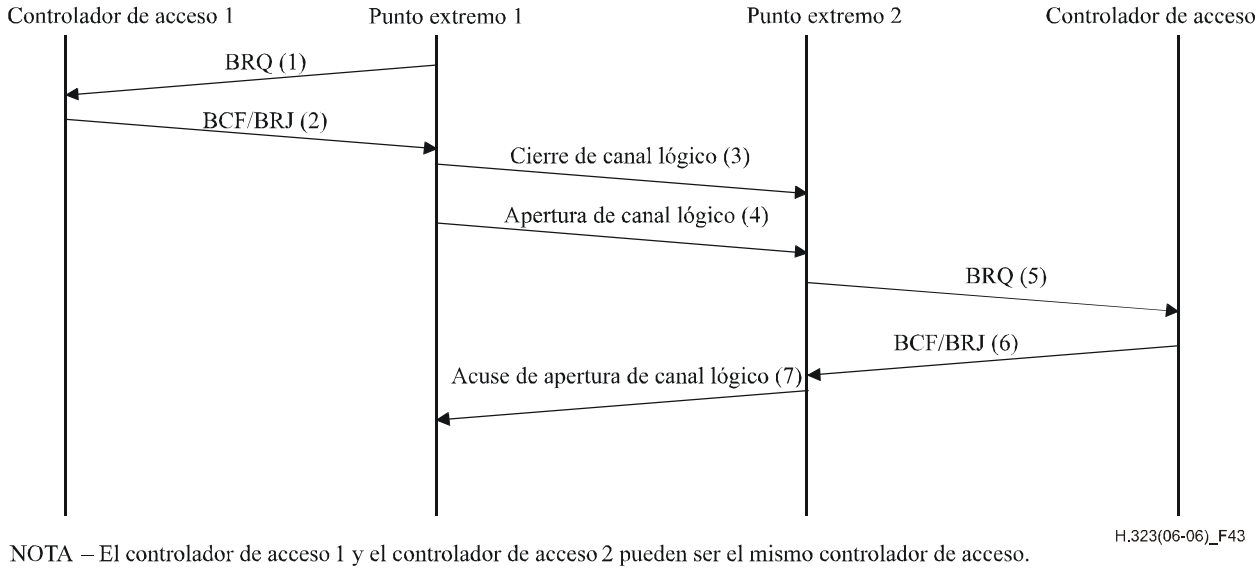
8.4.1 Cambios de anchura de banda

La anchura de banda de la llamada la establece y aprueba inicialmente el controlador de acceso, durante el intercambio de admisiones. Un punto extremo deberá asegurar que la suma correspondiente a todos los canales transmitidos y recibidos de audio y de vídeo excluidos cualesquiera encabezamientos RTP, encabezamientos de cabida útil RTP, encabezamientos de red y otra tara, se halla dentro de esa anchura de banda. Los canales de datos y de control no se incluyen en ese límite.

En cualquier momento durante una conferencia, los puntos extremos o el controlador de acceso pueden solicitar un aumento o una disminución de la anchura de banda de la llamada. Un punto extremo puede cambiar la velocidad binaria de un canal lógico sin solicitar un cambio de anchura de banda por el controlador de acceso si la suma de las velocidades binarias de todos los canales transmitidos y recibidos no supera la anchura de banda de llamada existente. Si el cambio da lugar a una velocidad binaria agregada que supera la anchura de banda de llamada existente, el punto extremo deberá pedir a su controlador de acceso un cambio de anchura de banda de la llamada y esperar la confirmación antes de aumentar efectivamente cualquier velocidad binaria. Se recomienda pedir un cambio de anchura de banda cuando un punto extremo utilice una anchura de banda reducida durante un periodo de tiempo prolongado, liberando así anchura de banda para otras llamadas.

Un punto extremo que desea cambiar su anchura de banda de llamada envía un mensaje de petición de cambio de ancho de banda (BRQ) (1) al controlador de acceso, el cual determina si la petición es aceptable. Los criterios utilizados para esa determinación quedan fuera del alcance de la presente Recomendación. Si el controlador de acceso determina que la petición no es aceptable, devuelve un mensaje de rechazo de cambio de ancho de banda (BRJ, *bandwidth change reject*) (2) al punto extremo. Si el controlador de acceso determina que la petición es aceptable, devuelve un mensaje de confirmación de cambio de anchura de banda (BCF, *bandwidth change confirm*) (2).

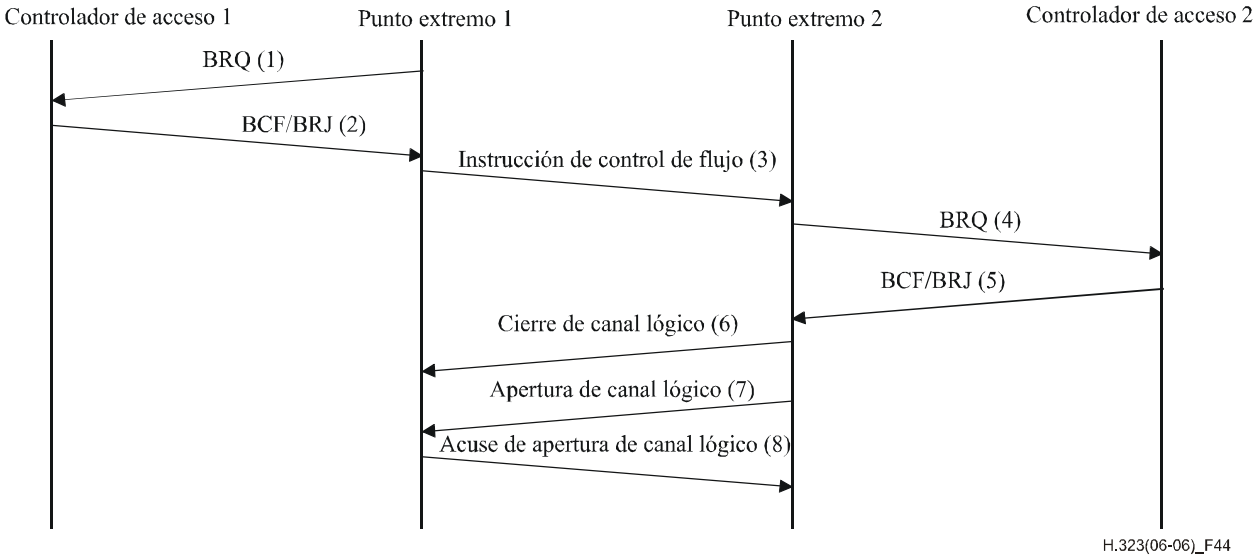
Si el punto extremo 1 desea incrementar su velocidad binaria transmitida en un canal lógico, determinará en primer lugar si en tal caso se sobrepasaría la anchura de banda de llamada (véase la figura 43). Si fuese a ocurrir así, el punto extremo 1 pedirá un cambio de anchura de banda (1 y 2) al controlador de acceso 1. Cuando la anchura de banda de llamada es suficiente para soportar el cambio, el punto extremo 1 envía un mensaje **closeLogicalChannel** (3) para cerrar el canal lógico. A continuación reabre el canal lógico utilizando el mensaje **openLogicalChannel** (4) especificando la nueva velocidad binaria. Si el punto extremo receptor desea aceptar el canal con la nueva velocidad binaria, debe asegurarse primero de que su anchura de banda de llamada no es sobrepasada a causa del cambio. Cuando sí lo sea, el punto extremo pedirá un cambio de anchura de banda de llamada (5 y 6) a su controlador de acceso. Cuando la anchura de banda de llamada es suficiente para soportar el canal, el punto extremo responde con un mensaje **openLogicalChannelAck** (7) y, cuando no es suficiente, responde con un mensaje **openLogicalChannelReject** (rechazo de apertura de canal lógico) indicando velocidad binaria inaceptable.



NOTA – El controlador de acceso 1 y el controlador de acceso 2 pueden ser el mismo controlador de acceso.

Figura 43/H.323 – Petición de cambio de anchura de banda – Cambio del transmisor

Si el punto extremo 1 desea incrementar su velocidad binaria transmitida en un canal lógico desde el punto extremo 2 sobre el que ejerce previamente un control del flujo a una velocidad binaria más baja, el punto extremo 1 determinará en primer lugar si en tal caso se sobrepasaría la anchura de banda de llamada (véase la figura 44). Si fuere a ocurrir así, el punto extremo 1 pedirá un cambio de anchura de banda al controlador de acceso 1. Cuando la anchura de banda de la llamada es suficiente para soportar el cambio, el punto extremo 1 envía un mensaje **flowControlCommand** (3) para indicar el nuevo límite superior de la velocidad binaria para el canal. Si el punto extremo 2 decide incrementar la velocidad binaria en el canal, debe asegurarse primero de que su anchura de banda de llamada no es sobrepasada a causa del cambio. Cuando si lo sea, el punto extremo 2 pedirá un cambio de anchura de banda (4 y 5) a su controlador de acceso. Si la anchura de banda es suficiente para soportar el canal, el punto extremo 2 enviará el mensaje **closeLogicalChannel** (6) para cerrar el canal lógico. A continuación reabre el canal lógico utilizando el **openLogicalChannel** (7) con la especificación de la nueva velocidad binaria. El punto extremo 1 deberá aceptar seguidamente el canal con la nueva velocidad binaria y responder con un **openLogicalChannelAck** (8).



NOTA – El controlador de acceso 1 y el controlador de acceso 2 pueden ser el mismo controlador de acceso.

Figura 44/H.323 – Petición de cambio de anchura de banda – Cambio del receptor

Un controlador de acceso que desea cambiar la velocidad binaria transmitida del punto extremo 1 envía un mensaje BRQ al punto extremo 1. Si la petición es de disminución de la velocidad binaria y el punto extremo puede soportar la velocidad binaria solicitada, el punto extremo 1 cumplirá la petición reduciendo su velocidad binaria agregada y devolviendo un BCF. Si el punto extremo 1 no soporta la velocidad binaria solicitada, puede devolver un mensaje BRJ. El punto extremo 1 puede iniciar la señalización H.245 apropiada para informar al punto extremo 2 de que las velocidades binarias han cambiado. Esto permitirá al punto extremo 2 informar a su controlador de acceso del cambio. Si la petición es de incremento, el punto extremo puede incrementar su velocidad binaria cuando así lo desee y lo permita el controlador de acceso.

Si el controlador de acceso desea aumentar la anchura de banda utilizada por el punto extremo, éste puede devolver un mensaje BCF para indicar la aceptación de la nueva velocidad binaria superior o un mensaje BRJ para indicar que rechaza la anchura de banda adicional. El punto extremo sólo debe aceptar la velocidad binaria superior si está preparado para utilizar la anchura de banda adicional.

El punto extremo enviará un mensaje BRQ al controlador de acceso siempre que la utilización de anchura de banda disminuya por debajo de lo especificado en el mensaje ARQ original o en el último mensaje BRQ o BCF. El punto extremo también enviará un mensaje BRQ al controlador de acceso siempre que la señalización del canal lógico de lugar a la adición o supresión de un tren multidifusión único hacia el punto extremo o desde éste.

El controlador de acceso puede utilizar la información de utilización de anchura de banda para mejorar la gestión de la anchura de banda en la red. Debe notarse que una gestión de anchura de banda precisa requiere que el controlador de acceso entienda cabalmente la topología de la red, lo cual queda fuera del alcance de esta Recomendación. Además, la utilización de la anchura de banda por parte del punto extremo puede, de hecho, ser distinta de la que había sido informada debido a la utilización de la supresión de silencios, de códecs de baja velocidad binaria u otros factores. Un punto extremo no enviará repetidamente mensajes BRQ a su controlador de acceso cuando la utilización real de la anchura de banda oscile debido a dichos factores. Más bien, el punto extremo debería solicitar la anchura de banda necesaria en función del conjunto de canales lógicos abiertos y no debería considerar los periodos de silencio u otros factores como una disminución de la anchura de banda.

8.4.2 Estado

Para determinar si un punto extremo se ha desconectado o ha pasado a un modo fallo, el controlador de acceso puede utilizar la secuencia de mensajes de petición de información (IRQ, *information request*) o de respuesta a petición de información (IRR, *information request response*) (véase la Rec. UIT-T H.225.0), a fin de sondear secuencialmente los puntos extremos con un intervalo establecido por el fabricante. El controlador de acceso puede solicitar información para una única llamada o para todas las llamadas activas. Excepto cuando se soliciten segmentos IRR adicionales, el intervalo de sondeo secuencial para solicitar información de una llamada en particular o de todas las llamadas deberá ser superior a 10 s. Sin embargo, el controlador de acceso puede enviar mensajes IRQ que contengan valores de **callReferenceValue** únicos sin tener en cuenta el periodo de sondeo. Este mensaje puede ser utilizado también por dispositivos de diagnóstico como los mencionados en 11.2.

Cuando un punto extremo transmite un mensaje IRR, éste incluirá el campo **perCallInfo** para proporcionar al controlador de acceso información detallada de las llamadas. Si el controlador de acceso solicita la situación de todas las llamadas y no existen llamadas activas, o de una sola llamada que ya no está activa o para la cual el punto extremo no tiene información, el punto extremo devolverá un mensaje IRR en el que incluye el campo **invalidCall** y no omitirá el campo **perCallInfo** del IRR.

Si el controlador de acceso desea recibir información detallada de la llamada para todas las llamadas activas en un punto extremo, puede enviar un mensaje IRQ con el campo **callReferenceValue** puesto a 0. El controlador de acceso debería incluir el campo **segmentedResponseSupported** a fin de permitir que las peticiones relativas a todas las llamadas se puedan segmentar si ello es necesario. Si se incluye el campo **segmentedResponseSupported**, el punto extremo devolverá toda o parte de la información de la llamada en el campo **perCallInfo** de un solo mensaje IRR. Si la segmentación no está permitida, pero en el mensaje IRR no puede incluirse toda la información de la llamada, el punto extremo incluirá el campo **incomplete** (**incompleto**) en el mensaje IRR. Si la segmentación está permitida, el punto extremo puede devolver uno o múltiples mensajes IRR en respuesta al mensaje IRQ. Si se devuelve un mensaje IRR que contenga toda la información de la llamada, el elemento **irrStatus** (**estado de irr**) no estará presente. Si la respuesta está segmentada en múltiples mensajes IRR, el punto extremo enviará el primer mensaje IRR e incluirá el campo **segment** (**segmento**). Si el controlador de acceso desea recibir el siguiente segmento, transmitirá otro mensaje IRQ que incluya el campo **segmentedResponseSupported**, que tiene **callReferenceValue** puesto a 0 y el campo **nextSegmentRequested** puesto al valor del siguiente segmento que el controlador de acceso espera recibir. Si el controlador de acceso desea recibir segmentos adicionales, enviará el mensaje IRQ siguiente dentro de los 5 segundos posteriores a la recepción del mensaje IRR previo. Si el punto extremo recibe la petición de un segmento adicional después de 5 segundos (más un tiempo adecuado fijado de forma local para tener en cuenta el retardo de la red), puede devolver un mensaje que incluya el campo **incomplete**. Cuando se recibe un mensaje IRQ de un controlador de acceso que solicita el segmento siguiente en el intervalo de tiempo permitido para ello, el punto extremo transmitirá el siguiente mensaje IRR que contenga el segmento siguiente de la información de llamada. Obsérvese que si se pierde un mensaje IRR, el controlador de acceso puede retransmitir una petición para el segmento previamente transmitido. Por lo tanto, el punto extremo estará preparado para transmitir el segmento previo o el siguiente. Si no hay disponibles más segmentos o cuando el punto extremo transmita el último segmento de una serie de mensajes IRR, el punto extremo devolverá un mensaje IRR que incluye el campo **complete**. El controlador de acceso no transmitirá un mensaje IRQ distinto al punto extremo que solicite toda la información de la llamada hasta que se transmita el último segmento de información o hasta que transcurra el periodo de sondeo de 10 segundos.

NOTA 1 – Puesto que las llamadas pueden comenzar o terminar después del envío del primer segmento de mensaje IRR que sea respuesta a un mensaje IRQ que solicite información de la llamada para todas las llamadas, el punto extremo puede optar o no por incluir dichas llamadas cuando envíe ulteriores segmentos de mensajes IRR. La decisión de comunicar dichas llamadas cuando se envíen ulteriores segmentos IRR, la toma el fabricante.

NOTA 2 – Para mejorar la calidad de funcionamiento y lograr una mejor escalabilidad, un controlador de acceso debería limitar la frecuencia utilizada para pedir información detallada de las llamadas. El pedido de información detallado para todas las llamadas es ventajoso cuando, por ejemplo, un punto extremo se registra por primera vez con el controlador de acceso. No obstante, la repetición de pedidos de esta información, en especial desde MCU o pasarelas en gran escala, pueden dar lugar a degradaciones de calidad inaceptables.

El controlador de acceso puede requerir a un punto extremo el envío periódico de un mensaje IRR no solicitado. El controlador de acceso lo indicará al punto extremo especificando la cadencia con que se debe enviar ese mensaje IRR en el campo **irrFrequency** (**frecuencia de irr**) del mensaje de confirmación de admisión (ACF). Un punto extremo que reciba la indicación de cadencia de **irrFrequency** enviará un mensaje IRR con esa cadencia mientras dura la llamada. Siempre que la cadencia esté en vigor, el controlador de acceso podrá seguir enviando mensajes IRQ al punto extremo, que responderá como se ha descrito más arriba.

Un punto extremo puede desear que algunos de los IRR no solicitados se entreguen fiablemente. El controlador de acceso puede hacer lo posible utilizando el campo **willRespondToIRR** en la RCF o ACF que puede acusar IRR no solicitados. En este caso, el punto extremo puede explícitamente pedir al controlador de acceso que envíe un acuse de recibo del IRR. El controlador de acceso responderá a dicho mensaje IRR enviando sea un acuse de recibo (IACK) o un acuse de recibo negativo (INAK). Si el controlador de acceso no anunciase que reconocerá los IRR, o si el punto extremo no solicitase dicho acuse de recibo, no seguirá ninguna respuesta al IRR.

Mientras dura una llamada, el punto extremo o el controlador de acceso pueden indagar periódicamente el estado de aquélla desde otro punto extremo. El punto extremo o el controlador de acceso solicitante emite un mensaje Indagación de estado. El punto extremo receptor del mensaje Indagación de estado responderá con un mensaje Estado indicando el estado en que en esos momentos se encuentra la llamada. Este procedimiento puede ser utilizado por el controlador de acceso para verificar periódicamente si una llamada sigue estando activa. Los puntos extremos podrán aceptar cualesquiera valores de estado válidos recibidos en el mensaje Estado, incluidos los que no pueden ser capaz de introducir. Hay que tener en cuenta que se trata de un mensaje H.225.0 enviado por el canal de señalización de llamada y no debe confundirse con un mensaje IRR, que es un mensaje RAS enviado por el canal RAS.

El controlador de acceso puede desear recibir copias de ciertas PDU de señalización de llamada H.225.0 cuando son recibidas o enviadas por un punto extremo. Un punto extremo indica su capacidad de enviar estas PDU fijando el **willSupplyUUIEs** (**suministrará UUIE**) en el mensaje ARQ o RRQ enviado al controlador de acceso. El controlador de acceso indica la lista de tipos de PDU de los que desea recibir copias, en el campo **uuiesRequested** (**uuie solicitadas**) en el ACF o RCF. También indica si desea copias cuando las PDU son enviadas o recibidas. Un punto extremo que indica esta capacidad y recibe esta lista, enviará una IRR al controlador de acceso cada vez que recibe/envía el tipo de PDU solicitada.

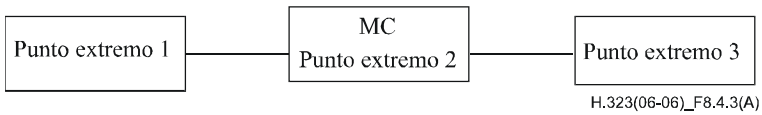
8.4.3 Ampliación de una conferencia ad hoc

Los siguientes procedimientos son opcionales para las terminales y pasarelas, y obligatorios para los MC.

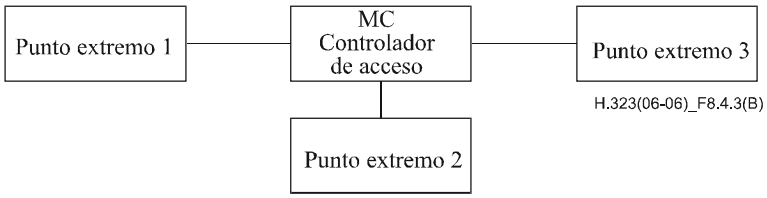
Cuando un usuario efectúa una llamada, el punto extremo llamante a menudo desconoce el propósito de la llamada. El usuario puede desear simplemente crear una conferencia para él mismo y el punto extremo llamado, el usuario puede desear incorporarse a una conferencia en la entidad llamada, o el usuario puede desear obtener una lista de conferencias que la entidad llamada puede proporcionar. Utilizando los procedimientos de esta cláusula, las conferencias pueden ampliarse de conferencias punto a punto a conferencias multipunto ad hoc.

Una conferencia multipunto ad hoc puede ser ampliada a partir de una conferencia punto a punto en la que participa un MC a una conferencia multipunto. En primer lugar, se crea una conferencia punto a punto entre dos puntos extremos (punto extremo 1 y punto extremo 2). Al menos un punto extremo, o el controlador de acceso, debe contener un MC. Una vez que se ha creado la conferencia punto a punto, ésta puede ser ampliada a conferencia multipunto de dos maneras diferentes. La primera manera es cuando cualquier punto extremo en la conferencia invita a otro punto extremo (punto extremo 3) a la conferencia llamando a ese punto extremo a través del MC. La segunda manera es que un punto extremo (punto extremo 3) se incorpore a una conferencia existente llamando a un punto extremo que participa en la conferencia.

La ampliación de la conferencia ad hoc puede efectuarse utilizando el modelo de señalización de llamada directa o el modelo de señalización de llamada encaminada por el controlador de acceso. La topología del canal de control H.245 para el modelo de señalización de llamada directa aparece como:



La topología del canal de control H.245 para el modelo de señalización de llamada encaminada por el controlador de acceso aparece como:



En ambos casos debe estar presente un MC en la conferencia en el momento de la ampliación a más de dos puntos extremos. Obsérvese que en el modelo con encaminamiento por el controlador de acceso, el MC puede estar situado en el controlador de acceso y/o en uno de los puntos extremos.

Los procedimientos requeridos para crear una conferencia punto a punto y ampliarla a través de invitación e incorporación, para cada modelo de llamada se tratan a continuación. Pueden también tratarse los procedimientos para que el punto extremo llamante descubra una lista de conferencias que la entidad llamada puede proporcionar.

Cabe señalar que la llamada es terminada por un fallo de la entidad que está proporcionando el MC.

8.4.3.1 Señalización de llamada de punto extremo directa – Creación de conferencia

El punto extremo 1 crea una conferencia con el punto extremo 2 como sigue:

A1) El punto extremo 1 envía un mensaje Establecimiento al punto extremo 2 que contiene un CID globalmente único = N y un **conferenceGoal = create** de acuerdo con el procedimiento indicado en 8.1.

A2) El punto extremo 2 tiene las siguientes opciones:

A2a) Si desea incorporarse a la conferencia, envía un mensaje Conexión con CID = N al punto extremo 1. En este caso si:

1) no está participando en otra conferencia; o

2) está participando en otra conferencia, es capaz de participar en múltiples conferencias al mismo tiempo, y el CID = N recibido no concuerda con el CID de cualquiera de las conferencias en la cual está participando en ese momento.

A2b) Si está en otra conferencia con CID = M y sólo puede participar en una conferencia a la vez:

1) rechaza la llamada enviando liberación completa indicando que está en conferencia; o

2) puede pedir al punto extremo 1 incorporarse a la conferencia con CID = M enviando un mensaje facilidad que indica **routeCallToMC** (**encaminamiento de llamada a MC**) con la dirección de transporte de canal de señalización de llamada del punto extremo que contiene el MC y CID = M de la conferencia. El tratamiento del mensaje facilidad por el punto extremo 1 se describe en 8.4.3.7.

A2c) Si no desea incorporarse a la conferencia, rechaza la llamada enviando liberación completa con la indicación destino ocupado.

A2d) Si el punto extremo 2 es un(a) MC(U) que acoge múltiples conferencias y desea proporcionar al punto extremo 1 una selección de conferencias a las que incorporarse, puede enviar un mensaje Facilidad que indique **conferenceListChoice** (**selección de lista de conferencias**) y una lista de conferencias dentro de las cuales pueda elegir el punto extremo 1. La lista de conferencias se envía como parte de la UUIE facilidad. Para facilitar la retrocompatibilidad con los puntos extremos de la versión 1, las listas de conferencias sólo se proporcionan si el **protocolIdentifier** en el mensaje Establecimiento del punto extremo 1 indica que es versión 2 o superior.

Al recibir este mensaje facilidad **conferenceListChoice**, el punto extremo 1 puede incorporarse a una conferencia de la lista de conferencias enviando un nuevo mensaje Establecimiento al (a la) MC(U) por el canal de señalización de llamada que contiene el CID seleccionado y que tiene **conferenceGoal = join**. Si el punto extremo 1 opta por no incorporarse a ninguna de las conferencias de la lista, enviará un mensaje Liberación Completa al (a la) MC(U).

A3) Si el punto extremo 2 entra en la conferencia, el punto extremo 1 utiliza la dirección de transporte del canal de control proporcionada en el mensaje Conexión para abrir el canal de control con el punto extremo 2.

A4) Los mensajes H.245 se intercambian como se describe a continuación:

A4a) Se intercambian mensajes **terminalCapabilitySet** entre los puntos extremos para determinar el número de versión de H.245 utilizado con el fin de analizar correctamente los mensajes recibidos restantes.

A4b) Mediante el procedimiento de determinación de principal-subordinado H.245, se determina que el punto extremo 2 es el principal. En el modelo encaminado por el controlador de acceso, el principal puede estar en un MC coubicado con el controlador de acceso. Si el principal tiene un MC, se convierte en el MC activo. Puede enviar la **mcLocationIndication** (**indicación de ubicación de mc**) al otro u otros puntos extremos. El MC puede estar activo en la conferencia en ese momento o cuando el usuario inicia la función de conferencia multipunto, a opción del fabricante.

A4c) El principal puede enviar el mensaje **terminalNumberAssign** a los puntos extremos. Los puntos extremos utilizarán el número del terminal de 8 bits y no utilizarán el número de MCU de 8 bits, del número de 16 bits asignado como los 8 bits bajos del campo SSRC en el encabezamiento RTP. Estos 8 bits bajos en SSRC identifican los trenes desde un punto extremo determinado.

A4d) Como las capacidades del receptor son conocidas de acuerdo con el mensaje **terminalCapabilitySet**, el transmisor abre los canales lógicos. Enviará **h2250MaximumSkewIndication** para cada par de audio y vídeo transmitido.

8.4.3.2 Señalización de llamada de punto extremo directa – Invitación a la conferencia

Hay dos casos de la invitación a la conferencia. Primero, el punto extremo que contiene el MC activo desea invitar a otro punto extremo a la conferencia. Segundo, un punto extremo que no contiene el MC activo desea invitar a otro punto extremo a la conferencia.

1) Después que se ha establecido una conferencia punto a punto utilizando los procedimientos indicados en A1 a A4 en 8.4.3.1, un punto extremo (punto extremo 2) que contiene el MC activo que desea incorporar otro punto extremo a la conferencia utilizará el siguiente procedimiento:

B1) El punto extremo 2 envía un mensaje Establecimiento al punto extremo 3 con CID = N y **conferenceGoal** = **invite** de acuerdo con los procedimientos de 8.1. Véase la figura 45.

B2) El punto extremo 3 tiene las siguientes opciones:

B2a) Si desea aceptar la invitación de incorporarse a la conferencia, envía un mensaje Conexión con CID = N al punto extremo 2.

B2b) Si desea rechazar la invitación de incorporarse a la conferencia, envía un mensaje Liberación Completa indicando destino ocupado al punto extremo 2.

B2c) Si está en otra conferencia con CID = M, puede pedir al punto extremo 2 incorporarse a la conferencia con CID = M enviando un mensaje facilidad con la indicación **routeCallToMC** con la dirección de transporte del canal de señalización de llamada del punto extremo que contiene el MC y el CID = M de la conferencia. El tratamiento del mensaje facilidad por el punto extremo 2 se describe en 8.4.3.7.

B2d) Si el CID recibido concuerda con el CID de una conferencia en la cual el punto extremo 3 está participando actualmente, rechazará la llamada enviando liberación completa con la indicación de que ya está en conferencia.

B3) Si el punto extremo 3 acepta la invitación, el punto extremo 2 utiliza la dirección del transporte del canal de control proporcionada en el mensaje Conexión para abrir el canal de control con el punto extremo 3.

B4) A continuación se intercambian los siguientes mensajes H.245:

C1) Se intercambian mensajes **terminalCapabilitySet** entre el MC y el punto extremo 3.

C2) Mediante el procedimiento de determinación de principal-subordinado H.245, se determina que el punto extremo 2 es ya el MC activo. Entonces el MC activo puede enviar **mcLocationIndication** al punto extremo 3.

C3) El MC enviará **multipointConference** en este momento a los tres puntos extremos.

C4) El MC puede enviar el mensaje **terminalNumberAssign** al punto extremo 3. Si se recibe, los puntos extremos utilizarán el número de terminal de 8 bits y no utilizarán el número de MCU de 8 bits, del número de 16 bits asignado como los 8 bits de orden inferior del campo SSRC en el encabezamiento RTP. Estos 8 bits de orden inferior en SSRC identifican los trenes procedentes de un determinado punto extremo.

C5) Un punto extremo puede obtener la lista de los otros puntos extremos que participan en la conferencia enviando el mensaje **terminalListRequest** al MC. El MC responde con la respuesta de **terminalListResponse** (**lista de terminales**).

C6) Cuando un nuevo punto extremo se incorpora a la conferencia, el MC envía el mensaje **terminalNumberAssign** al punto extremo 4 y el mensaje **terminalJoinedConference** a los puntos extremos 1, 2 y 3.

C7) Cuando un punto extremo abandona la conferencia, el MC envía el mensaje **terminalLeftConference** (**el terminal abandonó la conferencia**) a los puntos extremos restantes.

C8) El MC enviará la **communicationModeCommand** a todos los puntos extremos de la conferencia.

C9) El punto extremo 1 y el punto extremo 2 cerrarán sus canales lógicos que fueron creados durante la conferencia punto a punto si no concuerdan con la información contenida en el mensaje **communicationModeCommand**.

C10) Se pueden abrir ahora los canales lógicos entre el MC y los puntos extremos.

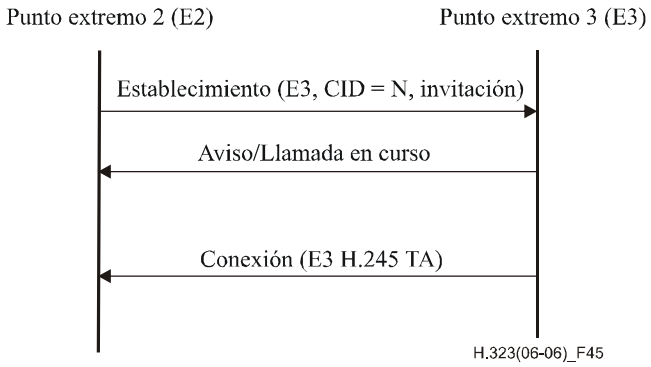


Figura 45/H.323 – Señalización de invitación con MC

2) Después que se ha establecido una conferencia punto a punto utilizando los procedimientos indicados en A1 a A4 en 8.4.3.1, un punto extremo (el punto extremo 1) que no contiene el MC activo que desea añadir otro punto extremo a la conferencia utilizará el siguiente procedimiento:

B1) El punto extremo 1 envía un mensaje Establecimiento al MC (punto extremo 2) con un nuevo CRV que indica una llamada al punto extremo 3 proporcionando la dirección de transporte del punto extremo 3, CID = N y **conferenceGoal = invite**. Véase la figura 46.

B2) El punto extremo 2 envía un mensaje Establecimiento al punto extremo 3 con CID = N y **conferenceGoal = invite**, de acuerdo con los procedimientos indicados en 8.1.

B3) Durante la señalización de la llamada con el punto extremo 3, el punto extremo 2 pasará los mensajes de señalización de llamada recibidos del punto extremo 3, incluido conexión, al punto extremo 1 (que invitó originalmente).

B4) El punto extremo 3 tiene las mismas opciones, descritas anteriormente, de aceptar o rechazar la invitación.

B5) Tras haber completado el procedimiento de establecimiento de la comunicación entre el punto extremo 2 y el punto extremo 3, el punto extremo 2 enviará un mensaje Liberación Completa al punto extremo 1.

B6) Si el punto extremo 3 acepta la invitación, el punto extremo 2 utiliza la dirección de transporte del canal de control proporcionada en el mensaje Conexión para abrir el canal de control con el punto extremo 3.

B7) Se intercambian después los mensajes H.245, según se ha descrito anteriormente en los procedimientos C1 a C10.

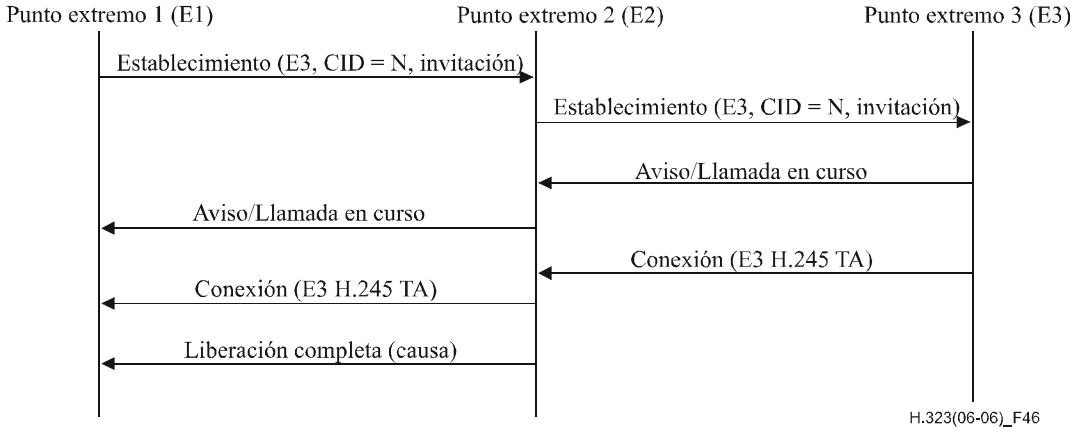


Figura 46/H.323 – Señalización de invitación sin MC

8.4.3.3 Señalización de llamada de punto extremo directa – Incorporación a la conferencia

Hay dos casos de incorporación a la conferencia. Primero, un punto extremo llama al punto extremo que contiene el MC activo. Segundo, un punto extremo llama a un punto extremo que no es el MC activo.

Una vez que se ha establecido una conferencia punto a punto utilizando los procedimientos A1 a A4 en 8.4.3.1, un punto extremo (punto extremo 3) que desea incorporarse a una conferencia puede tratar de conectar con el punto extremo que contiene el MC activo en la conferencia. En este caso, se aplicará el siguiente procedimiento:

B1) El punto extremo 3 envía un mensaje Establecimiento al punto extremo 2 con CID = N y **conferenceGoal = join** de acuerdo con el procedimiento de 8.1. Véase la figura 47.

B2) Si el CID concuerda con el CID de una conferencia activa en el MC, el punto extremo 2 (MC) tiene las siguiente opciones:

B2a) Si decide que se debe permitir al punto extremo 3 que se incorpore a la conferencia, envía el mensaje Conexión con CID = N.

B2b) Si decide que no se debe permitir al punto extremo 3 que se incorpore a la conferencia, envía el mensaje Liberación Completa con destino ocupado.

B3) Si el CID no concuerda con el CID de una conferencia activa en el MC, el punto extremo 2 enviará liberación completa indicando un CID inapropiado.

B4) Si el punto extremo 2 permite la incorporación, abre el canal de control con el punto extremo 3.

B5) Se intercambian después los mensajes H.245 como se describe anteriormente en los procedimientos C1 a C10.

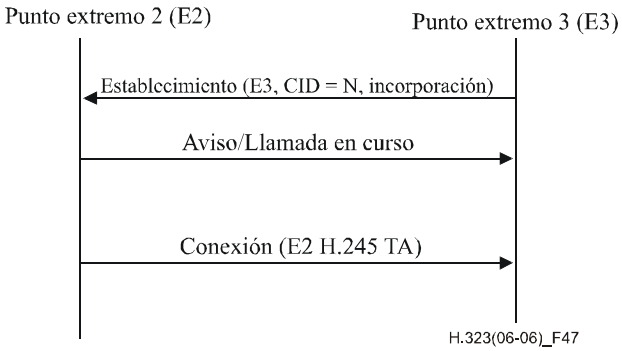


Figura 47/H.323 – Señalización de incorporación con MC

Después que se ha establecido una conferencia punto a punto utilizando los procedimientos indicados en A1 a A4, un punto extremo (punto extremo 3) que desea incorporarse a una conferencia puede tratar de conectar con un punto extremo que no contiene el MC activo en la conferencia. En este caso, se aplicará el siguiente procedimiento:

B1) El punto extremo 3 envía un mensaje Establecimiento al punto extremo 1 con CID = N y **conferenceGoal = join**, de acuerdo con el procedimiento indicado en 8.1. Véase la figura 48.

B2) El punto extremo 1 devuelve un mensaje facilidad que indica **routeCallToMC** con la dirección de transporte de canal de señalización de llamada del punto extremo 2 (que contiene el MC activo) y el CID = N de la conferencia.

B3) El punto extremo 3 envía después un mensaje Establecimiento al punto extremo 2 (MC) con CID = N y **conferenceGoal = join**, como se describe en el anterior procedimiento de incorporación a la conferencia.

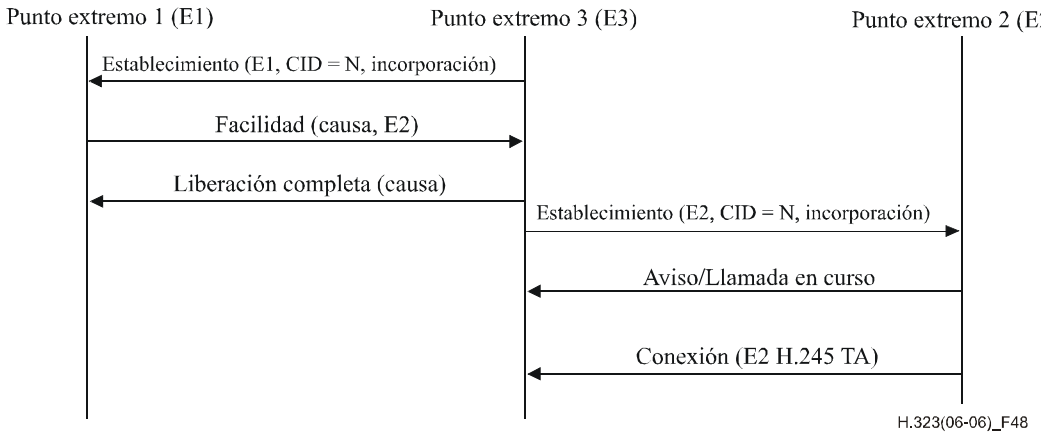


Figura 48/H.323 – Señalización de incorporación sin MC

8.4.3.4 Señalización de llamada encaminada por el controlador de acceso – Creación de conferencia

Cuando el controlador de acceso encamina el canal de señalización de llamada y el canal de control H.245, el controlador de acceso puede contener (o tener acceso a) un MC o una MCU. Los procedimientos A1 a A4 se utilizan para establecer la comunicación punto a punto.

Si el (la) MC(U) que acoge múltiples conferencias y desea proporcionar al punto extremo 1 una selección de conferencias a las que incorporarse, puede enviar un mensaje Facilidad que indique **conferenceListChoice** y una lista de conferencias de entre las cuales pueda elegir el punto extremo 1. La lista de conferencias se envía como parte de la UUIE Facilidad. Para permitir la retrocompatibilidad con los puntos extremos de la versión 1, las listas de conferencias sólo se proporcionan si el **protocolIdentifier** en el mensaje Establecimiento del punto extremo 1 indica que es versión 2 o superior.

Al recibir este mensaje Facilidad **conferenceListChoice**, el punto extremo 1 puede incorporarse a una conferencia de la lista de conferencias enviando un nuevo mensaje Establecimiento al(a la) MC(U) por el canal de señalización de llamada que contiene el CID seleccionado y que contiene **conferenceGoal = join**. Si el punto extremo 1 opta por no incorporarse a ninguna de las conferencias de la lista, enviará un mensaje Liberación Completa al(a la) MC(U).

Durante la determinación de principal-subordinado A4b), si el tipo de terminal del controlador de acceso es superior al **terminalType** recibido en el mensaje **masterSlaveDetermination**, el controlador de acceso puede tratar de pasar a ser el principal de la llamada. En este caso, el controlador de acceso enviará inmediatamente un mensaje **masterSlaveDeterminationAck** al origen del mensaje determinación de principal-subordinado indicando que es un subordinado, y llevará a cabo la determinación de principal-subordinado con la entidad de destino definida en 6.2.8.4. Si el controlador de acceso gana esa determinación de principal-subordinado, el MC asociado con el controlador de acceso será el MC activo. Si el **terminalType** del controlador de acceso no es superior al **terminalType** del punto extremo o el controlador de acceso decide no sustituir el tipo de terminal del punto extremo por el suyo propio, el controlador de acceso no modificará el valor del **terminalType** y reenviará de manera transparente todos los mensajes de ese procedimiento determinación de principal-subordinado.

8.4.3.5 Señalización de llamada encaminada por el controlador de acceso – Invitación a la conferencia

Después que se ha establecido una conferencia punto a punto utilizando los procedimientos A1 a A4 modificados anteriormente, un punto extremo (punto extremo 1 ó 2) que no contiene el MC activo que desea incorporar otro punto activo a la conferencia, utilizará el siguiente procedimiento:

B1) El punto extremo 1 envía un mensaje Establecimiento a través del controlador de acceso dirigido al punto extremo 3 con un nuevo CRV, CID = N y **conferenceGoal = invite**. Véase la figura 49.

B2) El controlador de acceso (MC) envía un mensaje Establecimiento al punto extremo 3 con CID = N y **conferenceGoal = invite**, de acuerdo con los procedimientos indicados en 8.1.

B3) Durante la señalización de llamada con el punto extremo 3, el controlador de acceso pasará los mensajes de señalización de llamada recibidos del punto extremo 3, incluido conexión, al punto extremo 1 (el invitador original).

B4) El punto extremo 3 tiene las mismas opciones, descritas anteriormente, de aceptar o rechazar la invitación.

B5) Tras completar el procedimiento de establecimiento de comunicación entre el controlador de acceso y el punto extremo 3, el controlador de acceso enviará un mensaje Liberación Completa al punto extremo 1.

B6) Si el punto extremo 3 acepta la invitación, el controlador de acceso utiliza la dirección de transporte del canal de control proporcionada en el mensaje Conexión para abrir el canal de control con el punto extremo 3.

B7) Se intercambian después los mensajes H.245 descritos anteriormente en los procedimientos C1 a C10 y el controlador de acceso participa en todos los procedimientos de determinación de principal-subordinado como el MC activo (C2). En este momento, los canales de control de los puntos extremos se deben conectar al MC y el MC deberá tener el control de la conferencia.

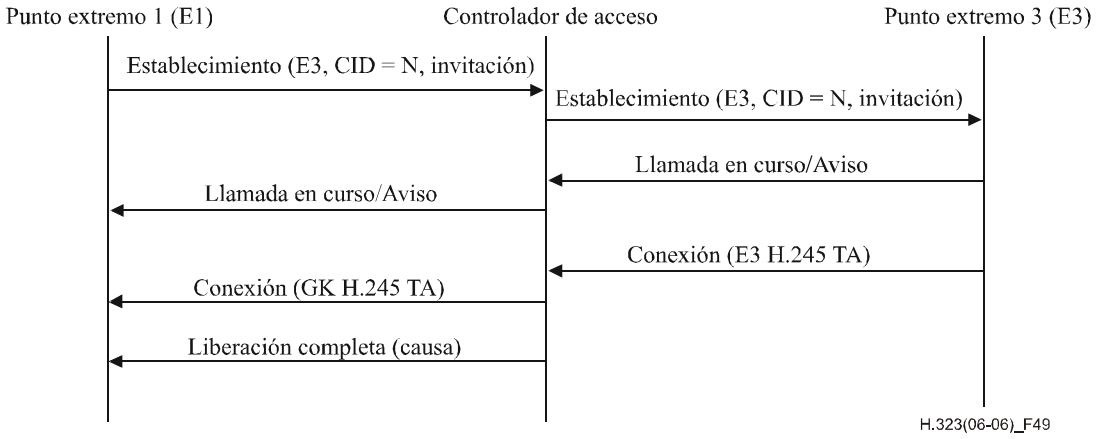


Figura 49/H.323 – Señalización de invitación encaminada por controlador de acceso

8.4.3.6 Modelo de llamada encaminada por el controlador de acceso – Incorporación a la conferencia

Después que se ha establecido una conferencia punto a punto utilizando los procedimientos indicados en A1 a A4 modificados anteriormente, un punto extremo (punto extremo 3) que desea incorporarse a la conferencia puede intentar conectar con un punto extremo que no contiene el MC activo en la conferencia. En este caso, se empleará el siguiente procedimiento:

B1) El punto extremo 3 envía un mensaje Establecimiento a través del controlador de acceso dirigido al punto extremo 1 con CID = N y **conferenceGoal = join**, de acuerdo con los procedimientos indicados en 8.1. Véase la figura 50.

B2) Si el CID concuerda con el CID de una conferencia activa en el MC, el controlador de acceso (MC) tiene las siguientes opciones:

- B2a) Si decide que se debe permitir que el punto extremo 3 se incorpore a la conferencia, envía el mensaje Conexión con CID = N al punto extremo 3.
- B2b) Si decide que no se debe permitir que el punto extremo 3 se incorpore a la conferencia, envía el mensaje Liberación Completa indicando destino ocupado.
- B2c) El controlador de acceso puede enviar el mensaje Establecimiento al punto extremo 1. El punto extremo 1 puede responder con un mensaje Facilidad indicando **routeCallToMC** o puede responder con Liberación Completa.

B3) Si el CID no concuerda con el CID de una conferencia activa en el MC, el controlador de acceso enviará Liberación Completa indicando un CID incorrecto.

B4) Si el controlador de acceso permite la incorporación, utiliza la dirección de transporte del canal de control proporcionada en el mensaje Establecimiento para abrir el canal de control con el punto extremo 3.

B5) A continuación se intercambian los mensajes H.245 según se describe anteriormente en los procedimientos C1 a C10 y el controlador de acceso participará en todos los procedimientos de determinación de principal-subordinado como el MC activo (C2). En este momento, se debe conectar los canales de control de los puntos extremos al MC, y el MC debe tener el control de la conferencia.

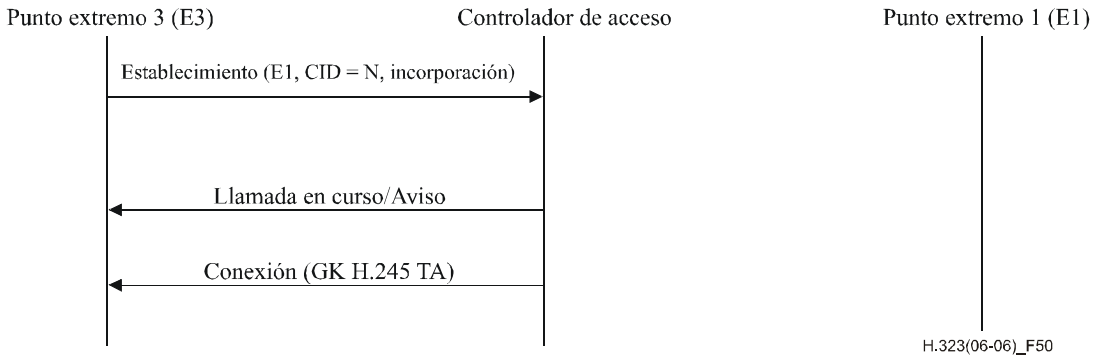


Figura 50/H.323 – Señalización de incorporación encaminada por controlador de acceso

8.4.3.7 Tratamiento del mensaje Facilidad

Al recibir un mensaje Facilidad que indica **routeCallToMC** con la dirección de transporte del canal de señalización de llamada del punto extremo que contiene el MC y el CID de una conferencia, un punto extremo puede liberar la llamada en curso y tratar de incorporarse a la conferencia indicada según los procedimientos de 8.4.3.3 o de 8.4.3.6.

Un punto extremo puede recibir dicho mensaje Facilidad como respuesta directa a su mensaje Establecimiento o durante la fase activa de una llamada.

8.4.3.8 Conferencia fuera de consulta

En esta cláusula se definen los procedimientos que ha de seguir un punto extremo (punto extremo A) para pedir una conferencia ad-hoc con otros dos o más puntos extremos (puntos extremos distantes B, C, etc.) con los que el punto extremo A ya tiene llamadas activas. Esto se aplica normalmente al caso, pero sin limitarse a él, en que se pide una conferencia ad-hoc fuera de una condición de consulta.

NOTA 1 – "Condición de consulta" se refiere a aquella estado en la que un punto extremo A tiene una llamada activa con un punto extremo C (llamada de consulta) mientras tiene uno o más puntos extremos retenidos, es decir llamada(s) retenida(s). Un punto extremo se puede poner en retención utilizando los procedimientos de la Rec. UIT-T H.450.4 [35], o de 8.4.6 o mediante procedimientos locales.

El punto extremo A tiene la capacidad de "mezclar" llamadas independientes a puntos extremos múltiples en una sola conferencia ya sea en el punto extremo A (como se describe en el escenario 1 que sigue) o formando la conferencia en una MCU separada (como se describe en el escenario 2, más adelante).

NOTA 2 – Los procedimientos de esta cláusula se refieren solamente a las llamadas en un punto extremo que se han de incorporar a una conferencia fuera de consulta. Un punto extremo puede tener llamadas adicionales que no participen en la conferencia y a las que no se aplicará lo especificado en esta cláusula.

8.4.3.8.1 Escenario 1: Conferencia proporcionada por punto extremo

Si el punto extremo A está capacitado, puede "mezclar" la llamada retenida y la llamada consultada en una conferencia con el resultado de una conversación tridireccional entre A, B y C. Para este escenario, el punto extremo A debe tener un MC. Son posibles tanto el modelo de conferencia centralizado como el descentralizado. Si se va a utilizar el modelo centralizado (es decir, si el terminal proporciona la mezcla/conmutación de medios), el punto extremo A deberá tener un MP.

Un punto extremo con MC y MP es de hecho una MCU y deberá utilizar **terminalType** 170, 180 ó 190 según proceda para la determinación de principal-subordinado.

Son posibles los siguientes escenarios:

1a) Si el punto extremo A es el principal de ambas llamadas a B y C, puede simplemente recuperar la llamada retenida en la conferencia con C y proclamarse a sí mismo el MC activo en ambas llamadas a través de la negociación principal-subordinado;

1b) Si el punto extremo A es un subordinado en una o más de las llamadas pero ninguna de las llamadas en las que es el subordinado tiene un MC activo, deberá reiniciar la determinación de principal-subordinado en todas las llamadas en las que es el subordinado utilizando el **terminalType** 240 según se especifica en el cuadro 1 para un MC activo. Si termina el procedimiento como principal en todas las llamadas, deberá actuar según se indica en 1a; si es el subordinado en una o más llamadas, el punto extremo A deberá actuar según se indica a continuación en 1c;

1c) Si una o más de las llamadas en las que el punto extremo A participa es ya una llamada en la que el punto extremo A no es el MC activo, deberán seguirse los procedimientos de puesta en cascada de las MCU.

Una vez establecida la conferencia dentro del punto extremo A, otro punto extremo D, al que está consultando el punto extremo A, puede ser invitado a participar en la conferencia existente según se describe en 8.4.3.2 y 8.4.3.5.

8.4.3.8.2 Escenario 2: Conferencia proporcionada por MCU

Si el punto extremo A tiene acceso a una MCU, deberán aplicarse los procedimientos siguientes para efectuar conferencia fuera de consulta:

2a) El punto extremo A establece una comunicación nueva a la MCU utilizando un mensaje Establecimiento con **conferenceGoal = create** y CID = N;

2b) El punto extremo A cancela su llamada con el punto extremo C utilizando un mensaje Liberación Completa con el **reason** puesto a **replaceWithConferenceInvite** (**sustitución por invitación a conferencia**) incluido el CID de argumento = N.

2c) El punto extremo A envía un mensaje Establecimiento a la MCU con **conferenceGoal = invite**, CID = N e información suficiente para que la MCU efectúe una llamada al punto extremo C (véase también 8.4.3.2).

2d) Los pasos 2b y 2c deberán repetirse con "punto extremo C" sustituido por "punto extremo B". Se señala que no se exige retirar la llamada a B del estado retención antes de invitarle a la conferencia.

2e) Para el intercambio de mensajes relacionados con la conferencia H.245, véanse los pasos C1 a C10 en 8.4.3.2 de H.323.

Mecanismos alternativos a los pasos 2b, 2c y 2d son los siguientes:

1) La transferencia de llamada H.450.2 [34] con el punto extremo A actuando como punto extremo "transferente", los puntos extremos B y C actuando como puntos extremos "transferidos" y el MC/la MCU actuando como punto extremo "al que se transfiere". El mensaje facilidad que contenga **callTransferInitiate Invoke APDU** deberá contener también el CID de elemento = N.

2) El mecanismo "reencaminamiento de mensaje facilidad a MC" H.225.0 (envío de un mensaje facilidad H.225.0 a los puntos extremos B y C conteniendo CID = N, **facilityReason = routeCallToMC** (**motivo de la facilidad = reencaminamiento de llamada MC**) y la dirección de la MCU) si no se soporta el servicio suplementario H.450.2.

Estos mecanismos alternativos se recomiendan si el punto extremo distante está situado en la red con conmutación de circuitos (RCC).

Un punto extremo (por ejemplo, el A) puede retirarse de la conferencia (por ejemplo, poniendo su llamada a la MCU en estado retención). El punto extremo A puede consultar seguidamente con otro punto extremo D que puede ser invitado a continuación a participar en la conferencia existente utilizando los procedimientos descritos en los pasos 2b y 2c anteriores con "punto extremo C" sustituido por "punto extremo D". Se pueden emplear mecanismos alternativos como los descritos más arriba utilizando la transferencia de llamada H.450.2 o el "reencaminamiento de mensaje facilidad a MC" H.225.0.

8.4.4 Servicios suplementarios

El soporte de los servicios suplementarios es opcional. Las Recomendaciones de la serie H.450.x describen un método de proveer servicios suplementarios en el entorno H.323.

8.4.5 Puesta en cascada multipunto

A fin de poner en cascada los MC, debe establecerse una comunicación entre las entidades que contienen los MC. Esta comunicación se establece según los procedimientos definidos en 8.1 y 8.4.3. Una vez establecida la comunicación, y abierto el canal de control H.245, el MC activo (determinado según los procedimientos principal/subordinado de 6.2.8.4) puede activar el MC en una entidad conectada. Esto se efectúa utilizando el mensaje H.245 **remoteMC** (**MC distante**). Se producirán los siguientes resultados en respuesta al mensaje **remoteMC** (**MC distante**):

Entidad llamante	**Entidad llamada**	**Cometido de conferencia**	**Emisor de MC distante**	**Selección de MC distante**	**Resultados**
MC activo	MC inactivo	**crear**	Entidad llamante	**Activación principal** (**masterActivate**)	El MC llamado hace la petición y se convierte en el MC principal
MC activo	MC inactivo	**invitar**	Entidad llamante	**Activación subordinado** (**slaveActivate**)	El MC llamado hace la petición y se convierte en el MC subordinado
MC activo	MC inactivo	**incorporarse**	N/A	N/A	No permitido
MC inactivo	MC activo	**crear**	N/A	N/A	No permitido
MC inactivo	MC activo	**invitar**	N/A	N/A	No permitido
MC inactivo	MC activo	**incorporarse**	Entidad llamada	**Activación subordinado** (**slaveActivate**)	El MC llamante hace la petición y se convierte en el MC subordinado

Una vez que se establece la conferencia en cascada, los MC principales o subordinados pueden invitar a otros puntos extremos a la conferencia. Habrá sólo un MC principal en una conferencia. Un MC subordinado sólo se pondrá en cascada con un MC principal. Los MC subordinados no se pondrán en cascada con otros MC subordinados. Esto permite sólo configuraciones en cascada en haltera o en estrella.

El MC subordinado identificará la conferencia en cascada utilizando el CID establecido por el principal cuando se creó la conferencia.

El MC subordinado aceptará y actuará sobre los mensajes **communicationsModeCommand** procedentes del MC principal. El MC subordinado remitirá estos mensajes a sus puntos extremos localmente conectados. El MC subordinado puede recibir mensajes **requestMode** (**modo petición**) procedentes de sus puntos extremos localmente conectados. Debe remitir éstos al MC principal. El MC subordinado no enviará mensajes **communicationsModeCommand** al MC principal.

El MC principal debe seguir los procedimientos de 8.4.3.2, C3 a C10 a fin de establecer un modo de funcionamiento común con el MC subordinado. Sobre la base de esta información, cada MC es responsable de abrir canales lógicos para la distribución de medios entre sus puntos extremos localmente conectados y puntos extremos designados por el MC principal.

Además de invitar nuevos puntos extremos a la conferencia, un MC que soporte múltiples conferencias puede directamente pasar puntos extremos a otra conferencia sin romper la conexión existente. Si se hace así, el MC debe enviar el mensaje **substituteCID** (**sustituir CID**) a estos puntos extremos. Los puntos extremos que reciben un mensaje **substituteCID** durante una llamada, continuarán utilizando el ID de la conferencia (CID) utilizado en los mensajes RAS anteriores (por ejemplo, ARQ, BRQ, etc.), cuando conversen con su controlador de acceso mientras dure esa llamada.

Las funciones de numeración de terminales y de control de la presidencia pueden seguir los procedimientos definidos en la Rec. UIT-T H.243. La utilización de T.120 en las conexiones en cascada se describe en las Recomendaciones de la serie T.120.

Cuando un principal envía una petición **remoteMC** con la selección **deActivate** (**desactivar**), el MC subordinado debe eliminar de la conferencia todos los puntos extremos.

8.4.6 Pausa y reencaminamiento iniciados por terceras partes

Para los fines de esta cláusula, un conjunto de capacidades vacío se define como un mensaje **terminalCapabilitySet** (**conjunto de capacidades de terminal**) que contiene sólo un número de secuencia y un identificador de protocolo.

Para permitir a los controladores de acceso reencaminar conexiones de puntos extremos que no soportan servicios suplementarios, los puntos extremos responderán a la recepción de un conjunto de capacidades vacío tal como se define en este apartado. Esta capacidad permite a los elementos "de red" tales como centralitas privadas (PBX), centros de llamada y sistemas IVR reencaminar conexiones independientemente de los servicios suplementarios y facilita los anuncios previos a la conexión. También puede utilizarse para demorar el establecimiento de medios H.245 cuando se están utilizando características tales como localización de usuarios por controladores de acceso. También se recomienda encarecidamente que los puntos extremos de la versión 1 soporten esta característica.

Al recibirse un conjunto de capacidades vacío, un punto extremo entrará en un estado "lado transmisor en pausa". Al entrar en este estado, el punto extremo detendrá la transmisión por canales lógicos establecidos, y cerrará todos los canales lógicos que abrió previamente, incluidos los canales lógicos bidireccionales. Cerrará estos canales de la manera ordinaria, es decir, enviando el mensaje **closeLogicalChannel**. El punto extremo no pedirá al punto extremo distante que cierre los canales lógicos, unidireccionales o bidireccionales, que éste abrió. El punto extremo enviará el mensaje **terminalCapabilitySetAck** (**acuse de conjunto de capacidades de terminal**) de la manera ordinaria: el mensaje puede enviarse antes de detener la transmisión, y no se interpretará como una indicación de que se ha detenido la transmisión.

Cuando está en el estado "lado transmisor en pausa", un punto extremo no iniciará la apertura de canales lógicos, pero aceptará la apertura y cierre de canales lógicos desde el extremo distante sobre la base de las reglas ordinarias y continuará recibiendo medios por los canales lógicos abiertos por el extremo distante. Esto permite que los puntos extremos reciban anuncios (por ejemplo, progreso de la llamada preconexión) en la que la entidad anunciante no desea recibir medios del punto extremo. Puede enviarse un mensaje **terminalCapabilitySet** siempre que cambian las capacidades de punto extremo, incluso cuando el punto extremo está en el estado "lado transmisor en pausa". Esto permite establecer comunicación entre dos puntos extremos que inicialmente no declararon capacidades algunas.

Un punto extremo en el estado "lado transmisor en pausa" puede también poner en dicho estado al otro punto extremo de la llamada mediante la transmisión de un mensaje de conjunto de capacidades vacío. Cuando reciba el mensaje de conjunto de capacidades vacío, el receptor se ajustará a los procedimientos definidos en esta cláusula.

Un punto extremo abandonará el estado "lado transmisor en pausa" a la recepción de cualquier mensaje **terminalCapabilitySet**, siempre que no sea un conjunto de capacidades vacío. Al abandonar este estado, un punto extremo reiniciará su estado H.245 a aquel en el que estaba inmediatamente después de efectuarse la conexión de transporte H.245 en el momento de establecimiento de la comunicación (es decir, al comienzo de la fase B), pero preservará la información de estado relativa a cualesquiera canales lógicos que estén abiertos. Esto pone al punto extremo en un estado H.245 conocido después de la pausa, lo cual permite a un punto extremo conectarse a un punto extremo diferente cuando es liberado del estado de pausa.

Después de abandonar el estado "lado transmisor en pausa", un punto extremo proseguirá con procedimientos de señalización de canal lógico abierto normales H.245: tomará parte en la señalización para la determinación principal/subordinado y puede realizar los procedimientos normales de señalización de canal lógico abierto. Cuando un MC abandona el estado "lado transmisor en pausa", actuará como si un nuevo punto extremo se hubiese incorporado a la conferencia.

Si un punto extremo en el estado "lado transmisor en pausa" ya hubiese transmitido un conjunto de capacidades vacío a fin de poner al otro extremo en el mismo estado, se supondrá que sigue en el estado de pausa hasta que reciba un conjunto de capacidades no vacío procedente del otro lado cuando libere al otro punto extremo del estado de pausa. El punto extremo en pausa deberá estar preparado para recibir OLC del otro punto extremo.

A menos que sus capacidades hayan cambiado, un punto extremo no necesita reenviar un conjunto de capacidades, ya que el controlador de acceso lo habrá suministrado al punto extremo distante para eliminar cualquier estado de pausa en el mismo. Esta opción de no enviar un conjunto de capacidades permite una reconexión más rápida. Si el primer mensaje **terminalCapabilitySet** enviado por un punto extremo después de abandonar el estado "lado transmisor en pausa" difiere del conjunto de capacidades que el controlador de acceso proporcionó al punto extremo distante, el controlador de acceso señalará al punto extremo distante que suprime capacidades que no fueron indicadas por el punto extremo iniciador.

NOTA 1 – Un punto extremo debe tener cuidado con las capacidades que envía en este momento. En particular, un punto extremo enviará todas las capacidades que desee para anunciarse y no una pequeña adición a las capacidades previamente señaladas. Además, si el punto extremo tiene tantas capacidades que requiere más de un **terminalCapabilitySet** para señalizarlas, puede haber una ventana de tiempo cuando el controlador de acceso ha eliminado las capacidades descritas en el segundo y posteriores mensajes **terminalCapabilitySet**.

NOTA 2 – Un conjunto de capacidades no vacío no se enviará a un punto extremo hasta que se hayan cerrado todos sus canales lógicos de transmisión. Una entidad de conmutación deberá también enviar un mensaje Facilidad de indicación de redireccionamiento H.450 si el punto extremo está siendo reencaminado.

8.5 Fase E – Terminación de la llamada

Cualquier punto extremo o entidad intermedia de señalización de llamada puede terminar la llamada. La terminación de llamada deberá realizarse de acuerdo con cualquiera de los procedimientos A o B siguientes:

Procedimiento A

A-1) Interrumpir la transmisión de vídeo al final de una imagen completa, en su caso.

A-2) Interrumpir la transmisión de datos, en su caso.

A-3) Interrumpir la transmisión de audio, en su caso.

A-4) Transmitir el mensaje Liberación Completa y cerrar el canal de señalización de llamada H.225.0 y, de estar abierto por separado, el canal de control H.245 sin enviar ningún mensaje H.245. Obsérvese que se supone implícito el cierre de los canales de medios.

A-5) Los puntos extremos deberán liberar la llamada con arreglo a los procedimientos definidos en 8.5.1 u 8.5.2.

Procedimiento B

B-1) Interrumpir la transmisión de vídeo al final de una imagen completa y a continuación cerrar todos los canales lógicos de vídeo, en su caso.

B-2) Interrumpir la transmisión de datos y a continuación cerrar todos los canales lógicos de datos, en su caso.

B-3) Interrumpir la transmisión de audio y a continuación cerrar todos los canales lógicos de audio, en su caso.

B-4) Transmitir el mensaje H.245 **endSessionCommand** por el canal de control H.245, para indicar al extremo distante que desea desconectarse de la llamada, e interrumpir a continuación la transmisión del mensaje H.245.

B-5) Esperar a recibir el mensaje **endSessionCommand** del otro punto extremo y cerrar a continuación el canal de control H.245.

B-6) Transmitir un mensaje Liberación Completa y cerrar el canal de señalización de llamada H.225.0.

B-7) Los puntos extremos deberán liberar la llamada con arreglo a los procedimientos definidos en 8.5.1 u 8.5.2.

Un punto extremo que reciba una **endSessionCommand** sin haberla transmitido primero, realizará los pasos B-1 a B-7 anteriores, con la salvedad de que en el paso B-5 esperará el mensaje **endSessionCommand** procedente del primer punto extremo.

La terminación de una llamada puede no terminar una conferencia; una conferencia puede ser terminada explícitamente utilizando un mensaje H.245 (**dropConference** (**abandonar conferencia**)). En este caso, los puntos extremos esperarán que el MC termine la llamada como se describe anteriormente.

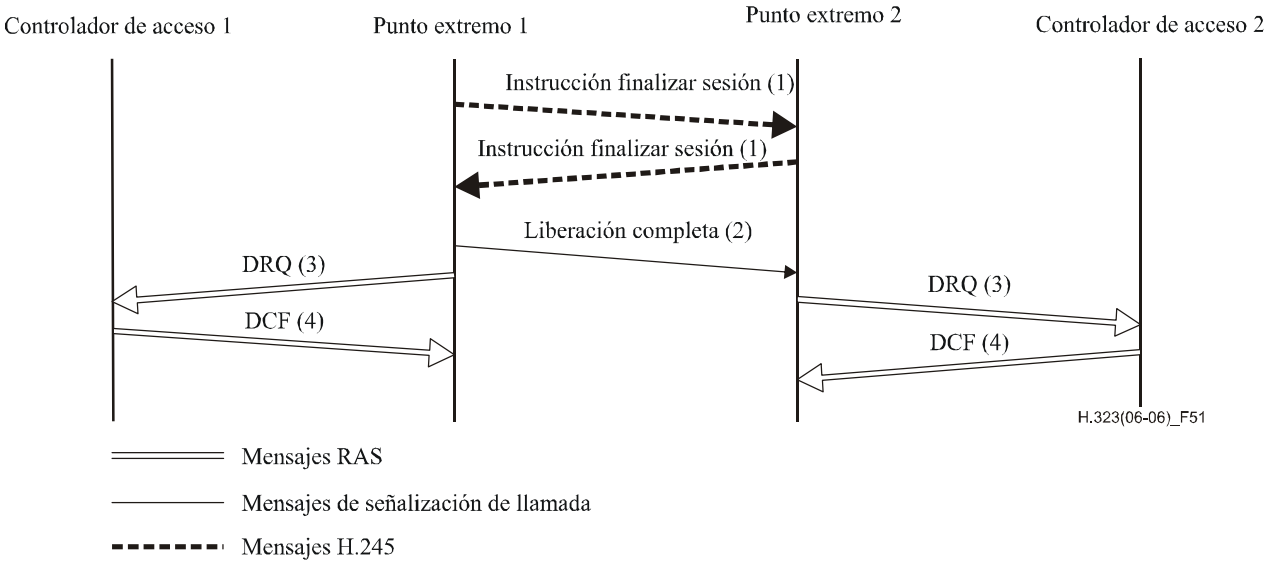
8.5.1 Liberación de la llamada sin un controlador de acceso

En las redes que no contienen un controlador de acceso, después de los pasos A-1 a A-5 o B-1 a B-6 anteriores se termina la llamada. No se requiere ninguna acción ulterior.

8.5.2 Liberación de la llamada con un controlador de acceso

En las redes que contienen un controlador de acceso, no es preciso que el controlador de acceso esté al corriente de la liberación de anchura de banda. Después de ejecutar los pasos A-1 a A-5 o B-1 a B-6 anteriores, cada punto extremo transmitirá un mensaje de petición de deslizamiento (DRQ, *disengage request*) (3) H.225.0 a su controlador de acceso. El controlador de acceso responderá con un mensaje de confirmación de deslizamiento (DCF, *disengage confirm*) (4). Después de enviar el mensaje DRQ, los puntos extremos no enviarán más mensajes IRR no solicitados al controlador de acceso. Véase la figura 51. En este punto la llamada está terminada. La figura 51 muestra el modelo de llamada directa, se sigue un procedimiento similar para el modelo encaminado por el controlador de acceso.

Los mensajes DRQ y DCF serán enviados por el canal RAS.



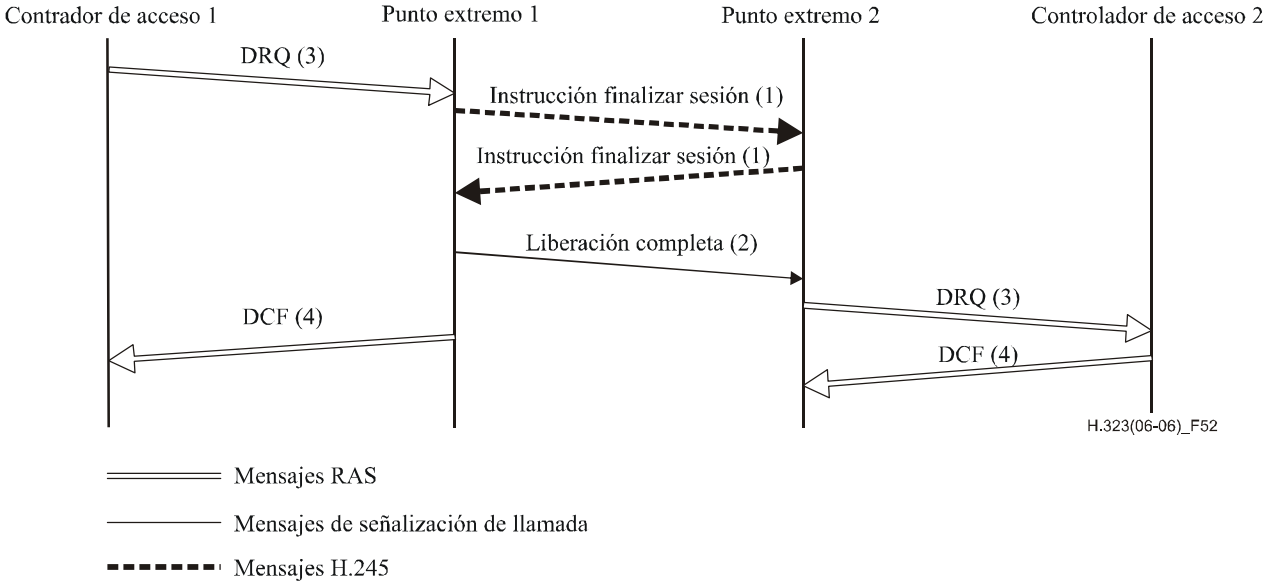
NOTA – El controlador de acceso 1 y el controlador de acceso 2 pueden ser el mismo controlador de acceso.

Figura 51/H.323 – Liberación de llamada iniciada por punto extremo

8.5.3 Liberación de la llamada por el controlador de acceso

El controlador de acceso puede terminar cualquier conferencia enviando un DRQ a un punto extremo (véase la figura 52). El punto extremo seguirá inmediatamente los pasos A-1 a A-5 o B-1 a B-6 anteriores y responderá a continuación al controlador de acceso con un DCF. El otro punto extremo, al recibir la **endSessionCommand** seguirá el procedimiento descrito más arriba. La figura 52 muestra el modelo de llamada directa; se sigue un procedimiento similar para el modelo encaminado por el controlador de acceso.

Si la conferencia es una conferencia multipunto, el controlador de acceso debe enviar un DRQ a cada punto extremo de la conferencia, para cerrar toda la conferencia.



NOTA – El controlador de acceso 1 y el controlador de acceso 2 pueden ser el mismo controlador de acceso.

Figura 52/H.323 – Liberación de llamada iniciada por controlador de acceso

NOTA – El mensaje liberación completa mencionado en la presente cláusula puede, en realidad, ir precedido de otros mensajes H.225.0 como parte del proceso de terminación de la llamada. Por ejemplo, cuando se tuneliza otro protocolo incluido en H.225.0, puede ser necesario intercambiar mensajes tunelizados antes de enviar el mensaje final de liberación completa. Además, como H.245 y H.225.0 pueden operar por conexiones separadas, un mensaje de finalizar sesión H.245 puede llegar antes que un mensaje H.225.0 transmitido previamente. Por ello, las implementaciones no deberán suponer que el mensaje H.225.0 que sigue inmediatamente a la recepción de un mensaje finalizar sesión H.245 será necesariamente una liberación completa.

8.6 Tratamiento de fallo de protocolo

El protocolo fiable subyacente del canal de señalización de llamada H.225.0 y del canal de control H.245 realiza el esfuerzo necesario para entregar y recibir datos por el canal antes de notificar un fallo de protocolo.

En el caso en que una capa de transporte fiable subyacente notifique un fallo, las entidades H.323 operarán de conformidad con el texto de la presente cláusula. Si el anexo R ha sido negociado satisfactoriamente entre dos entidades, la entidad que detecte un fallo deberá intentar recuperar la llamada de conformidad con el procedimiento que se describe en el anexo R.

Dependiendo del encaminamiento del canal de señalización de llamada y del canal de control H.245, bien el controlador de acceso o bien un punto extremo puede detectar el fallo de protocolo. Si el controlador de acceso detecta el fallo, tratará de restablecer el canal de control de llamada. Esto significa que el punto extremo tendrá siempre la posibilidad de establecer un canal en su dirección de transporte de canal de señalización de llamada. El fallo del canal de señalización de llamada no modificará el estado de la llamada. Después del restablecimiento del canal de señalización de llamada, el controlador de acceso puede enviar un mensaje estado preguntando cuál es el estado de la llamada del extremo distante, para asegurarse de que están en sincronismo, independientemente de si emplea o no el anexo R.

Si el punto extremo detecta el fallo, puede optar por terminar la llamada como se describe en la fase E, o intentar el restablecimiento del canal de señalización de llamada como se ha descrito más arriba.

Si durante una llamada un punto extremo desea saber si el otro punto extremo está todavía conectado y funcionando, puede enviar el mensaje de **roundTripDelayRequest** (**petición de retardo de ida y vuelta**) H.245. Puesto que el transporte del canal de control H.245 se realiza un canal fiable, esto dará lugar a una respuesta proveniente del otro punto extremo o a un error de la interfaz de transporte. En este último caso se utilizarán los procedimientos descritos anteriormente. Un punto extremo de una conferencia multipunto puede utilizar el mismo mecanismo; sin embargo, sólo se enterará de si todavía tiene o no una conexión con el MC. Téngase en cuenta que es posible que un punto extremo tenga una conexión libre de errores con el MC pero que permanezca sin recibir audio o vídeo de los demás terminales de la conferencia.

En algunos casos, el fallo del canal de señalización de llamada H.225.0 o del canal de control H.245 pueden no considerarse decisivos para la llamada. En una conversación con voz únicamente, en general no hay señalización entre entidades una vez que la llamada ha sido plenamente establecida, por lo que probablemente los usuarios sólo puedan perder funcionalidades de servicio suplementarias. Una pasarela de la RTPC puede ser capaz de utilizar la información procedente del circuito de la RTPC para determinar, por ejemplo, que existe una actividad vocal entre dos usuarios y que, a pesar de que el canal de señalización de llamada H.225.0 o el canal de control H.245 pueden haber fallado, sigue siendo posible proseguir la llamada y terminarla una vez que la actividad vocal deja de detectarse. El mecanismo utilizado para determinar la finalización de la llamada en esos casos, lo decide la implementación y está fuera del ámbito de esta Recomendación. No se impide a los dispositivos proseguir una llamada en caso de fallo y en ausencia de canales de señalización, si existe una manera de hacerlo. Una vez que el punto extremo ha determinado que la

llamada ha finalizado, los puntos extremos transmitirán un mensaje DRQ al controlador de acceso de la manera habitual.

Si se notifica un fallo de protocolo por el canal de señalización de llamada H.225.0 o por el canal de control H.245, y si no hay ningún medio de recuperar la llamada o proseguirla sin utilizar el canal de señalización de llamada H.225.0 o el canal de control H.245, este último (si está abierto), todos los canales lógicos asociados y el canal de señalización de llamada H.225.0 se cerrarán. Para ello, se seguirán los procedimientos de la fase E, como si el otro punto extremo hubiese emitido la **endSessionCommand** H.245. Esto incluye la transmisión del mensaje DRQ al controlador de acceso y la terminación de la llamada. En el caso en que el MC detecte un fallo en una conferencia multipuntos, el MC enviará mensajes **terminalLeftConference** a los demás terminales.

9 Interfuncionamiento con terminales de otros tipos

El interfuncionamiento con otros terminales se llevará a cabo a través de la pasarela. Véanse 6.3 y la Rec. UIT-T H.246.

9.1 Terminales sólo vocales

El interfuncionamiento con terminales sólo vocales (telefonía) por la RDSI o la RTGC se puede efectuar de las dos maneras siguientes:

1) utilizando una pasarela vocal RDSI-H.323;

2) utilizando una pasarela vocal RTGC-H.323.

La pasarela debe tener en cuenta las siguientes cuestiones:

– Conversión de código de audio:
  - RDSI: si se desea, ya que la RDSI utiliza la codificación G.711.
  - RTGC: de analógico a codificación G.711.

– Conversión de trenes binarios:
  - RDSI: H.225.0 a/de no tramada.
  - RTGC: generación de la H.225.0.

– Conversión de control (generación H.245).

– Conversión de señalización de control de llamada.

– Conversión de tono DTMF a/de mensaje **userInputIndication** H.245 y los tipos de parte útil RTP (descritos en 10.5).

9.2 Terminales de videotelefonía en la RDSI (Rec. UIT-T H.320)

El interfuncionamiento con terminales videotelefónicos en la RDSI (Rec. UIT-T H.320) se puede efectuar de la manera siguiente:

– Utilizando una pasarela H.323-H.320.

La pasarela debe tener en cuenta las siguientes cuestiones:

– Conversión de formato de vídeo (si se desea, H.261 es obligatorio para ambos tipos de terminal).

– Conversión de código de audio (si se desea, G.711 es obligatorio para ambos tipos de terminal).

– Conversión de protocolo de datos.

– Conversión de trenes binarios (H.225.0 a/de H.221).

– Conversión de control (H.245 a/de H.242).

– Conversión de señalización de control de llamada.

– Conversión de número SBE a/de mensaje de **userInputIndication** H.245 y los tipos de parte útil RTP (descritos en 10.5).

9.3 Terminales videotelefónicos en la RTGC (Rec. UIT-T H.324)

El interfuncionamiento con terminales videotelefónicos en la RTGC (Rec. UIT-T H.324) se puede efectuar de las dos maneras siguientes:

1) Utilizando una pasarela H.323-H.324.

2) Utilizando una pasarela H.323-H.320 en el supuesto de que exista una pasarela H.320-H.324 en la red con conmutación de circuitos.

La pasarela debe tener en cuenta las siguientes cuestiones:

– Conversión de formato de vídeo (si se desea, H.261 es obligatorio para ambos tipos de terminal).

– Conversión de protocolo de datos.

– Conversión de código de audio (G.711 es obligatorio para terminal H.323, G.723.1 es obligatorio para terminal H.324).

– Conversión de trenes binarios (H.225.0 a/de H.223).

– Conversión de señalización de control de llamada.

9.4 Terminales videotelefónicos en redes radioeléctricas móviles (Rec. UIT-T H.324/M – anexo C/H.324)

Queda en estudio.

9.5 Terminales videotelefónicos en redes ATM (RAST H.321 y H.310)

El interfuncionamiento con terminales videotelefónicos en redes ATM (terminales H.321 y H.310 RAST que funcionan en el modo de interfuncionamiento H.320/H.321) se puede efectuar de las dos maneras siguientes:

1) Utilizando una pasarela H.323-H.321.

2) Utilizando una pasarela H.323-H.320 en el supuesto de que exista una unidad de interfuncionamiento RDSI/ATM I.580 en la red.

La pasarela debe tener en cuenta las siguientes cuestiones:

– Conversión de formato de vídeo (si se desea, H.261 es obligatorio para ambos tipos de terminal).

– Conversión de protocolo de datos.

– Conversión de código de audio (si se desea, G.711 es obligatorio para ambos tipos de terminal).

– Conversión de trenes binarios (H.225.0 a/de H.221).

– Conversión de control (H.245 a/de H.242).

– Conversión de señalización de control de llamada.

9.6 Terminales videotelefónicos en las LAN con calidad de servicio garantizada (Rec. UIT-T H.322)

El interfuncionamiento con terminales videotelefónicos en LAN con calidad de servicio garantizada (Rec. UIT-T H.322) se puede efectuar de la manera siguiente:

– Utilizando una pasarela H.323-H.320 en el supuesto de que exista una pasarela LAN-RDSI con GQoS en la red.

La pasarela debe tener en cuenta las siguientes cuestiones:

– Conversión de formato de vídeo (si se desea, H.261 es obligatorio para ambos tipos de terminal).
– Conversión de protocolo de datos.
– Conversión de código de audio (si se desea, G.711 es obligatorio para ambos tipos de terminal).
– Conversión de trenes binarios (H.225.0 a/de H.221).
– Conversión de control (H.245 a/de H.242).
– Conversión de señalización de control de llamada.

9.7 Terminales de señales vocales y datos simultáneos en la RTGC (Rec. UIT-T V.70)

El interfuncionamiento con terminales de señales vocales y datos simultáneos en la RTGC (Rec. UIT-T V.70) se puede efectuar de la manera siguiente:

– Utilizando una pasarela H.323-V.70.

La pasarela debe tener en cuenta las siguientes cuestiones:

– Conversión de código de audio (G.711 a/del anexo A/G.729).
– Conversión de protocolo de datos.
– Conversión de trenes binarios (H.225.0 a/de V.76/V.75).
– Conversión de control (ambos terminales utilizan H.245).
– Conversión de señalización de control de llamada.

9.8 Terminales T.120 en la red de paquetes

Un terminal H.323 que tenga la capacidad T.120 deberá poder ser configurado como un terminal sólo T.120 que escucha y transmite en el identificador TSAP conocido T.120 normalizado. De esta manera, el terminal H.323 con capacidad de T.120 podrá participar en conferencias conformes solamente a T.120.

Un terminal de la red que sólo sea conforme con T.120 podrá participar en la porción T.120 de las conferencias H.323 multipunto. Véase 6.2.7.1.

9.9 Pasarela para transporte de medios H.323 en el ATM

Es posible transportar trenes de medios H.323 cuyo origen sean redes del IP no ATM a través de una red ATM utilizando pasarelas H.323 a H.323. Este mecanismo se describe en AF-SAA-0124.000 [32].

10 Mejoras opcionales

10.1 Criptación

La autenticación y la seguridad de los sistemas H.323 es opcional, pero si se introducen, se hará con arreglo a la Rec. UIT-T H.235.0 y a los documentos a los que ésta hace referencia.

10.2 Funcionamiento multipunto

10.2.1 Control e indicación H.243

H.245 contiene mensajes de control e indicación multipunto procedentes de H.243. Estos mensajes pueden utilizarse para proporcionar ciertas capacidades multipunto (como es el control de la presidencia) siguiendo los procedimientos definidos en Rec. UIT-T H.243.

NOTA – La cláusula 15/H.243 contiene orientación para la implementación de estas capacidades utilizando las Recomendaciones de la serie T.120.

10.3 Vinculación de llamadas en H.323

10.3.1 Descripción

La vinculación de llamadas constituye una característica opcional de H.323. En esta cláusula las expresiones en tiempo futuro se interpretarán como un requisito obligatorio, supuesto que se soporta la vinculación de llamadas.

10.3.1.1 Descripción general

La característica identificación de hilo permite que varias llamadas o conexiones de señalización independientes de llamada (las que se mantienen unidas desde el punto de vista del servicio o de la aplicación en lo que se refiere a su progreso) se mantengan vinculadas unas con otras.

La característica identificación global de llamada permite identificar una llamada o una conexión de señalización independiente de la llamada mediante un identificador único aplicable a la llamada o a la conexión de señalización independiente de la llamada extremo a extremo con independencia de su encaminamiento o de su historia.

NOTA – El identificador de llamada se define en 7.5 como un identificador global único de una llamada. Una nueva llamada básica desde el mismo punto extremo o entidad o una nueva llamada que sea parte de un escenario de servicio utilizaría un nuevo valor de identificador de llamada.

10.3.1.2 Definiciones de servicio

10.3.1.2.1 Identificación de hilo (TID, *thread ID*)

Es un valor asignado a llamadas que están vinculadas lógicamente con el propósito de mantener una correlación entre ellas. Si dos o más llamadas se encuentran lógicamente vinculadas (por ejemplo, debido a interacciones de servicios), el ID de hilo vigente de una de dichas llamadas se asigna a las restantes llamadas vinculadas.

10.3.1.2.2 Identificación global de llamada (GID, *global call ID*)

Es un valor asignado a una llamada extremo a extremo para identificar de forma inequívoca dicha llamada en todo su trayecto. Si varias llamadas distintas se transforman en una nueva llamada (debido a interacciones de servicio), los GID de las llamadas anteriores se actualizan (si han sido asignados previamente) o se les asigna un nuevo valor de GID para la nueva llamada extremo a extremo.

NOTA – Una llamada que debido a determinados servicios tenga varios extremos, puede acabar teniendo distintos identificadores de llamada para cada extremo. Por lo tanto, el identificador de llamada no es adecuado para identificar inequívocamente una llamada extremo a extremo.

10.3.2 Invocación y funcionamiento

Cada nueva llamada que se establezca recibirá un nuevo ID de llamada (véase 7.5). Debido a las interacciones entre servicios, pueden asignarse distintos ID de llamada a distintas partes (extremos de la llamada) de una llamada.

El ID global de llamada puede asignarse durante el establecimiento de la comunicación, mientras está en estado activo o mientras está en curso el establecimiento o la liberación de la llamada cuando dos o más llamadas se transforman en una nueva llamada debido a la invocación de determinados servicios o a una petición de aplicación.

El ID global de llamada puede cambiar durante la llamada debido a que ésta se transforme.

El ID de hilo puede asignarse durante el establecimiento de la comunicación, mientras ésta se encuentra en estado activo o mientras está en curso el establecimiento o la liberación de la llamada cuando dos o más llamadas se transforman en una nueva llamada debido a la invocación de algunos servicios o a una petición de aplicación.

El ID de hilo puede cambiar durante la duración de la llamada (por ejemplo, debido a interacciones entre servicios).

10.3.3 Interacción con servicios suplementarios H.450

En las subcláusulas siguientes se especifican las interacciones con los servicios suplementarios H.450 para los que existen normas en el momento de publicación de esta Recomendación.

Puesto que un ID de llamada es único para cada nueva llamada, no son de aplicación interacciones con otros servicios suplementarios. Todas las interacciones descritas en esta cláusula se aplican exclusivamente al ID global de llamada, al ID de hilo o a ambos.

El ID global de llamada y el ID de hilo se asignan durante el establecimiento de la comunicación básica con independencia de la invocación de servicios suplementarios realizada. A continuación se describen características de las interacciones para la invocación de servicios suplementarios específicos.

10.3.3.1 Transferencia de llamada

En esta cláusula se describe la utilización de los campos de vinculación de llamada cuando se utiliza H.450.2.

10.3.3.1.1 Transferencia sin consulta

El ID de hilo de la llamada transferida se heredará del ID de hilo de la llamada primaria. Por lo tanto, el punto extremo transferente proporcionará el ID de hilo de la llamada primaria al punto extremo transferido junto con la petición de transferencia de llamada. Si la llamada primaria no tiene un ID de hilo asignado, el punto extremo transferente generará uno. Si la entidad transferida no recibe un ID de hilo junto con la petición de transferencia de llamada, heredará el ID de hilo que se asignó a la comunicación primaria durante su establecimiento. Si no existe ningún ID de hilo disponible que heredar, el punto extremo transferido generará un ID de hilo y lo asignará a la llamada transferida (en el mensaje de establecimiento de comunicación) y a la llamada primaria (en el mensaje de liberación de llamada).

Una llamada transferida recibirá la asignación de un nuevo ID global de llamada. Si un controlador de acceso establece la comunicación transferida en nombre de un punto extremo transferido, el controlador de acceso asignará el mismo ID global de llamada a la ramificación de llamada restante de la llamada primaria. Ello garantiza que la llamada resultante después de una transferencia exitosa tenga un único GID extremo a extremo.

10.3.3.1.2 Transferencia con consulta

Durante la transferencia, la llamada transferida recibirá la asignación del mismo ID de hilo que la llamada primaria anterior si:

a) la llamada primaria es una llamada entrante y la llamada secundaria en una llamada saliente; o

b) ambas son llamadas entrantes y la comunicación primaria se ha establecido antes que la llamada secundaria; o

c) ambas son llamadas salientes y la comunicación primaria se ha establecido antes que la llamada secundaria.

Durante la transferencia, la llamada transferida recibirá la asignación del mismo ID de hilo que la llamada secundaria anterior si:

a) la llamada secundaria es una llamada entrante y la llamada primaria en una llamada saliente; o

b) ambas son llamadas entrantes y la comunicación secundaria se ha establecido antes que la llamada primaria; o

c) ambas son llamadas salientes y la comunicación secundaria se ha establecido antes que la llamada primaria.

El ID de hilo adecuado para la llamada transferida (basada en la llamada primaria o en la secundaria, según sea el estado) será proporcionado por el punto extremo transferente al punto extremo transferido junto con la petición de transferencia de llamada. Si la llamada desde la que se hereda el ID de hilo (llamada primaria o secundaria) no tiene asignado un ID de hilo, el punto extremo transferente generará uno. Si el punto extremo transferido no recibe un ID de hilo junto con la petición de transferencia de llamada (es decir, el punto extremo transferente no soporta la vinculación de llamada) generará un ID de hilo que será heredado de la llamada primaria, si ello es posible.

Cuando se realiza la transferencia, la entidad transferida asignará un nuevo valor de GID a la llamada transferida. Si un controlador de acceso ha establecido la comunicación transferida en nombre del punto extremo transferido, el controlador de acceso asignará el mismo GID a los restantes extremos de llamada de la llamada primaria. Un controlador de acceso que actúe en nombre del punto extremo al que se realiza la transferencia asignará el mismo GID a la parte restante de la llamada secundaria. Ello asegura que la llamada resultante después de la transferencia exitosa tiene un GID único extremo a extremo.

Una entidad transferente puede, opcionalmente, "agrupar" la llamada primaria y la llamada secundaria. Las reglas de vinculación de llamada para la llamada resultante (llamada "agrupada") será la misma que la arriba especificada para una llamada transferida.

10.3.3.2 Desviación de llamada

En esta cláusula se describe la utilización de los campos de vinculación de llamada cuando se utiliza lo especificado en la Rec. UIT-T H.450.3 [39].

La llamada de origen, la llamada que realiza el reenvío y la llamada reenviada utilizarán el mismo ID de hilo.

El ID de hilo de la llamada reenviada y de la llamada originaria será heredado del ID de hilo de la llamada que realiza el reenvío. Por lo tanto, el punto extremo servido asignará un ID de hilo a la llamada que realiza el reenvío (si no se ha asignado ya como parte de la llamada básica) y proporcionará este ID de hilo a la entidad que realiza el reencaminamiento junto con la petición de reenvío de llamada. La entidad reencaminadora utilizará este ID de hilo como ID de hilo para el establecimiento de la comunicación reenviada. Además, dicho ID de hilo será asignado/actualizado al extremo de llamada de origen (si existe).

Si la entidad reencaminadora no recibe un ID de hilo junto con la petición de reenvío de llamada, heredará el ID de hilo que hubiese sido asignado a la llamada que realiza el reenvío durante el establecimiento de la comunicación. Si no existe disponible ningún ID de hilo que pueda ser heredado, el punto extremo reencaminador generará un ID de hilo y lo asignará a la llamada que realiza el reenvío, a la llamada reenviada y a la llamada de origen.

En el establecimiento de la comunicación se asignará un nuevo GID a la llamada extremo a extremo desde el usuario llamante (es decir, el usuario desviado) al usuario hacia el que se realiza el desvío mediante la asignación de un nuevo GID en el establecimiento de la comunicación desviada y asignando (o actualizando) el mismo GID al extremo de llamada origen (si existe).

10.3.3.3 Retención de llamada y llamada de consulta

En esta cláusula se describe la utilización de los campos de vinculación de llamadas cuando se utiliza lo especificado en la Rec. UIT-T H.450.4.

Una llamada de consulta utilizará el mismo ID de hilo que la primera llamada.

NOTA – Es el punto extremo quien decide si una llamada es una llamada de consulta o una llamada básica adicional.

Una llamada de consulta utilizará un nuevo ID global de llamada.

10.3.3.4 Depósito de llamada/extracción de llamada

En esta cláusula se describe la utilización de los campos de vinculación de llamada cuando se utiliza lo especificado en la Rec. UIT-T H.450.5 [40].

La llamada en depósito tendrá el mismo ID de hilo que la llamada primaria, sin embargo, utilizará un GID diferente.

Si está disponible, el ID de hilo se utilizará para la asociación de conexiones de señalización independientes de la llamada (indicando notificaciones de grupo y peticiones de extracción), para la llamada del usuario llamante/depositado al usuario extractor, y para una llamada previamente avisada/depositada.

NOTA – El depósito/extracción de llamada contiene un identificador de extracción de llamada específico que es utilizado por el usuario extractor.

Las conexiones de señalización independientes de la llamada utilizadas como parte del depósito o extracción de la llamada utilizarán nuevos GID. La llamada del usuario llamante/usuario depositado al usuario extractor tendrá un nuevo GID global extremo a extremo.

10.3.3.5 Llamada en espera

No existe interacción entre la vinculación de llamada y la Rec. UIT-T H.450.6 [41].

10.3.3.6 Indicación de mensaje en espera

No existe interacción entre la vinculación de llamada y la Rec. UIT-T H.450.7 [42].

10.3.3.7 Servicio de identificación de nombre

No existe interacción entre la vinculación de llamada y la Rec. UIT-T H.450.8 [43].

10.4 Tunelización de mensajes de señalización no H.323

A fin de soportar en un sistema H.323 la información de señalización no H.323 existente, es necesario permitir el transporte de información de señalización no H.323 en sistemas H.323. En esta cláusula se presenta una forma genérica de tunelización de mensajes de señalización en un mensaje de control de llamada H.225.0.

Los procedimientos de esta cláusula se aplican a cualquier tipo de punto extremo. Los túneles de señalización se terminan en una entidad lógica denominada una "terminación de túnel". Típicamente, estas terminaciones de túneles se localizan en pasarelas que interconectan partes de una red no H.323 con una red H.323 tal como se muestra en la figura 53. Si en la red H.323 existe un controlador de acceso, éste puede participar en la tunelización de señalización no H.323.

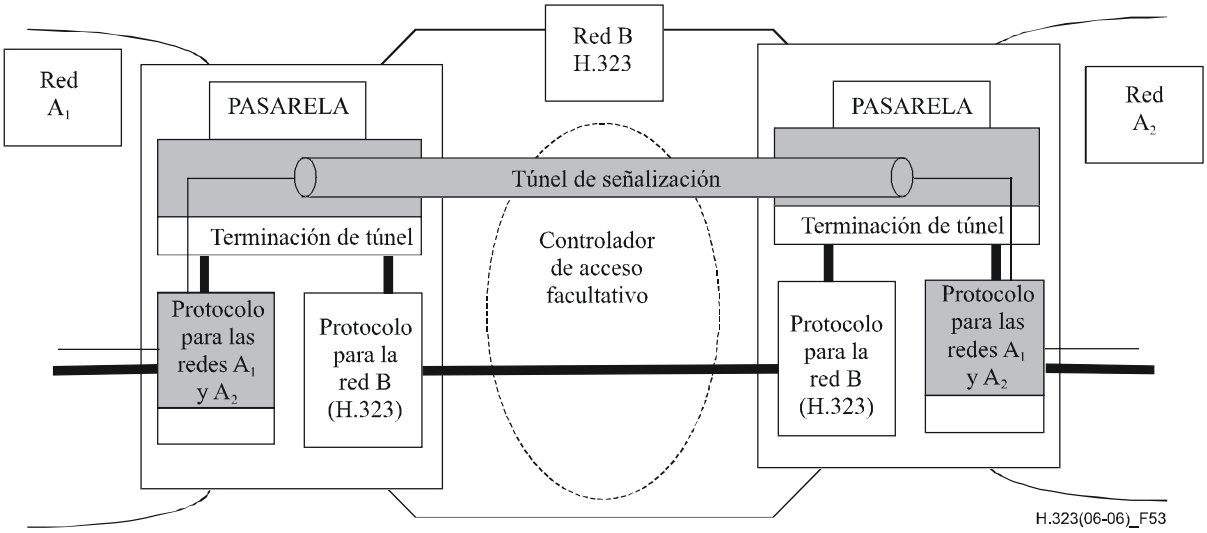


Figura 53/H.323 – Tunelización de señalización entre pasarelas

En algunos casos, la terminación del túnel puede estar localizada en un controlador de acceso, tal como se ilustra en la figura 54. En 10.4.2 se describe cómo interviene un controlador de acceso en un túnel.

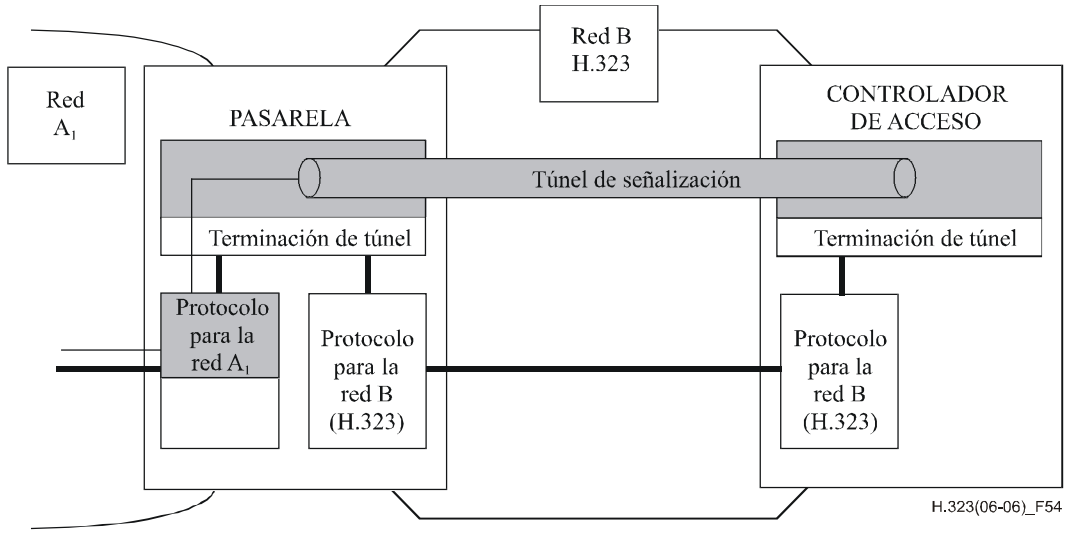


Figura 54/H.323 – Tunelización de señalización entre una pasarela y una terminación de túnel en un controlador de acceso

Los estados y procedimientos del control de llamada del protocolo tunelizado son diferentes de los estados y procedimientos de control de llamada del protocolo H.225.0: un punto extremo que soporte la señalización tunelizada debe ser capaz de distinguir ambos.

Cualquier protocolo de señalización puede ser tunelizado y se identifica mediante el **TunnelledProtocol** (**protocolo tunelizado**). Algunos ejemplos de protocolos de señalización que pueden ser tunelizados son los siguientes:

- QSIG.
- PU-RDSI.
- DSS1 RDSI.
- DPNSS.
- Protocolo de red PBX propietario.

10.4.1 Indicación del soporte de protocolos tunelizados

Los protocolos que pueden tunelizarse se enumeran de forma priorizada en el campo **supportedTunnelledProtocols** (**protocolos tunelizados soportados**) de **EndpointType** (**tipo punto extremo**). Es una lista priorizada de protocolos que pueden ser tunelizados.

Cuando un punto extremo se registra ante su controlador de acceso, puede indicar los protocolos tunelizados que soporta en GRQ y en RRQ como parte del **EndpointType**. El **EndpointType** contiene una lista priorizada de los protocolos tunelizados soportados, siendo el primero de ellos el preferido. En la ACF o LCF que un controlador de acceso devuelve en respuesta a una ARQ o una LRQ, el **destinationType** indica los protocolos de señalización tunelizados que soporta el destino, también en forma de lista priorizada. Puesto que el anexo G/H.225.0 importa la secuencia **EndpointType**, esta capacidad puede asimismo ser transportada utilizando lo indicado en el anexo G/H.225.0.

Un punto extremo origen que desee indicar los protocolos de señalización que puede tunelizar, incluirá la lista priorizada en la **sourceInfo.supportedTunnelledProtocols** (**información de la fuente.protocolos tunelizados soportados**) del mensaje Establecimiento. Un punto extremo de terminación que desee indicar los protocolos de señalización que puede tunelizar, incluirá la lista priorizada **destinationInfo.supportedTunnelledProtocols** (**información del destino.protocolos tunelizados soportados**) en todos los mensajes que incluyan el campo **destinationInfo** (**información del destino**) que envía en respuesta al mensaje Establecimiento. Si un punto extremo origen no recibe esta indicación, considera que el punto extremo de terminación no soporta ningún protocolo tunelizado.

10.4.2 Solicitud de un túnel de protocolo específico a un controlador de acceso

Una entidad puede solicitar a un controlador de acceso un túnel de protocolo determinado especificando el protocolo particular en el campo **desiredTunnelledProtocol** (**protocolo tunelizado deseado**) en un ARQ o LRQ.

10.4.3 Tunelización de un protocolo de señalización en mensajes de señalización de llamada H.225.0

Un punto extremo puede tunelizar un protocolo de señalización incluyendo el **tunnelledSignallingMessage** (**mensaje de señalización tunelizada**) en cualquier mensaje de señalización de llamada H.225.0. Sin embargo, no es recomendable tunelizar un protocolo de señalización en un mensaje de señalización de llamada H.225.0 que no tenga un significado extremo a extremo, tal como el mensaje llamada en curso, puesto que la información puede no ser recibida en el otro extremo.

Si un punto extremo sólo permite que la llamada se curse si se soporta la tunelización, incluirá la bandera **tunnellingRequired** (**tunelización requerida**) en el mensaje Establecimiento; la bandera **tunnellingRequired** no se incluirá en ningún otro mensaje que no sea el de establecimiento. Si un punto extremo recibe un **tunnelledSignallingMessage** con la bandera **tunnellingRequired** fijada en el mensaje Establecimiento y no puede tunelizar el protocolo, terminará la llamada enviando una Liberación Completa cuyo **reason** sea **tunnelledSignallingRejected** (**señalización tunelizada**

rechazada); una bandera **tunnellingRequired** incluida en cualquier otro mensaje distinto a establecimiento será ignorada.

La información de protocolo tunelizada se incluye en el campo **messageContent** (**contenido de mensaje**) y el campo **tunnelledProtocolID** (**identificador de protocolo tunelizado**) identifica el protocolo tunelizado. En una llamada H.323 sólo puede ser tunelizado un único protocolo. En un único mensaje de señalización de llamada H.225.0 pueden agregarse múltiples mensajes tunelizados del mismo protocolo.

El túnel será liberado utilizando los procedimientos normales de liberación H.323.

Los procedimientos de señalización de llamada H.225.0 pueden utilizarse para establecer una conexión de señalización independiente de la llamada entre puntos extremos pares. La tunelización puede utilizarse en este contexto a fin de proporcionar señalización independiente del portador para el protocolo tunelizado. En este caso, no se necesita ningún canal de control H.245 ni canales de medios. En el mensaje Establecimiento H.225.0 debería incluirse un elemento de información de capacidad de portador tal como se describe en el cuadro 2/H.450.1. El mensaje Establecimiento utilizado en los procedimientos de señalización independientes de la llamada incluirá un campo **conferenceGoal** cuyo valor está fijado en **callIndependentSupplementaryService**. Estos procedimientos de conexión de señalización independientes de la llamada para la tunelización no se utilizarán conjuntamente con un servicio suplementario H.450 en la misma conexión de señalización independiente de la llamada.

10.4.4 Consideraciones sobre el controlador de acceso

En un modelo de llamadas encaminadas directamente, el controlador de acceso no está implicado en la señalización de control de llamada H.225.0 y, por lo tanto, no realiza la tunelización de señalización en H.225.0. Dichos controladores de acceso no afectan a la tunelización entre dos puntos extremos que soporten la tunelización de señalización. En el modelo de encaminamiento por el controlador de acceso, éste participa en la provisión de un túnel entre los puntos extremos pares pasando la información de señalización tunelizada recibida. El controlador de acceso también puede utilizar los mensajes facilidad o progreso para transportar mensajes tunelizados, tal como se expone en 8.2.2.

En el modelo de encaminamiento por el controlador de acceso, éste puede interceptar y actuar sobre los mensajes de señalización tunelizados. La terminación de un túnel de señalización se realiza mediante una función de terminación de túnel que, tal como se ha descrito anteriormente, puede estar localizada en el controlador de acceso. Lo que el controlador de acceso hace con el protocolo tunelizado queda fuera del alcance de esta Recomendación. Sin embargo, si el controlador de acceso puede proporcionar servicio de señalización no H.323, puede terminar el túnel de señalización y generar los mensajes H.225.0 apropiados para los puntos extremos de la llamada. Alternativamente, puede modificar la información de señalización tunelizada: si así lo hace, es asumiendo la responsabilidad de terminar e iniciar el protocolo tunelizado. Un controlador de acceso que no entienda el protocolo tunelizado o que no pretenda actuar sobre el protocolo tunelizado o proporcionar servicio alguno en dicho plano, pasará el mensaje de señalización tunelizado inalterado para preservar la integridad del protocolo tunelizado.

10.5 Utilización de la cabida útil RTP para cifras DTMF, tonos de telefonía y señales telefónicas

Es posible llevar tonos DTMF, tonos relacionados con el facsímil, tonos de línea de abonado normalizados, tonos específicos del país y eventos troncales utilizando un tipo diferente de cabida útil RTP dinámica en el mismo tren RTP que los medios. Muchas aplicaciones, por ejemplo sistemas IVR y sistemas vocales, se basan en la sincronización de la entrada DTMF.

RFC 2833 [56] describe la manera de transportar esos tonos y eventos con el RTP. Un punto extremo puede indicar que soporta la recepción de los tonos y eventos de RFC 2833 incluyendo la **receiveRTPAudioTelephonyEventCapability** (**capacidad de recepción de evento telefónico de audio RTP**) o la **receiveRTPAudioToneCapability** (**capacidad de recepción de tono de audio RTP**) en el conjunto de capacidades del terminal. Alternativamente, un punto extremo puede indicar que soporta los tonos y eventos RFC 2833 incluyendo el **audioTelephonyEvent** o el **audioToneAudioCapability** en el conjunto de capacidades del terminal. Cuando se utilicen procedimientos de conexión rápida, estas capacidades podrán enviarse utilizando los procedimientos parallelH245 de 8.2.4.

Los eventos telefónicos nombrados son una descripción lógica de los tonos DTMF, los tonos relacionados con el facsímil, el tono de línea de abonado normalizados, los tonos específicos del país y los eventos troncales. Un número decimal identifica a cada evento. Cuando se utilizan eventos telefónicos, es obligatorio el soporte de las siguientes DTMF: 0-9, #, *, A, B, C, D. Todas las demás son facultativas.

Los tonos de telefonía son una descripción de las propiedades de la forma de onda, lo que resulta de utilidad cuando es necesario reproducir exactamente tonos no normalizados.

Una vez abierto un canal lógico para el tren de medios, el emisor puede enviar cualquiera de los eventos o tonos de telefonía anunciados por el receptor en el conjunto de capacidades del terminal por el mismo canal lógico utilizando el tipo de cabida útil RTP negociado en la negociación del conjunto de capacidades de los terminales.

Si un punto extremo envía información de DTMF, el envío puede efectuarlo en una **UserInputIndication** y/o utilizando cabida útil RTP para las cifras de DTMF, los tonos de telefonía y las señales telefónicas.

Si la DTMF se envía tanto vía RTP como en una **UserInputIndication** en forma alfanumérica, deberá codificarse en la estructura **extendedAlphanumeric** (**alfanumérica ampliada**), y deberá incluirse el campo **rtpPayloadIndication** (**indicación de cabida útil RTP**). Si la DTMF se envía tanto vía RTP como en una **UserInputIndication** en la forma de señal, deberá incluirse el campo **rtpPayloadIndication** en la estructura de la **signal** (**señal**). Si la DTMF se envía solamente en forma alfanumérica, deberá codificarse en el campo **alphanumeric** (**alfanumérico**). Si la DTMF se envía solamente en forma de señal, no se incluirá el campo **rtpPayloadIndication**.

En los sistemas H.323 no se utilizará RFC 2833 para retransmitir información de facsímil. Por el contrario, deberán seguirse los procedimientos definidos en el anexo D en el caso de puntos extremos que deseen transmitir información de facsímil T.38.

NOTA – Las entidades H.323 anteriores a la versión 4 no tenían la capacidad de enviar información de DTMF vía RTP que se describe en esta cláusula. Por ello, todas las entidades deberán soportar la posibilidad de envío de información de DTMF mediante el mensaje **UserInputIndication**.

11 Mantenimiento

11.1 Bucles para fines de mantenimiento

En la Rec. UIT-T H.245 se definen ciertas funciones de bucle que permiten la verificación de algunos aspectos funcionales del terminal y asegurar un funcionamiento correcto del sistema y una calidad de servicio satisfactoria a la parte distante.

La petición **systemLoop** (**bucle de sistema**) y la petición **logicalChannelLoop** (**bucle de canal lógico**) no deberán ser utilizadas. La petición **mediaLoop** (**bucle de medios**) es opcional. Un punto extremo que reciba la **maintenanceLoopOffCommand** (**instrucción desconexión de bucle de mantenimiento**) desconectará todos los bucles existentes en ese momento.

En relación con los bucles, se definen dos modos:

a) Modo funcionamiento normal: Ningún bucle. Se indica en **a** en la figura 55. Éste será el modo por defecto y el modo al que se pasará cuando se reciba la **maintenanceLoopOffCommand**.

b) Modo bucle de medios: Bucle de tren de medios en la interfaz analógica de entrada/salida. Al recibirse la petición **mediaLoop** definida en la Rec. UIT-T H.245, se activará tan pronto como sea posible el bucle del contenido del canal lógico seleccionado a la interfaz analógica del códec vídeo/audio hacia el códec vídeo/audio, de tal manera que se ponga en bucle el contenido de los medios codificados y recodificados, como se indica en **b** de la figura 55. Este bucle es opcional. Sólo deberá utilizarse cuando se abra en cada sentido un canal lógico único que contenga el mismo tipo de medios. No está definido el funcionamiento cuando se abren múltiples canales en el sentido de retorno.

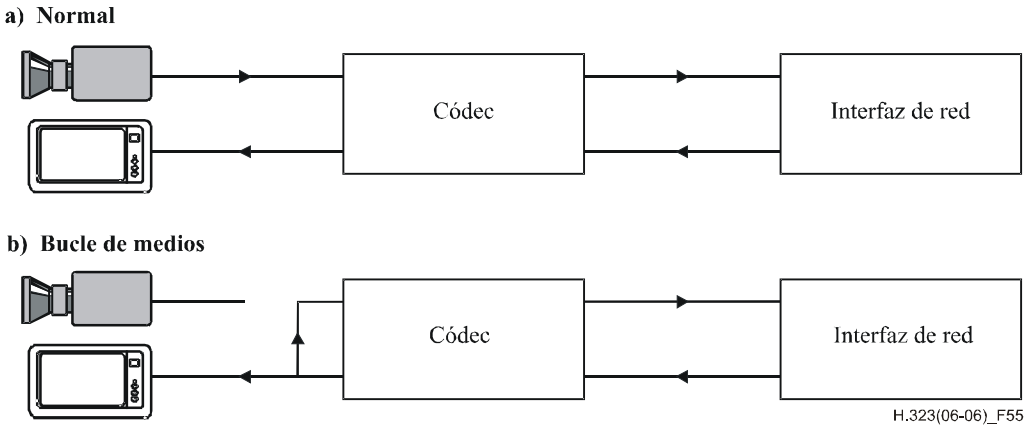


Figura 55/H.323 – Bucles

Una pasarela hacia H.324 que recibe una petición **systemLoop** H.245 o una petición **logicalChannelLoop** H.245, o bien una pasarela hacia H.320, H.321 o H.322 que recibe una instrucción de bucle digital H.230 procedente de un punto extremo de RCC puede efectuar la función de bucle apropiada dentro de la pasarela. La pasarela no pasará estas peticiones al punto extremo de red. Una pasarela hacia H.324, que reciba una petición **mediaLoop** H.245 procedente de un punto extremo de RCC pasará la petición al punto extremo de red. Una pasarela a H.320, H.321 o H.322 que reciba una instrucción bucle de vídeo o bucle de audio H.230 procedente de un punto extremo de RCC la convertirá en la petición **mediaLoop** H.245 apropiada y la enviará al punto extremo de red.

Una pasarela hacia H.320, H.321 o H.322 que reciba una petición **mediaLoop** H.245 procedente de un punto extremo de red la convertirá en la instrucción bucle de vídeo o bucle de audio H.230 apropiada y la enviará al punto extremo de RCC.

Una pasarela hacia H.324 puede enviar una petición **systemLoop** H.245 o una petición **logicalChannelLoop** H.245 al punto extremo de RCC. Una pasarela hacia H.320, H.321 o H.322 puede enviar una instrucción bucle digital H.230 al punto extremo de RCC. Si un punto extremo de red está en una llamada al punto extremo de RCC, el audio y el vídeo enviados al punto extremo de red pueden ser el audio o vídeo puestos en bucle, un mensaje de audio o vídeo pregrabado indicando la condición de bucle o no ser audio ni vídeo.

11.2 Métodos de supervisión

Todos los terminales deberán soportar el mensaje de petición de información/respuesta a petición de información (IRQ/IRR) de la Rec. UIT-T H.225.0. El mensaje de respuesta a petición de información contiene el identificador de TSAP de todos los canales que en un momento dado están activos en la llamada, incluyendo los de control T.120 y H.245, así como los de audio y vídeo. Esta información puede ser utilizada por dispositivos de mantenimiento de tercera parte de supervisión de conferencias H.323 para verificar el funcionamiento del sistema.

Anexo A

Mensajes H.245 utilizados por puntos extremos H.323

Las reglas que siguen se aplican a la utilización de mensajes H.245 por puntos extremos H.323:

- Un punto extremo no deberá funcionar impropiamente o, de otro modo, resultar afectado de manera adversa por la recepción de mensajes H.245 que no reconozca. Cuando un punto extremo reciba una petición, respuesta o instrucción no reconocida devolverá "función no soportada". (Esto no se requiere para indicaciones.)
- En los cuadros A.1 a A.12 se utilizan las abreviaturas siguientes:

  M Obligatorio (*mandatory*).

  O Opcional (*optional*).

  F Prohibido transmitir (*forbidden to transmit*).
- Un mensaje señalado como obligatorio para el punto extremo receptor indica que el punto extremo aceptará el mensaje y realizará la acción procedente. Un mensaje señalado como obligatorio para el punto extremo transmisor indica que el punto extremo generará el mensaje en las circunstancias apropiadas.

Cuadro A.1/H.323 – Mensajes de determinación principal-subordinado

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Determinación	M	M
Acuse de determinación	M	M
Rechazo de determinación	M	M
Liberación de determinación	M	M

Cuadro A.2/H.323 – Mensajes de capacidad de terminal

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Conjunto de capacidades	M	M
Acuse de conjunto de capacidades	M	M
Rechazo de conjunto de capacidades	M	M
Liberación de conjunto de capacidades	M	M

Cuadro A.3/H.323 – Mensajes de señalización de canal lógico

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Apertura de canal lógico	M	M
Acuse de apertura de canal lógico	M	M
Rechazo de apertura de canal lógico	M	M
Confirmación de apertura de canal lógico	M	M
Cierre de canal lógico	M	M
Acuse de cierre de canal lógico	M	M
Petición de cierre de canal	M	O
Acuse de petición de cierre de canal	O	O
Rechazo de petición de cierre de canal	O	M
Liberación de petición de cierre de canal	O	M

Cuadro A.4/H.323 – Mensajes de señalización del cuadro múltiplex

Mensaje	Estado
Envío de inscripción múltiplex	F
Acuse de envío de inscripción múltiplex	F
Rechazo de envío de inscripción múltiplex	F
Liberación de envío de inscripción múltiplex	F

Cuadro A.5/H.323 – Mensajes de petición de señalización del cuadro múltiplex

Mensaje	Estado
Petición de inscripción múltiplex	F
Acuse de petición de inscripción múltiplex	F
Rechazo de petición de inscripción múltiplex	F
Liberación de petición de inscripción múltiplex	F

Cuadro A.6/H.323 – Mensajes de petición de modo

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Petición de modo	M	O
Acuse de petición de modo	M	O
Rechazo de petición de modo	O	M
Liberación de petición de modo	O	M

Cuadro A.7/H.323 – Mensajes de retardo de ida y vuelta

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Petición de retardo de ida y vuelta	M	O
Respuesta de retardo de ida y vuelta	O	M

Cuadro A.8/H.323 – Mensajes de bucle de mantenimiento

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Petición de bucle de mantenimiento		
Bucle de sistema	F	F
Bucle de medios	O (nota)	O (nota)
Bucle de canal lógico	F	F
Acuse de bucle de mantenimiento	O	O
Rechazo de bucle de mantenimiento	O	M
Desconexión de bucle de mantenimiento	M	O
NOTA – Obligatorio en las pasarelas.		

Cuadro A.9/H.323 – Mensajes de petición y respuesta de conferencia

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Petición de lista de terminales	O	O
Exclusión de terminal	O	O
Cédame la presidencia	O	O
Cancelación de "Cédame la presidencia"	O	O
Introduzca contraseña H.243	O	O
Introduzca ID de terminal H.243	O	O
Introduzca ID de conferencia H.243	O	O
Petición de ID de terminal	O	O
Respuesta de ID de terminal	O	O
Respuesta de ID de terminal MC	O	O
Introduzca dirección de extensión	O	O
Introduzca respuesta de dirección	O	O
Respuesta de lista de terminales	O	O
Respuesta a "Cédame la presidencia"	O	O
Respuesta de ID de conferencia	O	O
Respuesta de contraseña	O	O

Cuadro A.10/H.323 – Instrucciones

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Enviar conjunto de capacidades del terminal	M	M
Criptación	O	O
Control del flujo	M	O
Finalizar sesión	M	M
Instrucciones varias		
Ecualización de retardo	O	O
Ausencia de retardo	O	O
Instrucción modo multipunto	M	O
Cancelación de instrucción modo multipunto	M	O
Congelación de imagen de vídeo	M	O
Actualización rápida de imagen de vídeo	M	O
Actualización rápida de GOB de vídeo	M	O
Actualización rápida de MB de vídeo	M	O
Equilibrado de la resolución espacial-temporal de vídeo	O	O
Envío de sincronización de vídeo en cada GOB	O	O
Cancelación del envío de sincronización de vídeo en cada GOB	O	O
Petición de ID de terminal	O	O
Rechazo de instrucción vídeo	O	O
Respuesta a "Cédame presidencia"	O	O
Instrucciones de conferencia		
Difúndame mi canal lógico	O	O
Cancelación de "Difúndame mi canal lógico"	O	O
Ponga al terminal en difusor	O	O
Cancelación de "Ponga al terminal en difusor"	O	O
Envíe esta fuente	O	O
Cancelar "Envíe esta fuente"	O	O
Abandonar conferencia	O	O

Cuadro A.11/H.323 – Instrucciones del modo conferencia

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Instrucción modo de comunicación	M	O
Petición de modo de comunicación	O	O
Respuesta de modo de comunicación	O	O

Cuadro A.12/H.323 – Instrucciones

Mensaje	Estado en el punto extremo receptor	Estado en el punto extremo transmisor
Función no entendida	M	M
Función no soportada	M	M
Indicaciones varias		
Canal lógico activo	O	O
Canal lógico inactivo	O	O
Conferencia multipunto	M	O
Cancelación de conferencia multipunto	M	O
Indicación multipunto de ausencia de comunicación	O	O
Cancelación de indicación multipunto de ausencia de comunicación	O	O
Indicación multipunto de estado secundario	O	O
Cancelación de indicación multipunto de estado secundario	O	O
Indicación de vídeo preparado para activación	O	O
Indicación de vídeo sobre compromiso resolución temporal-espacial	O	O
MB de vídeo no decodificados	O	O
Indicaciones de la conferencia		
Número SBE	O	O
Asignación de número de terminal	M	O
El terminal se incorporó a conferencia	O	O
El terminal abandonó la conferencia	O	O
Visto al menos por otro	O	O
Cancelación de "Visto al menos por otro"	O	O
Visto por todos	O	O
Cancelación de "Visto por todos"	O	O
Terminal que está usted viendo	O	O
Petición de la palabra	O	O
Indicaciones del vendedor	O	O
Indicación de ubicación del MC	M	O
Indicación de fluctuación de fase	O	O
Indicación de asimetría H.223	F	F
Indicación de asimetría máxima H.225.0	O	M
Indicación de nuevo canal virtual ATM	F	F
Entrada de usuario	M (para 0-9, * y #)	M (para 0-9, * y #)

Se permiten instrucciones, peticiones, etc., no normalizadas.

Anexo B

Procedimientos para los códecs vídeo por capas

B.1 Alcance

Este anexo describe mejoras en el marco de la especificación H.323, para incorporar los códecs vídeo por capas. El procedimiento descrito es escalable para conferencias multipunto.

B.2 Introducción

La codificación vídeo por capas es una técnica que permite que la información vídeo se transmita en múltiples trenes de datos a fin de obtener escalabilidad. Se puede conseguir escalabilidad de anchura de banda, escalabilidad temporal, escalabilidad SNR y/o escalabilidad espacial. El anexo O/H.263 describe el uso de la codificación por capas en H.263. Las conferencias pueden aprovechar esta característica para dar servicio a puntos extremos conectados que tengan diferentes capacidades, utilizando un tren de bits. Esto permitirá una utilización más eficaz de la anchura de banda de la red.

B.3 Métodos de escalabilidad

La escalabilidad de un tren de vídeo está relacionada con la generación de un tren que sólo puede decodificarse en parte debido a limitaciones de los recursos disponibles. La escalabilidad puede desearse para superar limitaciones de la potencia de computación disponible, o para acomodar limitaciones de anchura de banda.

Hay tres tipos de escalamiento disponibles en la Rec. UIT-T H.263: temporal, de relación señal/ruido (SNR, *signal-to-noise ratio*) y espacial. Otros códecs de vídeo pueden tener capacidad por capas similar. Todos estos métodos pueden utilizarse por separado, o juntos para crear un tren de bits escalable multicapa. La resolución, la velocidad de trama y la calidad de la imagen sólo pueden aumentarse añadiendo capas escalables. La capa de base puede utilizarse para garantizar un nivel mínimo de calidad de imagen. Los puntos extremos pueden entonces utilizar capas adicionales para añadir calidad de imagen aumentando la velocidad de trama, el tamaño de la trama de visualización, o la exactitud de las imágenes decodificadas. Permitir métodos de escalamiento múltiple en una conferencia puede añadir eficiencia de recursos, especialmente cuando los puntos extremos participantes tienen variadas capacidades de procesamiento y de anchura de banda. Esto es especialmente cierto para las conferencias multipunto y de bajo acoplamiento.

B.4 Establecimiento de la comunicación

El establecimiento de la comunicación H.323 tiene lugar siguiendo los mismos procedimientos descritos en la cláusula 8. La capacidad de codificación por capas será señalizada utilizando los métodos de intercambio de capacidades H.245. Existen puntos de código en H.245 que identifican claramente qué métodos por capas son soportados por los puntos extremos. Los puntos extremos utilizarán estas capacidades a fin de señalizar los métodos por capas exactos que soportan.

El uso de métodos de capacidades simultáneas en H.245 se utilizan para indicar qué métodos de estratificación serán utilizados juntos para crear las capas de vídeo cuando van a enviarse en dos o más canales lógicos. Es también posible enviar dos o más capas en canales lógicos simples. Las capas de vídeo exactas que se utilizarán se señalizarán durante la **openLogicalChannel** de la misma manera que se utiliza actualmente para indicar qué **tipo de datos** de vídeo se utilizarán, con la diferencia de que el punto extremo indicará dependencias entre el canal lógico de la capa base y los canales lógicos de las capas de mejora.

B.5 Utilización de sesiones RTP y capas de códec

Se desea permitir sesiones RTP separadas para las diferentes calidades de vídeo disponibles. La capa de base debe considerarse la sesión de vídeo primaria, y su nivel la mínima calidad de vídeo disponible en la conferencia. Las capas de mejora pueden enviase en sesiones RTP separadas. El parámetro **forward/reverseLogicalChannelDependency** (**dependencia de canal lógico directa/inversa**), añadido a la **openLogicalChannel** H.245, se utilizará para indicar cómo se organizan las capas de vídeo, lo cual se detalla en las cláusulas siguientes. Las indicaciones de tiempo RTP deben ser las mismas en las capas de base y en todas las capas de mejora dependientes correspondientes a una trama para permitir el reensamblado y la correcta visualización.

B.5.1 Base asociada al audio para la sincronización con el movimiento de los labios

La sesión de vídeo de base debe estar asociada con la sesión de audio correspondiente o la pista de audio del vídeo, con fines de sincronización con el movimiento de los labios. Esto se hace de la misma manera que las sesiones de vídeo no estratificadas asociadas con su audio correspondiente. Se hace utilizando los parámetros **associatedSessionID** (**ID de sesión asociada**) y **sessionID** situados en los **H2250LogicalChannelParameters**. Las capas de mejora pueden también estar asociadas con el audio o con la capa de base utilizando **associatedSessionID**. El código de dependencia se indicará utilizando el parámetro **forwardLogicalChannelDependency** (**dependencia de canal lógico directo**) y **reverseLogicalChannelDependency** (**dependencia de canal lógico inverso**) en la instrucción **openLogicalChannel** como se explica a continuación.

B.5.2 Dependencia de las capas de mejora

La dependencia de las capas de mejora puede crear muchos casos complejos utilizando múltiples capas que contengan múltiples tipos de tramas de mejora. La dependencia entre capas se indicará utilizando el parámetro **forward/reverseLogicalChannelDependency**, añadido a la instrucción H.245 **openLogicalChannel**. La dependencia se utiliza para indicar que los datos enviados por el canal lógico no pueden utilizarse sin el contenido del canal lógico del que dependen. Las capas de mejora, por definición, deben codificarse diferencialmente con respecto a la capa de vídeo que están mejorando, y son por tanto dependientes de esa capa de vídeo para una decodificación correcta. Si una capa de mejora se envía por un canal lógico separado, indicará la capa a partir de la cual fue diferencialmente codificada en el parámetro **forward/reverseLogicalChannelDependency**.

Puesto que el parámetro **forward/reverseLogicalChannelDependency** permite la indicación de un único canal lógico, los canales lógicos necesitan abrirse en orden de dependencia empezando por la capa de base. Un punto extremo habrá enviado o recibido el **openLogicalChannelAck** para cualquier canal lógico que se utilice en un parámetro **forward/reverseLogicalChannelDependency**. Un punto extremo enviará un **openLogicalChannel** para un canal lógico dependiente sólo después de que el canal lógico del cual esté pendiente se ha abierto y se haya acusado recibo del mismo. Los canales lógicos que tienen dependencia común pueden abrirse en paralelo. Las capas de mejora deben indicarse dependientes de la capa más alta requerida para una decodificación adecuada.

Suponiendo que se utilizan sesiones RTP separadas para cada capa, puede construirse un ejemplo, tal como se muestra en la figura B.1.

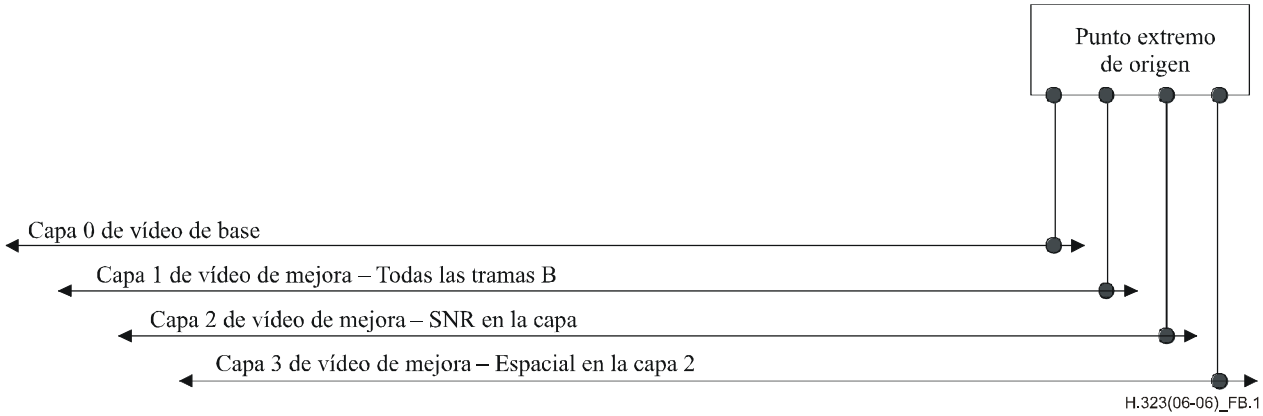


Figura B.1/H.323 – Modelo con vídeo por capas

En este ejemplo, se crea vídeo estratificado de cuatro capas:

1) El vídeo de base, no dependiente de ninguna otra capa. Está asociado con su audio correspondiente.

2) Nivel de mejora uno compuesto por tramas B, dependiente del vídeo de base. Se indica que es dependiente de la sesión de vídeo de base, capa 0.

3) Nivel de mejora dos, que es la mejora de la SNR del vídeo de base, dependiente sólo del vídeo de base, capa 0. Se indica que es dependiente de la sesión de vídeo de base.

4) Nivel de mejora tres, que consiste en la mejora espacial del nivel de mejora dos, dependiente de la capa 2, lo que implica que también se requiere la base. Se indica que es dependiente del vídeo en la capa 2.

En este ejemplo el canal lógico de vídeo debe abrirse primero. El **openLogicalChannel** para las capas de mejora 1 y 2 puede enviarse simultáneamente sólo después de recibir el **openLogicalChannelAck** del canal lógico de vídeo de base. El **openLogicalChannel** para la capa de mejora 3 sólo puede enviarse después de que se ha recibido o enviado el **openLogicalChannelAck** para el canal lógico utilizado para la capa de mejora 2.

B.6 Posibles modelos de estratificación

Hay muchos métodos posibles de estratificar el vídeo y la organización de las sesiones RTP correspondientes. La razón de que las capas puedan necesitar estar separadas es que se utilizan para escalamiento de la potencia del decodificador o para escalamiento de la utilización de anchura de banda. Puede ser conveniente separar todas las tramas que no sean B en capas separadas que puedan descartarse si no pueden utilizarse. Una característica importante del códec por capas es que en cualquier momento un punto extremo puede descartar cualquiera de las capas de mejora, sin afectar a la calidad del vídeo de base, a fin de proporcionar escalamiento de potencia del decodificador.

De manera similar, las capas pueden necesitar organizarse en capas de utilización de anchura de banda que correspondan a las anchuras de banda comunicadas por los puntos extremos conectados a la conferencia. Esto permitiría a la conferencia acomodar conferencias multipunto que tengan puntos extremos que utilicen métodos de conexión que puedan limitar la anchura de banda disponible, y crear una capa que les dé el mejor vídeo posible a esa anchura de banda. El punto extremo puede añadir o sustraer capas a medida que aumente o disminuya la anchura de banda disponible.

B.6.1 Múltiples canales lógicos y múltiples sesiones RTP para un tren por capas

Si el escalamiento de la anchura de banda es el objetivo de utilizar estratificación, cada capa debe fluir por un canal lógico separado con una sesión RTP separada. Esto significa que lo que constituye una única fuente de vídeo tendrá ahora que coordinarse entre múltiples canales lógicos y sesiones RTP.

Si el objetivo de la estratificación es el escalamiento de la potencia del procesador, las capas de mejora pueden enviarse, con el vídeo de base por un único canal lógico y una única sesión RTP.

Si el objetivo es una combinación de escalamiento de anchura de banda y de potencia del procesador, pueden entonces enviarse grupos de capas de mejora, enviadas en canales lógicos por grupos. La elección de las capas y del agrupamiento es una elección basada en las necesidades del sistema. El método utilizado para hacer estas elecciones depende de la implementación y queda fuera del alcance de esta Recomendación.

B.6.2 Consecuencias de utilizar una capa por canal lógico y por sesión RTP

Las consecuencias de utilizar un único canal lógico y una única sesión RTP para cada capa es que el codificador y el decodificador tienen la tarea adicional de dividir y reensamblar el tren de vídeo con arreglo al modelo de estratificación elegido. Este modelo es señalizado al lado recepción para que éste pueda interpretar correctamente la información de capa. Se señaliza utilizando capacidades H.245, con una capacidad por canal lógico que, cuando se combina con las dependencias, describirá suficientemente el modelo de estratificación. Durante el intercambio de capacidades se señalizan posibles modelos de estratificación utilizando la característica capacidades simultáneas de la Rec. UIT-T H.245.

Se necesitará una consideración estricta de la temporización a utilizar para asegurar que las capas estén correctamente sincronizadas. Para H.323, ello se tratará en el formato de la cabida útil del RTP.

B.7 Consecuencias sobre las conferencias multipunto

La utilización prevista más probable de la estratificación de vídeo es para conferencias multipunto. En H.323 ésta puede ser efectuada por una MCU centralizada, utilizada para mezclado de audio y conmutación de vídeo, o utilizando un modelo descentralizado, con cada punto extremo responsable de la conmutación de vídeo, y del mezclado de audio. En ambos casos, el MC debe efectuar la función de comunicar lo que el modelo de estratificación supone para la conferencia. Esto se hace utilizando la **communicationModeCommand**.

A fin de que un punto extremo reciba una capa de vídeo, debe abrirse un canal lógico que contenga esa capa. La decisión de abrir un canal lógico puede tomarla el MC o el punto extremo enviando un mensaje **openLogicalChannel**. Si un MC o un punto extremo decide no abrir un canal lógico, debe rechazar el **openLogicalChannel** cuando es ofrecido. El MC o el punto extremo sólo puede ofrecer un canal lógico que corresponda a un **dataType** soportado por el punto extremo receptor.

Cuando se implementa soporte para códecs por capas, un MC puede aplicar dos criterios. Si el MC no toma decisiones en cuanto a qué canales lógicos serán abiertos, el modelo puede denominarse "MC imparcial". En este modelo el MC ofrece todos los medios a todos los puntos extremos sin considerar ninguna QoS comunicada. Cuando el MC toma la decisión de hacer valer estrictamente la QoS, el modelo se denomina "MC decisión". Estos modelos se exponen más detenidamente a continuación.

B.7.1 Modelo MC imparcial

El modelo MC imparcial no depende de las adiciones al conjunto de capacidades QoS, y como tal puede permitir una implementación de un MC más simple. En este caso, el punto extremo debe juzgar si tiene suficiente anchura de banda para aceptar canales lógicos ofrecidos por el MC. En caso de que exceda las capacidades de transmisión del punto extremo o de la red subyacente, el punto extremo puede entonces rechazar el canal lógico. Este método exigirá que el punto extremo tenga conocimiento de la anchura de banda de red disponible. El MC debe indicar todos los medios disponibles en la **communicationModeCommand**.

B.7.2 Modelo MC decisión

El modelo MC decisión depende de la adición de capacidades de calidad de servicio (QoS) al conjunto de capacidades del terminal, lo cual se ha propuesto anteriormente y hay trabajo en curso. El MC puede entonces examinar las capacidades QoS de los puntos extremos y ofrecer solamente canales lógicos que estén dentro de la QoS del punto extremo. El punto extremo necesitará determinar su QoS al comienzo de la conferencia e indicar que está utilizando las capacidades QoS definidas por trabajos en curso.

En el modelo MC decisión, el MC puede enviar una **communicationModeCommand** a un punto extremo que sólo muestre las sesiones dentro de las capacidades de QoS del punto extremo. De este modo, el MC puede hacer valer estrictamente la utilización de anchura de banda.

B.7.3 Conferencia multipunto que contiene puntos extremos en diferentes anchuras de banda

En el modelo en el que la conferencia multipunto contiene puntos extremos que tienen diferentes capacidades de anchura de banda, tendrá que sintonizarse la estratificación por capas para hacer corresponder estos niveles de anchura de banda. Esto puede efectuarse mediante dos posibles métodos. Uno se ilustra en la figura B.2.

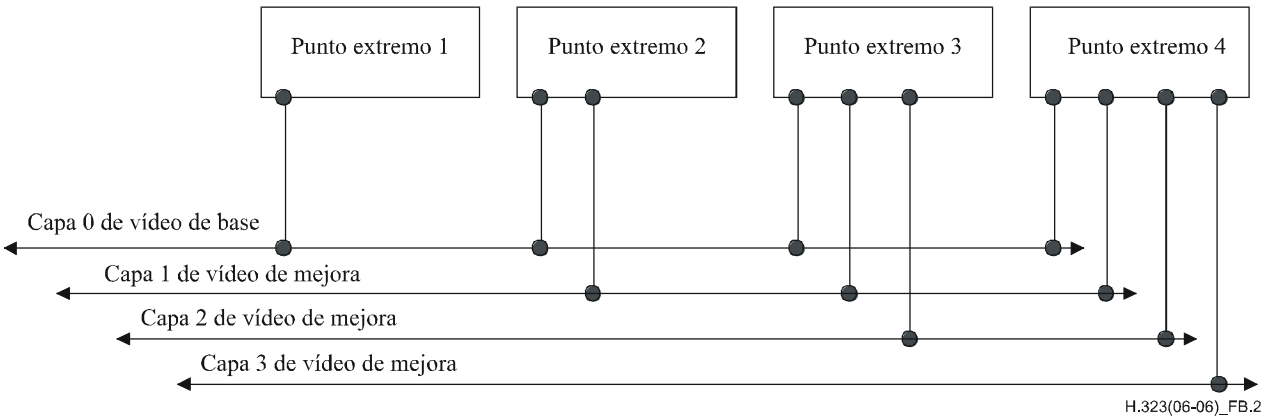


Figura B.2/H.323 – Los puntos extremos se conectan a una o más capas según la anchura de banda

En este caso, los puntos extremos se conectan a la capa de base de vídeo y a las capas de mejora hasta la anchura de banda total deseada. Cada capa de mejora está en un canal lógico separado. Los puntos extremos tienen la tarea adicional de recombinar las capas para crear el tren de vídeo. El punto extremo emisor debe tener capacidad para la anchura de banda combinada de todos los trenes que origina. En este caso, cada punto extremo puede haber comunicado un conjunto de capacidades diferente. El MC examinará las capacidades y el QoS, y creará un modelo de estratificación que es probable que proporcione el mejor uso de las capacidades y de la anchura de banda de los puntos

extremos. Esta estratificación es indicada en la **communicationModeCommand** mediante la indicación de **sessionDependency** (**dependencia de sesión**) en la **communicationModeTableEntry** (**entrada de la tabla de modos de comunicación**). El campo **sessionDependency** es fijado por el MC para indicar cuándo una sesión es dependiente de otra sesión para una decodificación significativa de sus datos. Esta información se traducirá a **logicalChannelNumbers** (**números de canal lógico**) cuando se abra un canal lógico dependiente, según los canales lógicos que se abran realmente.

En el caso anteriormente citado, utilizando el modelo MC decisión el MC ofrecerá a los puntos extremos los canales lógicos que corresponden a las capas que corresponden con las capacidades de cada punto extremo. El MC ofrecerá al punto extremo 1 sólo el canal lógico correspondiente a la capa de vídeo de base. Al punto extremo 2 se le ofrecerá el canal lógico correspondiente a la capa de vídeo de base y a la capa 1 de vídeo de mejora. Al punto extremo 3 se ofrecerán tres canales lógicos correspondientes a las capas de vídeo de base y dos capas de mejora, y al punto extremo 4 se ofrecerán todos los canales lógicos de vídeo.

En el caso MC imparcial, el MC ofrecerá todos los canales lógicos a todos los puntos extremos que estén dentro de sus capacidades de **dataType**. Los puntos extremos rechazarán cualquier canal lógico que les haga exceder sus capacidades de anchura de banda.

En la figura B.3 se muestra un segundo modelo de estratificación. En este modelo, cada canal lógico contiene un tren de vídeo totalmente independiente.

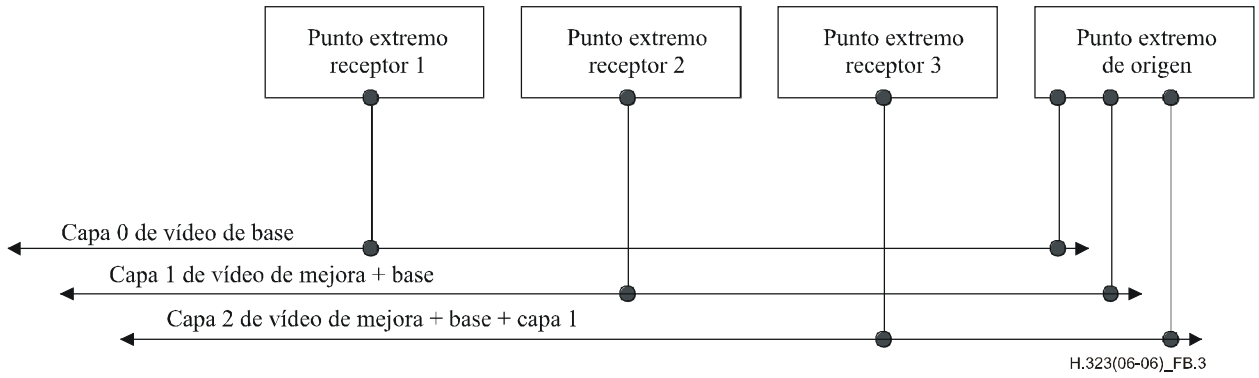


Figura B.3/H.323 – Los puntos extremos se conectan a una sola capa según la anchura de banda

En este caso, el punto extremo se conectará sólo al canal lógico que corresponde a la anchura de banda que tiene disponible. Este tren tiene todas las capas que componen el tren de vídeo hasta la anchura de banda del canal lógico. Este método elimina la tarea adicional de los puntos extremos de recombinar el vídeo, pero carga al emisor con la producción de varios trenes de vídeo. Éste es un uso menos eficiente de los recursos de red, ya que las capas de mejora incluyen todas las capas inferiores.

A fin de efectuar la correcta sincronización de los labios, cualquier sesión que contenga vídeo de base debe ir asociada con la sesión de audio correspondiente a su pista de audio, utilizando el **associatedSessionID** en los **H2250LogicalChannelParameters**. En el ejemplo presentado en la figura B.2, la sesión de vídeo de base debe estar asociada con la sesión de audio para la sincronización del movimiento de los labios. En el ejemplo presentado en la figura B.3 las tres sesiones de vídeo deben estar asociadas con la sesión de audio para la sincronización del movimiento de los labios, ya que las tres contienen vídeo de base.

B.8 Utilización de la QoS de red para los trenes de vídeo por capas

Deben considerarse varias características importantes de la naturaleza de la utilización de la codificación por capas cuando se utilizan QoS de red para la entrega de trenes de vídeo codificados por capas. Una capa de mejora no puede decodificarse adecuadamente sin recibir las capas de las cuales es dependiente. Las capas de vídeo de mejora pueden descartarse sin afectar a la decodificación de la capa de la cual son dependientes.

Si está disponible, la QoS de la red puede utilizarse para ayudar a garantizar que un tren de vídeo será entregado por la red. Puesto que el vídeo por capas puede ser entregado utilizando múltiples trenes entregados en conexiones de red separadas, pueden utilizarse diferentes QoS en cada capa de vídeo. La QoS utilizada en los trenes de vídeo por capas deben especificarse cuando se abre el canal lógico.

Es importante que una capa de vídeo dependiente tenga la información de la cual es dependiente en el momento en que ha de decodificarse la capa dependiente. Esto conduce a reglas generales relativas al uso de la QoS:

1) A las capas dependientes entregadas utilizando la QoS de red, también debe entregárseles la capa de la que son dependientes utilizando la QoS.
2) Si cualquier capa de vídeo de la conferencia debe entregarse utilizando QoS, la capa de base debe entregarse utilizando la QoS de la red.
3) Mientras más próxima esté la capa de vídeo a la capa de base, mayores deben ser las garantías de entrega.

Anexo C

H.323 sobre ATM

C.1 Introducción

Ésta es una mejora opcional que permite a los puntos extremos H.323 establecer trenes de medios basados en la QoS sobre redes ATM utilizando AAL 5.

C.2 Alcance

Este anexo especifica un método mejorado de utilizar H.323 sobre AAL 5. H.323 siempre puede utilizarse sobre ATM haciendo uso de un método IP sobre ATM. Sin embargo, es menos eficaz que utilizar canales virtuales (VC, *virtual channels*) AAL 5 directamente para el transporte de los trenes de audio y vídeo de H.323. Cuando los trenes de medios fluyen directamente por AAL 5, pueden aprovecharse de un VC ATM basado en la QoS.

Este anexo mantiene el uso de un protocolo de red de paquetes para que en las comunicaciones H.245 y H.225.0 se asegure la interoperabilidad con puntos extremos H.323 que están utilizando un protocolo de red de paquetes para todos los trenes (sea sobre ATM u otros medios). La interoperabilidad con los puntos extremos H.323 basados en una norma anterior (legados) se consigue, sin el uso de una pasarela, requiriendo primero el modo de funcionamiento básico, en el que un punto extremo envía trenes de medios mediante un servicio de datagramas utilizando un protocolo de red de paquetes, por ejemplo UDP/IP sobre ATM. En el modo básico, a menos que se haya potenciado la infraestructura del protocolo de red de paquetes, la red puede no ser capaz de ofrecer QoS.

C.2.1 Conferencia punto a punto

Este anexo especifica un método de comunicación punto a punto entre dos puntos extremos H.323 utilizando AAL 5 VC para los trenes de medios. Se especifica el protocolo necesario para pasar a este modo de comunicación, así como los elementos de información que han de utilizarse en la señalización ATM.

C.2.2 Multipunto basado en MCU

Se desprende que las comunicaciones multipunto basadas en MCU pueden producirse entre varios puntos extremos H.323 utilizando AAL 5 VC para los trenes de medios. Actualmente no se especifica soporte alguno para el multipunto descentralizado H.323 utilizando capacidad ATM punto a multipunto. Este asunto queda en estudio.

C.2.3 Interoperabilidad H.323 con puntos extremos que utilizan IP

La interoperabilidad está garantizada con un punto extremo que utiliza IP en toda la conexión H.323. Este anexo define métodos que permiten a un punto extremo detectar si hay soporte para la opción de utilizar AAL 5 directamente. Un punto extremo conforme a este anexo debe aceptar que los trenes de audio y de vídeo puedan producirse en AAL 5 VC o en puertos UDP/IP.

C.3 Arquitectura

La arquitectura de protocolo básica del sistema se muestra en la figura C.1. Utiliza IP en ATM para la entrega de los mensajes H.225.0 y H.245 y para la parte RTCP de los trenes de audio y de vídeo. Utiliza AAL 5 directamente para la parte RTP de los trenes de audio y vídeo.

NOTA – Los trenes de medios H.323, comprimidos en paquetes de longitud variable según la Rec. UIT-T H.225.0, se hacen corresponder fácilmente con AAL 5. Sería difícil hacerlos corresponder con AAL 1, alternativa esta que no presenta ventajas claras.

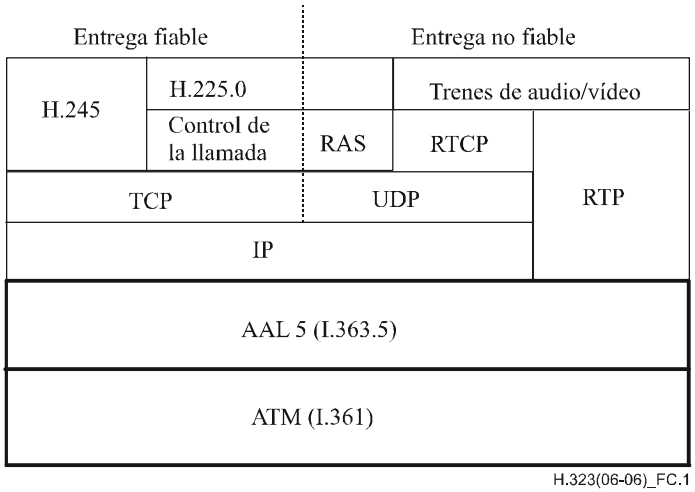


Figura C.1/H.323 – Arquitectura para H.323 en ATM AAL 5

C.3.1 Visión general del sistema

La arquitectura del sistema está diseñada para utilizar H.323, y sus protocolos componentes, que se especifican actualmente. Se designa también para utilizar servicios ordinariamente disponibles de AAL 5 en ATM.

C.3.2 Interfuncionamiento con otros puntos extremos de las Recomendaciones del UIT-T de la serie H

El interfuncionamiento con otros puntos extremos de las Recomendaciones de la serie H se efectuará mediante el uso de dispositivos de pasarela tal como se describe en la Rec. UIT-T H.323. Los vendedores de pasarelas necesitarán soportar los métodos descritos en este anexo, si desean soportar el uso directo de VC AAL 5 por puntos extremos H.323.

Debe señalarse que el interfuncionamiento con otros puntos extremos H.323 basados en IP no requiere una pasarela.

C.3.3 H.225.0 en IP sobre ATM

La comunicación H.225.0 requiere que TPC/IP y UDP/IP utilicen uno de los métodos disponibles para los IP sobre ATM. No se expresa preferencia aquí sobre qué método de IP sobre ATM utilizar. Si dos puntos extremos en el mismo segmento de red utilizan diferentes métodos IP sobre ATM, deben utilizar los encaminadores de IP para reenviar sus paquetes.

El punto extremo escuchará los puertos TCP conocidos identificados en la Rec. UIT-T H.225.0. Si el punto extremo se utiliza en una red con un controlador de acceso, el punto extremo debe utilizar los métodos descritos en la Rec. UIT-T H.225.0 para descubrir el controlador de acceso y registrarse en él. Esto exige el soporte de multidifusión de UDP. Si la multidifusión no está disponible en la red, el punto extremo puede reconfigurarse con la dirección o direcciones del controlador o controladores de acceso.

Los métodos expuestos en la Rec. UIT-T H.225.0, combinados con un método IP sobre ATM se utilizarán para establecer el canal de control H.245 en TCP/IP.

C.3.4 H.245 en TCP/IP sobre ATM

Una vez que el canal de control H.245 fiable ha sido establecido utilizando métodos descritos en la Rec. UIT-T H.225.0, se establecen canales adicionales para audio, vídeo y datos sobre la base de los resultados del intercambio de capacidades H.245 utilizando procedimientos de apertura de canal lógico H.245.

C.3.5 Direccionamiento para trenes A/V

H.323 tiene la capacidad para que los trenes de audio y vídeo se establezcan con una dirección diferente que los canales de control H.245. Esto es una suerte, porque un canal TCP/IP está establecido con una dirección IP, y el audio y el vídeo, opcionalmente, han de enviarse en RTP sobre AAL 5 directamente a una dirección ATM.

H.323 también tiene la capacidad de que el tren RTCP se direccione separadamente del tren RTP. El tren RTPC continuará siendo direccionado sobre una dirección IP, aun cuando el tren RTP sea direccionado sobre una dirección ATM.

C.3.6 Capacidades de transporte añadidas a un conjunto de capacidades de transporte

Para el funcionamiento de H.323 en AAL 5, se hace en H.245 una adición al conjunto de **TransportCapability** (**capacidades de transporte**). Ésta incluye capacidades a nivel de transporte tales como el soporte de capacidad de transferencia ATM (DBR, SBR1, SBR2, SBR3, ABT/DT, ABT/IT, ABR) que se definen en la Rec. UIT-T I.371. Los terminales que no envíen este nuevo parámetro de capacidad, no utilizarán los nuevos métodos descritos en este anexo. La información **TransportCapability** puede ser enviada como parte del intercambio de conjunto de capacidades de terminal en la fase intercambio de capacidades. También se incluye en **openLogicalChannel**.

C.3.7 Elementos de la señalización ATM

C.3.7.1 Dirección ATM

La dirección ATM para un tren RTP estará en el subcampo **mediaChannel** de **H2250LogicalChannelParameters** del mensaje H.245 **openLogicalChannelAck** (o el **OpenLogicalChannel** en el caso de conexión rápida). El subcampo **mediaChannel** de **UnicastAddress** o **MulticastAddress** se rellenará con la dirección de sistema extremo ATM de estilo NSAP de 20 octetos.

El uso de E.164 para la dirección se trata insertándolo como la parte IDP (AFI = 0x45) de una dirección NSAP. En este caso, se requiere un número E.164 internacional.

C.3.7.2 Número de puerto

El campo **portNumber** (**número de puerto**) del mensaje **openLogicalChannel** se transporta en el elemento de información transporte de información genérica (GIT, *generic information transfer*) según [33]. El formato del elemento de información GIT se especifica más adelante en C.4.1.1. Esto permite al lado del receptor asociar el VC ATM con el canal lógico RTP adecuado.

Para que exista retrocompatibilidad con puntos extremos Rec. UIT-T H.323 versión 2, los puntos extremos Rec. UIT-T H.323 versión 3 (y posteriores) deberán también poder utilizar la B-HLI, de acuerdo con la Rec. UIT-T H.323 versión 2, anexo C, para transportar el campo **portNumber** del **openLogicalChannel**. Un punto extremo H.323 versión 3 (o posterior) utilizará la B-HLI sólo si tiene conocimiento previo de que el punto extremo de terminación es H.323 versión 2. En casos en los que no se conoce la versión H.323 del punto extremo de terminación, tal como ocurre al establecer una comunicación utilizando conexión rápida, los puntos extremos intentarán establecer el VC ATM utilizando el elemento de información GIT para transportar el **portNumber**. Si falla la conexión, el punto de extremo llamante reintentará el establecimiento de comunicación utilizando B-HLI en lugar de GIT. Si el establecimiento de VC con B-HLI también falla, el terminal supondrá que la conectividad ATM no está disponible y recurrirá a utilizar RTP/UDP/IP para canales de medios. El formato del elemento de información B-HLI se especifica en C.4.1.2.

C.3.8 Trenes A/V en RTP en AAL 5

La puesta en servicio de la primitiva **openLogicalChannel** en H.245 desencadena el establecimiento de la conexión. Los trenes de audio y vídeo se establecen entonces a la dirección ATM de destino. El tamaño de la unidad de transmisión máxima (MTU, *maximum transmission unit*) se señalizará en el elemento de información parámetros AAL. La elección de la MTU puede afectar a la eficacia del sistema debido a la paquetización de AAL 5. Las reglas de paquetización de AAL 5 figuran en la Rec. UIT-T I.363.5. Si se utiliza el valor por defecto no-AAL 5 de 1536 octetos, la MTU es paquetizada en 33 células ATM y la última célula AAL 5 contiene sólo relleno y el número AAL 5. El campo de dirección en el **mediaChannel** debe utilizarse para determinar si debe abrirse un VC ATM o un puerto UDP.

En el caso de que falle el establecimiento del VC ATM, el punto extremo hará un reintento utilizando RTP/RTCP y el protocolo de transporte de capa superior, como por ejemplo UDP.

Se puede utilizar opcionalmente la compresión de encabezamiento en RTP que se describe en la sección 2 de AF-SAA-0124.000 [32], en cuyo caso se debe negociar utilizando el **mediaTransportType** (**tipo de transporte de medios**).

C.3.8.1 Canales lógicos unidireccionales

H.323 no tiene ningún concepto del sentido inverso en un canal lógico unidireccional. Sin embargo, una característica importante de los VC ATM punto a punto es que son intrínsecamente bidireccionales. Por tanto es deseable el uso de ambos sentidos de un VC ATM. De otro modo, los trenes de audio y vídeo necesitarán cada uno ser enviados en dos VC diferentes, uno para cada sentido.

Se alienta a que los puntos extremos conformes a este anexo abran sus trenes de medios como canales lógicos bidireccionales. Se reduce así el número de VC AAL 5 a dos en situaciones típicas, un VC para audio y otro para vídeo.

C.3.8.2 Canales lógicos bidireccionales

Si se indica la utilización bidireccional, el punto extremo receptor enviará un **openLogicalChannelAck** (o la **openLogicalChannel** en el caso de conexión rápida) y deben entonces vigilar que el otro punto extremo abra un VC ATM. Cuando se haya completado el VC ATM, puede entonces utilizar el sentido inverso para el tipo de medios indicado en la **openLogicalChannel**. El punto extremo que inicia la instrucción **openLogicalChannel** es el punto extremo que abrirá el VC ATM.

Si ha de utilizarse QoS, se limitará a la **capacidad H2250** (**H2250Capability**) declarada por el otro punto extremo. La QoS elegida es señalizada como parte del establecimiento de un VC ATM.

Si ambos puntos extremos tienen instrucciones **openLogicalChannel** incompletas para la misma sesión de medios, se resuelven utilizando los métodos principal/subordinado descritos en la Rec. UIT-T H.245.

C.3.8.3 Tamaño máximo de la unidad de transmisión

La MTU máxima para AAL 5 es 65 535 octetos. Como parte de la **H2250Capability**, el tamaño de MTU puede especificarse en el intercambio de capacidades durante el establecimiento H.245. El máximo tamaño de MTU hacia adelante y hacia atrás será igual y se tomará del menor de los valores locales y distantes especificados en el intercambio de capacidades.

El tamaño de MTU es señalizado como el máximo tamaño CPCS-PDU de la AAL 5 para un VC ATM.

C.3.8.4 RTCP en IP sobre ATM

Es obligatorio abrir el canal lógico para tráfico RTCP en un puerto UDP/IP, utilizando IP sobre ATM. No se permite al RTCP viajar directamente en un VC AAL 5.

C.3.9 Consideraciones de QoS (opcional)

C.3.9.1 Clases de QoS definidas en la Rec. UIT-T I.356

La Rec. UIT-T I.356 define cuatro clases de QoS, Clase 1 (clase rigurosa), Clase 2 (clase tolerante), Clase 3 (clase binivel) y Clase U. El cuadro C.1 resume las diferencias entre las clases de QoS.

Cuadro C.1/H.323 – Definiciones de clases de QoS y objetivos de calidad de funcionamiento de la red provisionales

	CTD	CDV 2 ptos	CLR (0+1)	CLR (0)	CER	CMR	SECBR
Por defecto	Ninguno	Ninguno	Ninguno	Ninguno	4×10^{-6}	1/día	10^{-4}
Clase 1 (rigurosa)	400 ms	3 ms	3×10^{-7}	Ninguno	Por defecto	Por defecto	Por defecto
Clase 2 (tolerante)	U	U	10^{-3}	Ninguno	Por defecto	Por defecto	Por defecto
Clase 3 (binivel)	U	U	U	10	Por defecto	Por defecto	Por defecto
Clase U	U	U	U	U	U	U	U

CDV: Variación del retardo de célula; CER: Tasa de errores de células; CLR: Tasa de pérdida de células; CMR: Velocidad de inserción incorrecta de células; CTD: Retardo de transferencia de células; SECBR: Tasa de bloques de células con muchos errores; U: No especificado/no limitado.

C.3.9.2 Capacidad transferencia ATM definida en la Rec. UIT-T I.371

La capacidad de transferencia ATM (ATC, *ATM transfer capability*), definida en la Rec. UIT-T I.371 como un conjunto de parámetros y procedimientos de capa ATM, está destinada a soportar un modelo de servicio de capa ATM y una gama de clases de QoS asociadas. Las ATC de control de bucle abierto (DBR y SBR) y las ATC controladas de bucle cerrado (ABT y ABR) se especifican en la Rec. UIT-T I.371. La SBR se subdivide en SBR1, SBR2 y SBR3, dependiendo de cómo se traten las células CLP = 0/1. ABT se subdivide en ABT/DT y ABT/IT dependiendo del uso de negociación relativa a la tasa de células en bloque. El cuadro C.2 resume la asociación de las ATC con las clases de QoS.

Cuadro C.2/H.323 – Asociación de las ATC con las clases de QoS (del cuadro 3/I.356)

Capacidades de transferencia ATM (ATC)	DBR, SBR1, ABT/DT, ABT/IT	DBR, SBR1, ABT/DT, ABT/IT	SBR2, SBR3, ABR	Cualquier ATC
Clase de QoS aplicable	Clase 1 (rigurosa)	Clase 2 (tolerante)	Clase 3 (binivel)	Clase U

ABR: Velocidad binaria disponible; ABT/DT: Transferencia de bloques ATM/transmisión diferida; ABT/IT: Transferencia de bloques ATM/transmisión inmediata; DBR: Velocidad binaria determinista; SBR1: Configuración 1 de velocidad binaria estadística; SBR2: Configuración 2 de velocidad binaria estadística; SBR3: Configuración 3 de velocidad binaria estadística.

C.3.9.3 Capacidad de transferencia de banda ancha definida en la Rec. UIT-T Q.2961.2

Los códigos de capacidad de transferencia de banda ancha (BTC, *broadband transfer capability*) (DBR, BTC5, BTC9, BTC10 y SBR1) en el elemento de información capacidad portadora de banda ancha se definen en la Rec. UIT-T Q.2961.2, y combinaciones válidas de los parámetros clase portadora, capacidad de transferencia de banda ancha y descriptor de tráfico ATM se especifican en el anexo A/Q.2961.2. En el mensaje Establecimiento, el usuario puede especificar la BTC según el tráfico que genera y el uso previsto de los servicios de red. En el cuadro A.1/Q.2961.2 se indican tres combinaciones válidas para la clase portadora BCOB-A, 8 combinaciones para BCOB-C y 13 combinaciones para BCOB-X o FR.

C.3.9.4 Apertura de canales virtuales

El punto extremo que originó el **openLogicalChannel** aceptado es responsable de abrir el VC ATM. El soporte de la QoS en el VC ATM es señalizado al mismo tiempo que se establece. Si tiene éxito, la red ATM proporciona una QoS garantizada durante el tiempo de vida del VC abierto. La QoS se especifica en términos de elementos de información (IE, *information element*) Q.2931, incluido el descriptor de tráfico ATM y la capacidad portadora de banda ancha.

C.3.9.5 Utilización de DBR

El tráfico ATM más probablemente disponible es del tipo velocidad constante utilizando DBR. El uso de DBR es señalizado como parte del IE de capacidad portadora de banda ancha ATM (clase portadora = "BCOB-A"). Es también posible la utilización de otro tipo de tráfico ATM, tal como SBR con temporización extremo a extremo requerida [clase portadora = "BCOB-X" y campo BTC = "SBR1 (0010011)"].

C.3.9.6 Fijación de la velocidad de células adecuada

Es importante fijar los parámetros de velocidad de células adecuada en el elemento de información descriptor de tráfico ATM. La velocidad de células de cresta puede obtenerse de los parámetros de intercambio de capacidades H.245 y del tamaño del paquete del formato de la cabida útil RTP. Para el vídeo, el campo **maxBitRate** (**velocidad binaria máxima**) puede utilizarse a partir de la **H261VideoCapability** (**capacidad de vídeo H261**) o de la **H263VideoCapability** (**capacidad de vídeo H263**) para determinar la velocidad de células ATM. Para el audio, la capacidad de audio elegida implica la velocidad binaria a utilizar. Por ejemplo, el uso de la **g711Ulaw64k** (**ley μ a 64 kbit/s g711**) sugiere el uso de un canal de audio a 64 kbit/s, mientras que el uso de **g728** indica el uso de un canal a 16 kbit/s. El formato de la cabida útil RTP indica el tamaño de paquete. Para cada paquete debe añadirse la tara de paquete AAL subsiguiente y cualquier relleno necesario para cumplir las reglas de paquetización de AAL. Esto da lugar a una velocidad binaria de tara que está asociada con el tamaño del paquete y con el modo en el que el paquete está encapsulado en la AAL, y la frecuencia de esta tara derivada de este encapsulado.

La velocidad binaria de los datos a enviar, y la paquetización de los datos conforme a las reglas de paquetización de AAL determinan la velocidad de células. La paquetización determinará el número real de células que debe enviarse para un determinado tren de datos a una determinada velocidad binaria. La elección de la MTU puede afectar a la paquetización, como se explica en C.3.8.

C.4 Sección de protocolo

C.4.1 Elementos de información de señalización ATM

C.4.1.1 Transporte de información genérica

Parámetro de IE	Valor	Notas
Norma/aplicación relacionada con el identificador (octeto 5)	0000 1011	Rec. UIT-T H.323
Tipo de identificador (octeto 6)	0000 1011	**portNumber** H.245
Longitud del identificador (octeto 6.1)	0000 0010	2 octetos
Valor del identificador (octetos 6.2-6.3)	**portNumber** H.245	**portNumber** H.245 de 16 bits con codificación binaria directa

Los puntos extremos H.323 versión 3 (o posteriores) pondrán el indicador de acción del ID del elemento de información GIT a "liberar llamada", de acuerdo con 4.5.1/Q.2931. En este caso, si el punto extremo de terminación no soporta la codificación de elementos de información GIT, rechazará la llamada con el valor de causa 100 para el *contenido de elemento de información no válido* de acuerdo con 5.7.2/Q.2931. Si el intento de establecimiento del VC ATM es rechazado

porque el punto extremo de terminación no entiende el GIT, rechazará el establecimiento de comunicación VC con el número de causa 99, *Elemento de información inexistente o no implementado*, de acuerdo con 5.7.2/Q.2931.

Debe señalarse que el campo **portNumber** en H.245 sólo tiene 16 bits de longitud.

El **portNumber** H.245 es utilizado por el punto extremo receptor para asociar el VC ATM con el canal lógico RTP apropiado. El punto extremo que inicia la instrucción **openLogicalChannel** es el punto extremo que abre el VC ATM. Es posible que el punto extremo iniciador seleccione un **portNumber** H.245 que ya esté siendo utilizado por el punto extremo de recepción. Esto haría que fallara el procedimiento OLC.

Además, el puerto RTCP de recepción también lo especifica el punto extremo de iniciación por implicación. La presente Recomendación establece que los datos de RTCP correspondientes fluirán en un número de puerto UDP igual al **portNumber** H.245 más 1. Es posible que el número de puerto resultante para RTCP, el **portNumber** H.245 más 1, esté siendo utilizado en el punto extremo de recepción ya que el **portNumber** H.245 es seleccionado por el punto extremo de iniciación.

Debido a los problemas señalados, el punto extremo de recepción deberá tener la posibilidad de seleccionar el **portNumber** H.245. Si el **portNumber** no se especifica en el **openLogicalChannel**, el punto extremo de recepción especificará un **portNumber** en el mensaje **openLogicalChannelAck** (u **openLogicalChannel** en el caso de conexión rápida). Se recomienda que el punto extremo de transmisión no especifique un **portNumber** en el **openLogicalChannel**, exigiendo así que el punto extremo de recepción especifique uno en el mensaje **openLogicalChannelAck** (u **openLogicalChannel** en el caso de conexión rápida).

El campo **portNumber** del mensaje **openLogicalChannel** se utiliza para seleccionar el **portNumber** H.245. El punto extremo de recepción utiliza dicho número de puerto H.245 para asociar el VC ATM con el canal lógico RTP apropiado. Si el punto extremo de recepción encuentra que el **portNumber** H.245 dado es inadecuado, puede seleccionar un nuevo **portNumber** H.245 y utilizar el campo **portNumber** del mensaje **openLogicalChannelAck** (u **openLogicalChannel** en el caso de conexión rápida) para indicar el valor nuevo al punto extremo iniciador. El campo **portNumber** H.245 seleccionado es transportado en el elemento de información GIT. De esta manera, el lado de recepción puede asociar el VC ATM con el canal lógico RTP apropiado.

El número de puerto de asociación de VC se representa en el orden de octetos de la red en los octetos 6.2 y 6.3 del GIT (es decir, el octeto 6.2 contiene el MSB y el octeto 6.3 contiene el LSB).

C.4.1.2 Información de capa alta de banda ancha

Parámetros de ID	Valor	Notas
Longitud del contenido de B-HLI (octetos 3-4)	3	
Tipo de información de capa alta (octeto 5)	"0000 0001"	Específico del usuario
Información de capa alta (octetos 5-7)	**portNumber** H.245	**portNumber** H.245 de 16 bits con codificación binaria directa

La B-HLI sólo se utiliza para la retrocompatibilidad con puntos extremos H.323 versión 2, que se describe en C.3.7.2.

C.4.1.3 Parámetros de la capa de adaptación ATM

Parámetros de IE	Valor	Notas
Tipo de AAL (octeto 5)	"0000 0101"	AAL 5
Tamaño máximo hacia adelante de SDU CPCS de AAL 5 (octetos 6.1-6.2)	Tamaño MTU	El más pequeño de los dos valores **mTUsize** dados por **QoSCapability.atmParams** local y distante
Tamaño máximo hacia atrás de SDU CPCS de AAL 5 (octetos 7.1-7.2)	Tamaño MTU	Igual que hacia delante
Tipo de SSCS (octeto 8.1)	"0000 0000"	SSCS nulo

C.4.1.4 Elemento de información capacidad portadora de banda ancha ATM

a) En el caso de que el tipo de tráfico ATM en la Rec. UIT-T H.245 sea igual a "DBR":

Parámetro de IE	Valor	Notas
Clase portadora	BCOB-A	
Susceptibilidad al recorte	Susceptible al recorte	
Configuración de conexión del plano de usuario	Punto a punto	

b) En el caso de que el tipo de tráfico ATM en la Rec. UIT-T H.245 sea igual a "SBR1" con temporización extremo a extremo requerida:

Parámetro de IE	Valor	Notas
Clase portadora	BCOB-X	
Capacidad portadora de banda ancha	"0010011" (SBR1)	SBR1 con temporización extremo a extremo requerida
Susceptibilidad al recorte	Susceptible al recorte	
Configuración de conexión del plano de usuario	Punto a punto	

C.4.2 Utilización de H.245

El establecimiento de una comunicación H.323 con trenes de medios AAL 5 se efectúa de manera similar al modo básico de H.323 en IP. La diferencia es que el intercambio **openLogicalChannel** completado en H.245 debe dar lugar a que se establezca un VC AAL 5. Esto se ilustra en las figuras C.2 y C.3 para la utilización de VC unidireccional y la utilización de VC bidireccional respectivamente.

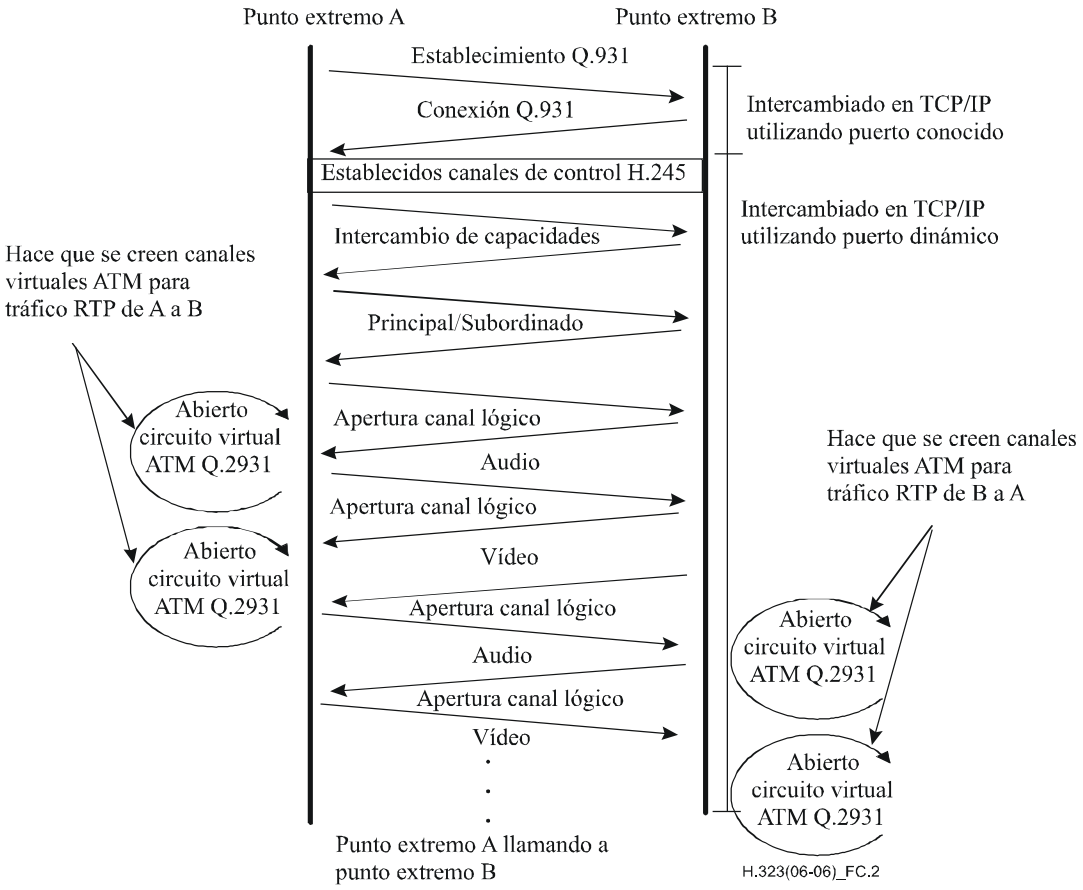


Figura C.2/H.323 – Establecimiento de la comunicación H.323 mostrando el efecto ATM – VC ATM utilizados unidireccionalmente

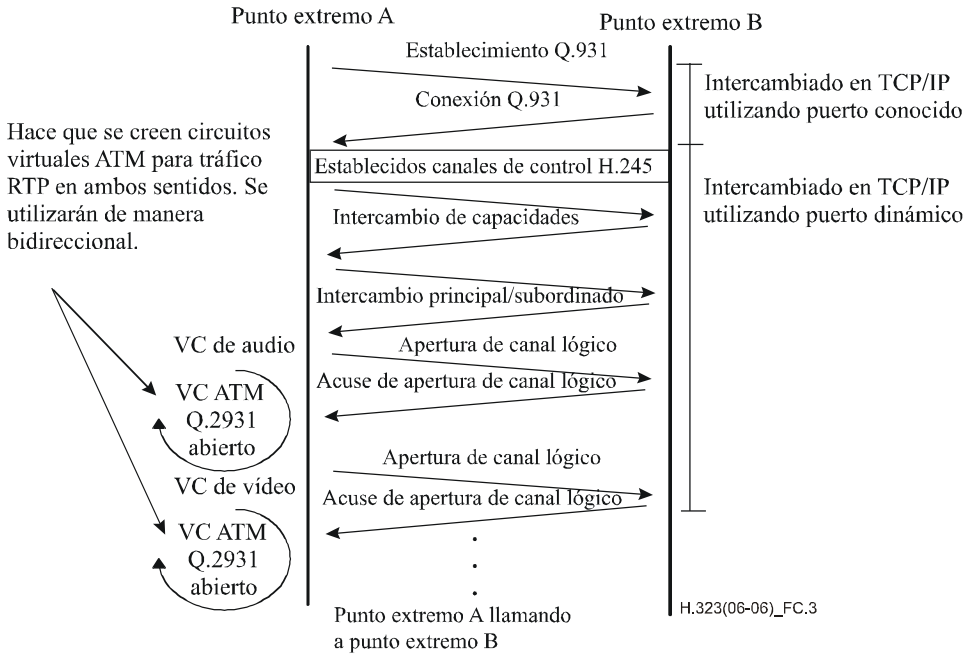


Figura C.3/H.323 – Establecimiento de la comunicación H.323 mostrando el efecto ATM – VC ATM utilizados bidireccionalmente

Debe señalarse que los establecimientos de VC ATM se producirán sólo en un sentido si se utilizan canales lógicos bidireccionales. En este caso, el punto extremo que acusa recibo de **openLogicalChanel** meramente vinculará la conexión ATM entrante a una sesión RTP utilizando el número de puerto de asociación de VC.

C.4.3 Utilización de RTP

RTP y RTCP se definen en el anexo A/H.225.0. RTCP se requiere actualmente para todas las conexiones H.323, por lo que se requiere aun cuando se utilice un VC AAL 5. El RTCP es transportado por UDP/IP, no directamente por el VC AAL 5.

C.4.4 Interfuncionamiento con H.323 en IP

Como las comunicaciones H.225.0 y H.245 se hacen en IP, el punto extremo podrá recibir llamadas de cualquier otro punto extremo que esté correctamente conectado a la red IP. Es posible que se utilicen puntos extremos H.323 en ATM que no soporten los métodos descritos en este anexo. Seguirán estrictamente el método básico de utilizar UDP/IP para los trenes A/V. En este caso, el punto extremo no declarará las nuevas **transportCapabilities** en H.245 y rehusará abrir canales lógicos utilizando VC direccionados en ATM.

El protocolo para **openLogicalChannel** utilizando VC AAL 5 para trenes A/V sólo debe utilizarse si las capacidades recibidas han indicado que se soporta el método de este anexo. Si este parámetro de capacidad no está presente en el conjunto de capacidades de terminal, el punto extremo sólo debería utilizar **openLogicalChannel** utilizando UDP/IP sobre ATM. Esto asegurará que el punto extremo pueda comunicar con otros puntos extremos que soportan H.323, pudiendo no soportar los métodos de este anexo.

Anexo D

Facsímil en tiempo real por sistemas H.323

D.1 Introducción

En la actualidad, el facsímil y las señales vocales se envían normalmente utilizando la RTPC con la misma infraestructura de llamada y direccionamiento. Es muy conveniente continuar con este enfoque en el contexto de la presente Recomendación. Desde un nivel superior, el facsímil puede ser considerado como otro tipo de tráfico en tiempo real similar a un determinado codificador de señales vocales. Esto parece ser lo apropiado, ya que el facsímil que entra en el mundo del empaquetado a través de una pasarela procedente de la RTPC debería ser tratado lógicamente de manera similar a las señales vocales si el cliente espera un servicio de transmisión de extremo a extremo en tiempo real asegurada. La conversión de facsímil a correo electrónico u otros métodos de almacenamiento y retransmisión representa un servicio nuevo que queda fuera del alcance de la presente Recomendación, que es un protocolo en tiempo real. Se reconoce la posibilidad de que los fabricantes deseen proporcionar una pasarela que permita el repliegue al servicio de almacenamiento y retransmisión cuando falle una llamada facsímil en tiempo real. La decisión de cómo y cuándo se hace esto, o utilizando qué medios se implementa un servicio facsímil con almacenamiento y retransmisión, queda fuera del ámbito de aplicación de la presente Recomendación.

La Rec. UIT-T T.38 [55] define un protocolo de facsímil Internet que consta de mensajes y datos intercambiados entre pasarelas facsímil conectadas por una red con protocolo Internet (IP, *Internet protocol*). En el presente anexo se hace uso de la Rec. UIT-T T.38. La comunicación entre las pasarelas y los terminales facsímil del grupo 3 y del grupo 4 queda fuera del alcance de aplicación de dicha Recomendación. En la figura D.1 se muestra el modelo de referencia de T.38 con tres

escenarios. En el primero de ellos, los dos terminales facsímil del equipo facsímil G3 (G3FE, *group 3 facsimile equipment*) tradicionales se conectan virtualmente a través de las pasarelas una vez establecidas las comunicaciones de la RTPC. Toda la negociación de capacidades y para el establecimiento de la sesión T.30 [54] se lleva a cabo entre los terminales. En el segundo escenario, el terminal facsímil del grupo 3 tradicional se conecta con un facsímil que funciona por Internet (IAF, *Internet aware fax*).

El IAF está conectado directamente a la red IP. En el tercer escenario, los dos IAF están conectados directamente a la red IP. En todos los escenarios, se utilizan paquetes T.38 en la red IP para comunicar información facsímil T.4 y T.30. El transporte de los paquetes T.38 se hace utilizando el protocolo de control de transmisión (TCP, *transmission control protocol*) por redes IP, el protocolo de datagramas de usuario (UDP, *user datagram protocol*) por redes IP (UDPTL) o el protocolo en tiempo real (RTP, *real time protocol*) con el mecanismo H.323.

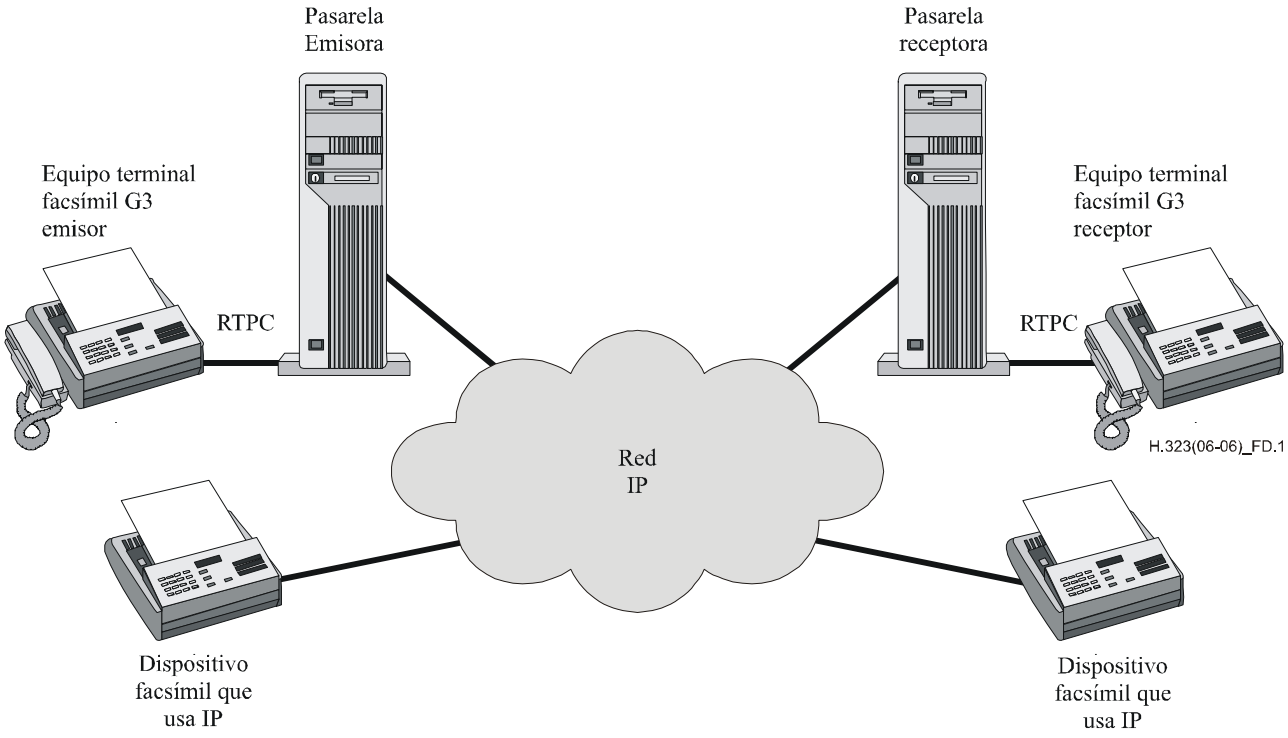


Figura D.1/H.323 – Modelo de transmisión facsímil por redes IP

D.2 Alcance

El presente anexo se refiere a la utilización de los procedimientos H.323 para transferir paquetes T.38 en tiempo real por la red IP. Las entidades H.323 que soporten capacidades facsímil deberán utilizar T.38 para la prestación de servicios facsímil en tiempo real, como se describe en este anexo.

Los puntos extremos con capacidad facsímil H.323 deberán soportar la utilización del TCP y el UDPTL tal como se describe en la Rec. UIT-T T.38 y, opcionalmente, pueden soportar el RTP. El anexo B/T.38 describe un terminal T.38 que sólo soporta un subconjunto de mensajes H.245 que utiliza la tunelización H.245. Sin embargo, el terminal del anexo B/T.38 puede interfuncionar con un terminal del anexo D utilizando los procedimientos de 8.1.7, "Procedimiento de conexión rápida" y de 8.2.1, "Encapsulado de mensajes H.245 dentro de mensajes de señalización de llamada H.225.0" de la presente Recomendación. Los terminales del anexo B/T.38 interfuncionan con los terminales H.323 sin ser conformes a esta Recomendación. Un terminal H.323 que soporte los procedimientos de este anexo deberá interfuncionar con los terminales del anexo B/T.38.

D.3 Procedimientos de apertura de canales para el envío de paquetes T.38

La conexión rápida se utiliza para describir los procedimientos H.323 de apertura de canales para el transporte de paquetes T.38. También se puede utilizar la secuencia tradicional, aunque no se describe aquí.

D.3.1 Apertura del canal vocal

Se pueden abrir cero, uno (canal de emisor a receptor o canal de receptor a emisor), o dos (canal de emisor a receptor y canal de receptor a emisor) canales lógicos vocales, dependiendo de la capacidad del emisor y del receptor. Si se desea un canal vocal, éste se abrirá como se especifica en los procedimientos de 8.1.7, "Conexión rápida". No es obligatorio el soporte de la voz por las aplicaciones facsímil en el presente anexo.

D.3.2 Apertura de los canales facsímil

Para la transferencia de los paquetes T.38 pueden abrirse dos canales lógicos unidireccionales que pueden ser fiables o no fiables (canal de emisor a receptor y canal de receptor a emisor), tal como se muestra en la figura D.2 u, opcionalmente, un canal bidireccional fiable, tal como se muestra en la figura D.3. Los paquetes T.38 se pueden transferir utilizando el TCP, el UDPTL o el RTP. En general, la utilización del TCP es más eficaz cuando la anchura de banda para la comunicación facsímil es limitada. Por otra parte, la utilización del UDPTL o el RTP puede ser más eficaz cuando la anchura de banda para la comunicación facsímil es suficiente.

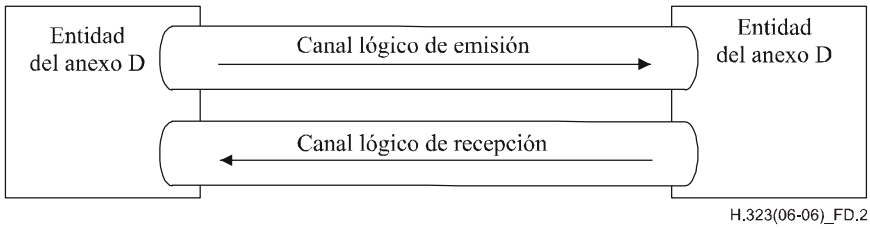


Figura D.2/H.323 – Pareja de canales unidireccionales

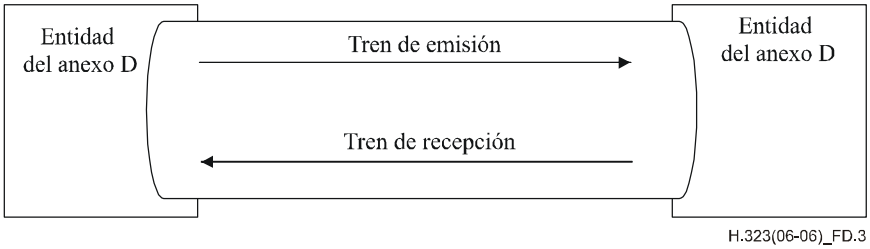


Figura D.3/H.323 – Un único canal bidireccional

NOTA – En la primera versión de este anexo, no era posible utilizar un único canal bidireccional fiable. Para asegurar la retrocompatibilidad, el punto extremo puede especificar el soporte de canales bidireccionales fiables incluyendo la SECUENCIA **t38FaxTcpOptions** (**opciones Tcp fax t38**) y fijando el campo **t38TCPBidirectionalMode** (**modo bidireccional TCP t38**) a VERDADERO. Si el otro punto extremo no incluye la SECUENCIA **t38FaxTcpOptions**, el punto extremo considerará que no se soporta un único canal bidireccional fiable y utilizará dos canales unidireccionales fiables o no fiables.

El terminal emisor especifica un puerto TCP/UDP en el procedimiento **OpenLogicalChannel** del elemento **fastStart** de *Establecimiento*. El terminal receptor deberá indicar su puerto TCP (o UDP) en el procedimiento **OpenLogicalChannel** del elemento **fastStart** tal como se especifica en los procedimientos de 8.1.7, "Conexión rápida".

El terminal receptor abrirá el puerto TCP/UDP en función de las preferencias del emisor. Si el terminal emisor prefiere UDPTL, RTP o TCP, lo indicará ordenando sus propuestas en la secuencia **fastStart** según se indica en 8.1.7.1. El terminal receptor puede seleccionar el protocolo de transporte, TCP o UDP, devolviendo las propuestas que desea en las estructuras **OpenLogicalChannel** del elemento **fastStart** de *Conexión*.

Las figuras D.4 y D.5 muestran la señalización utilizada en la apertura de canales unidireccionales y bidireccionales utilizando el procedimiento de conexión rápida.

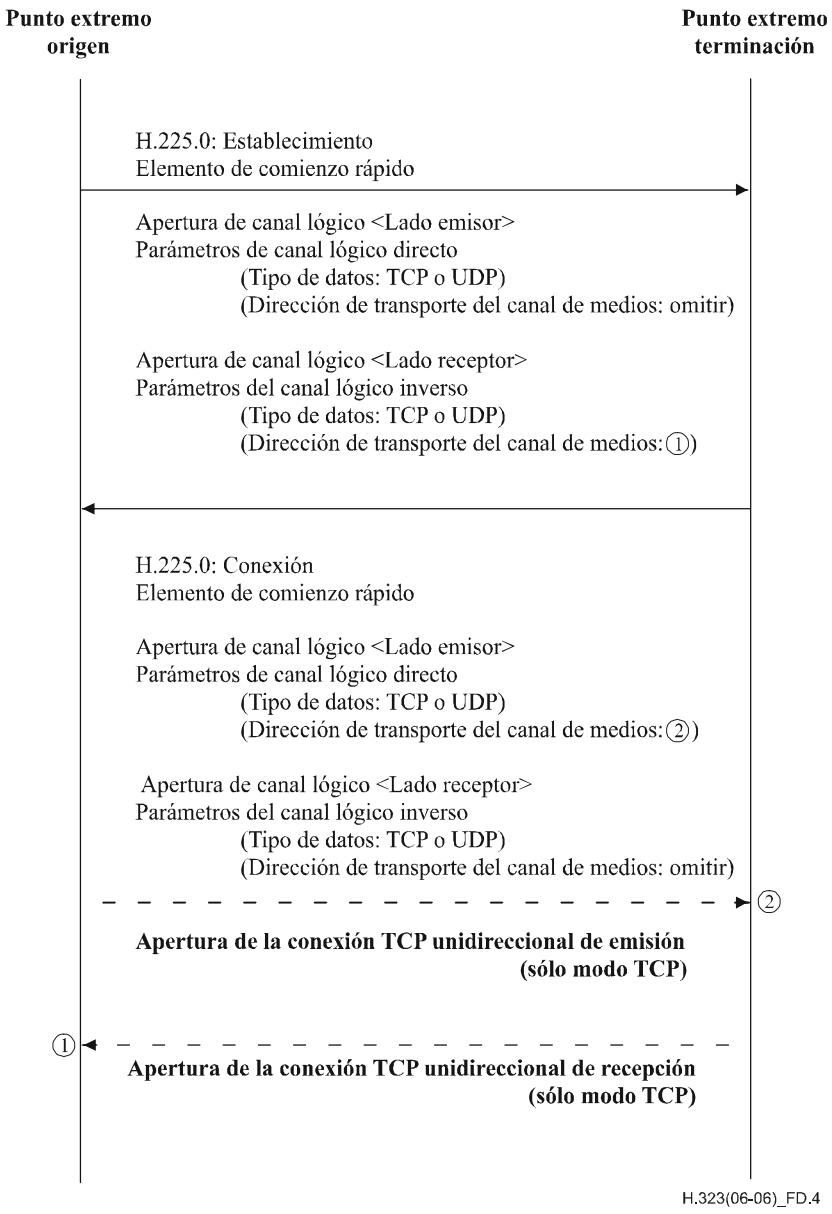


Figura D.4/H.323 – Dos canales unidireccionales con conexión rápida

En el ejemplo anterior, los canales T.38 se proponen como UDPTL o TCP. Para proponer un canal lógico unidireccional que utilice el RTP para transportar paquetes T.38, el parámetro de apertura de canal lógico de **tipo de datos** deberá fijarse en **datos de audio** y deberá incluir las capacidades de audio genérico H.245 para T.38 como se especifica en el anexo G/T.38.

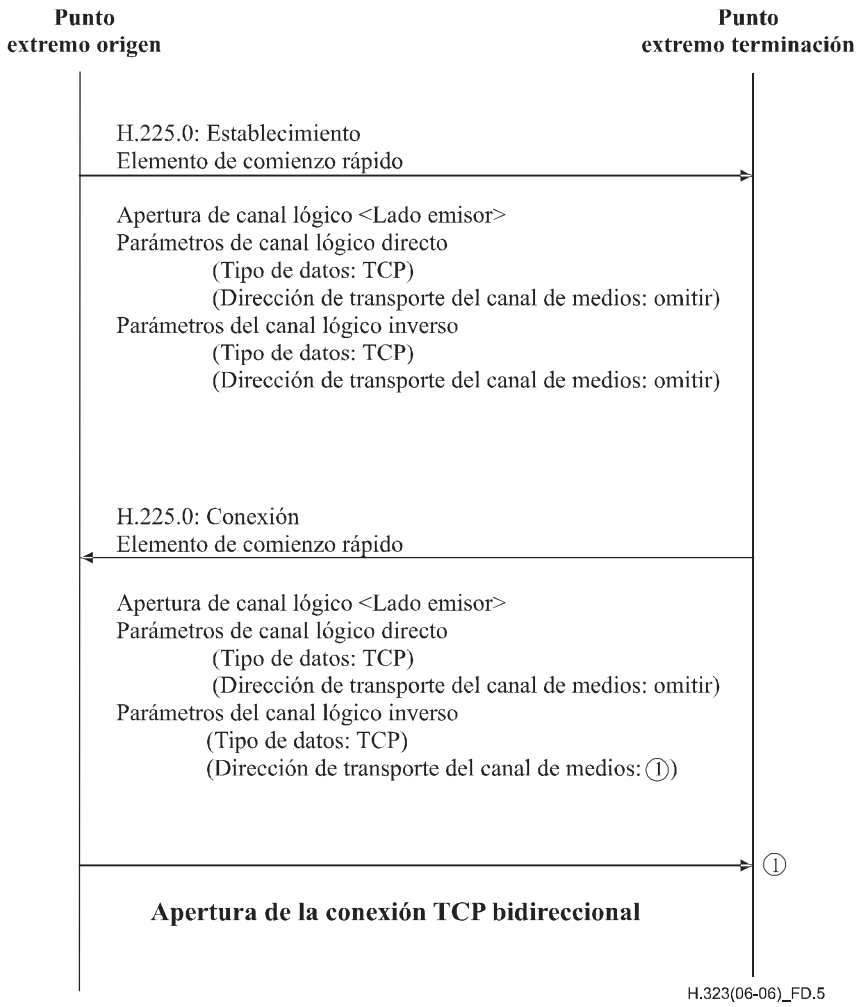


Figura D.5/H.323 – Un canal bidireccional fiable con conexión rápida

D.3.3 Transmisión de DTMF

Los tonos de multifrecuencia bitono (DTMF) deberán ser enviados por los terminales del anexo D, utilizando una **UserInputIndication** a efectos de interfuncionamiento con los terminales del anexo B/T.38. Los terminales del anexo D pueden enviar tonos DTMF dentro de banda con las señales vocales o a través de RFC 2833 cuando en la llamada no se utilicen los terminales del anexo B/T.38.

D.4 Procedimiento de conexión no rápida

Obsérvese que en la conexión no rápida pueden utilizarse los procedimientos **OpenLogicalChannel** normales H.245 para abrir y cerrar canales facsímil con UDPTL, RTP y TCP (véase 6.2.8.2). También puede utilizarse la señalización tunelizada H.245 la apertura y cierre de canales. Se señala asimismo que los procedimientos de conexión no rápida y no tunelizados H.245 no se aplican al interfuncionamiento con la Rec. UIT-T T.38.

Las figuras D.6 y D.7 muestran la señalización utilizada para la apertura de canales unidireccionales y bidireccionales cuando no se utiliza la conexión rápida.

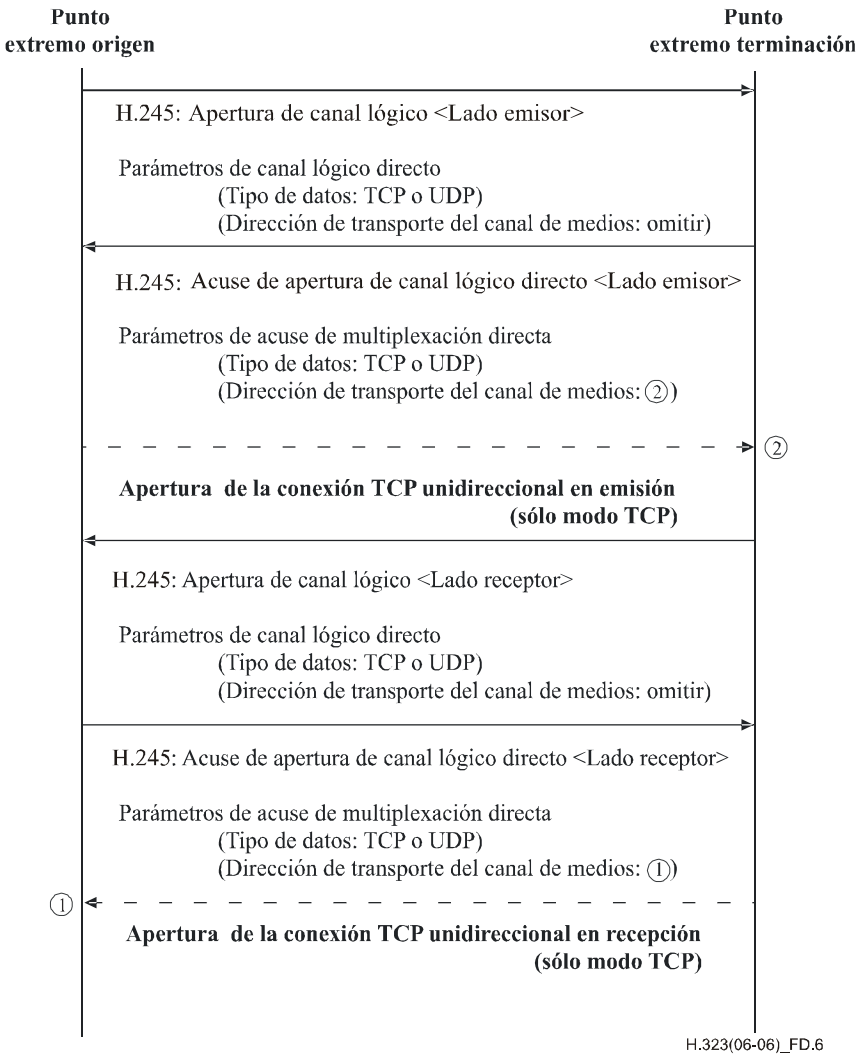


Figura D.6/H.323 – Dos canales unidireccionales sin conexión rápida

En el ejemplo anterior, los canales T.38 se proponen como UDPTL o TCP. Para proponer un canal lógico unidireccional que utilice el RTP para transportar paquetes T.38, el parámetro de apertura de canal lógico de **tipo de datos** deberá fijarse en **datos de audio** y deberá incluir las capacidades de audio genérico H.245 para T.38 como se especifica en el anexo G/T.38.

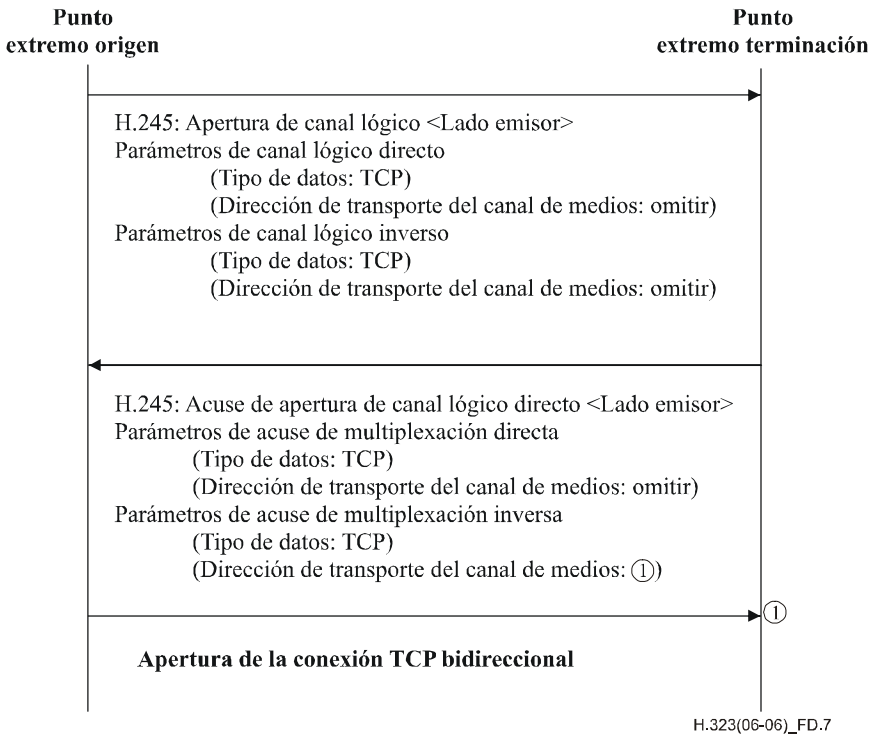


Figura D.7/H.323 – Un canal bidireccional sin conexión rápida

D.5 Sustitución de un tren de audio existente por un tren de facsímil T.38

Un punto extremo que desee sustituir un tren de audio existente por un tren de facsímil, utilizará el mecanismo siguiente.

Una vez que se haya establecido la comunicación de audio – idealmente utilizando una conexión rápida y con anterioridad a la recepción del mensaje CONEXIÓN – el punto extremo que desee sustituir el tren de audio por el facsímil T.38 iniciará los procedimientos H.245 haciendo uso de la tunelización si aún no se han iniciado los procedimientos H.245.

Durante el intercambio de capacidades H.245, cada punto extremo expresará cuál es su capacidad para la recepción y transmisión de facsímil T.38 mediante la inclusión del campo **t38fax** (**facsímil T.38**) de la estructura **DataApplicationCapability** (**capacidad de aplicación de datos**) y, opcionalmente, de las capacidades de audio genérico T38RTP especificadas en el anexo G/T.38. La presencia de estas capacidades indica que el punto extremo distante soporta el modo facsímil T.38.

Debe señalarse que el mensaje Conexión puede llegar mientras se está ejecutando los procedimientos H.245. Una vez que han finalizado los procedimientos H.245 y se ha recibido el mensaje Conexión, cualquiera de los puntos extremos puede detectar los tonos de facsímil (es decir, CNG o CED) o la presencia de una portadora V.21 y banderas de control de alto nivel de enlace de datos (HDLC, *high level data link control*). Los escenarios típicos de detección de llamada facsímil se basan en el análisis del tono llamante CNG y en una respuesta del tono de contestación CED y/o la iniciación de los procedimientos de facsímil que utilizan la portadora V.21 y las banderas HDLC. Se señala que, en algunas implementaciones, la presencia de CNG o CED es facultativa. Así pues, ambos puntos extremos deberán desempeñar un papel activo para detectar el facsímil adecuadamente.

Cuando se utilizan dos canales facsímil unidireccionales, el punto extremo que ha detectado el tono iniciará el procedimiento de petición de modo H.245 normalizado enviando el mensaje **requestMode** a su parte distante, siendo el modo solicitado modo datos **t38fax** o las capacidades de audio genérico T38RTP. El punto extremo que recibe el mensaje **RequestMode** devolverá un **requestModeAck** (**acuse de petición de modo**). Al recibir **requestModeAck**, el punto extremo iniciador cerrará su canal de audio y abrirá un canal lógico T.38. Igualmente, el extremo distante cerrará su canal lógico de audio y abrirá un canal lógico facsímil T.38. Después de que se hayan recibido acuses para cada uno de los canales lógicos T.38 abiertos, tiene lugar la transmisión y recepción facsímil.

En la figura D.8 se ilustra una transición exitosa de voz a facsímil cuando ya se ha abierto un canal H.245 separado para dos canales de medios unidireccionales. Obsérvese que en este diagrama y en los diagramas siguientes, los puntos extremos de origen y de terminación no necesariamente se refieren a los puntos extremos emisor y receptor o llamante y llamado. Cualquier punto extremo puede iniciar los procedimiento H.245 para efectuar la transición de la transmisión de voz a la transmisión facsímil.

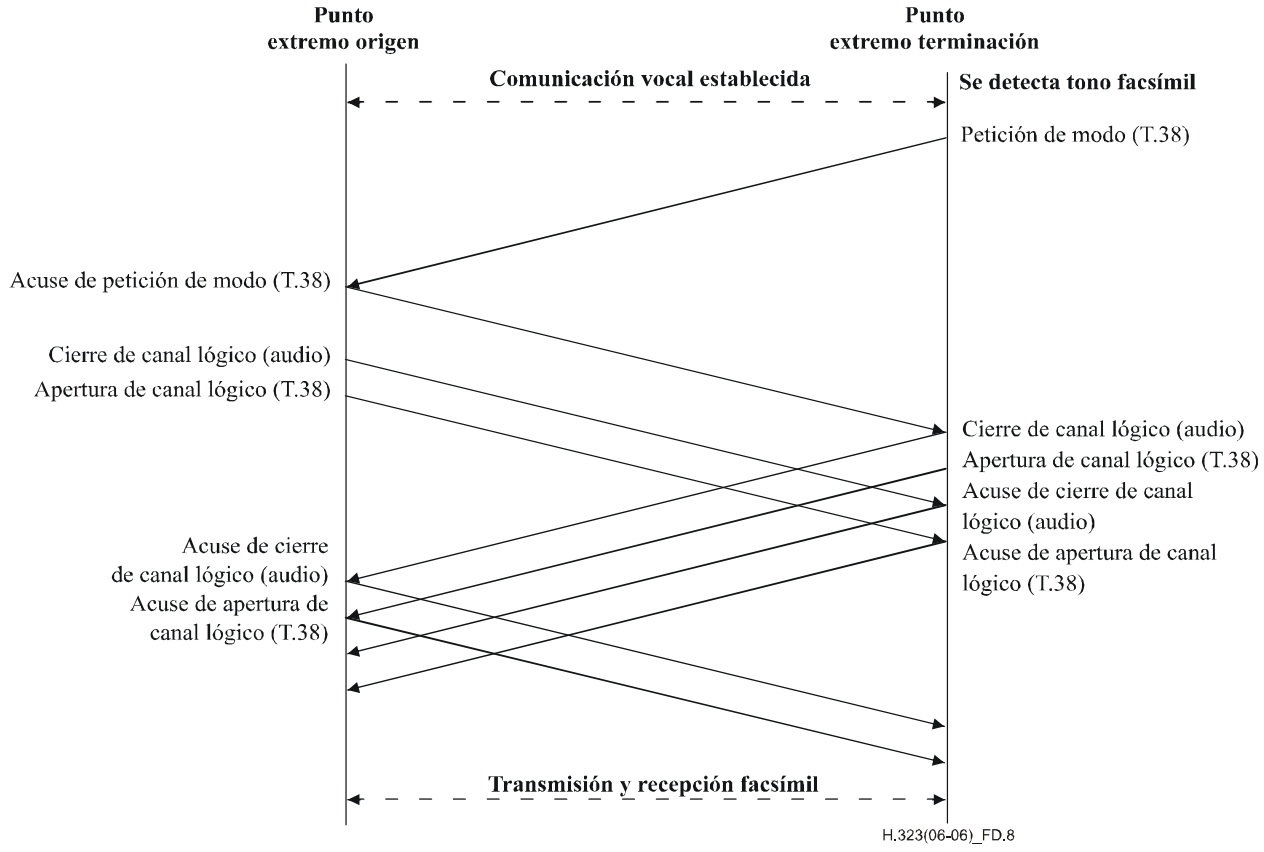


Figura D.8/H.323 – Conmutación exitosa de una llamada vocal existente a T.38 utilizando dos canales de medios unidireccionales sin tunelización

En la figura D.9 se muestra una transición exitosa de voz a facsímil utilizando la tunelización H.245 para dos canales de medios unidireccionales.

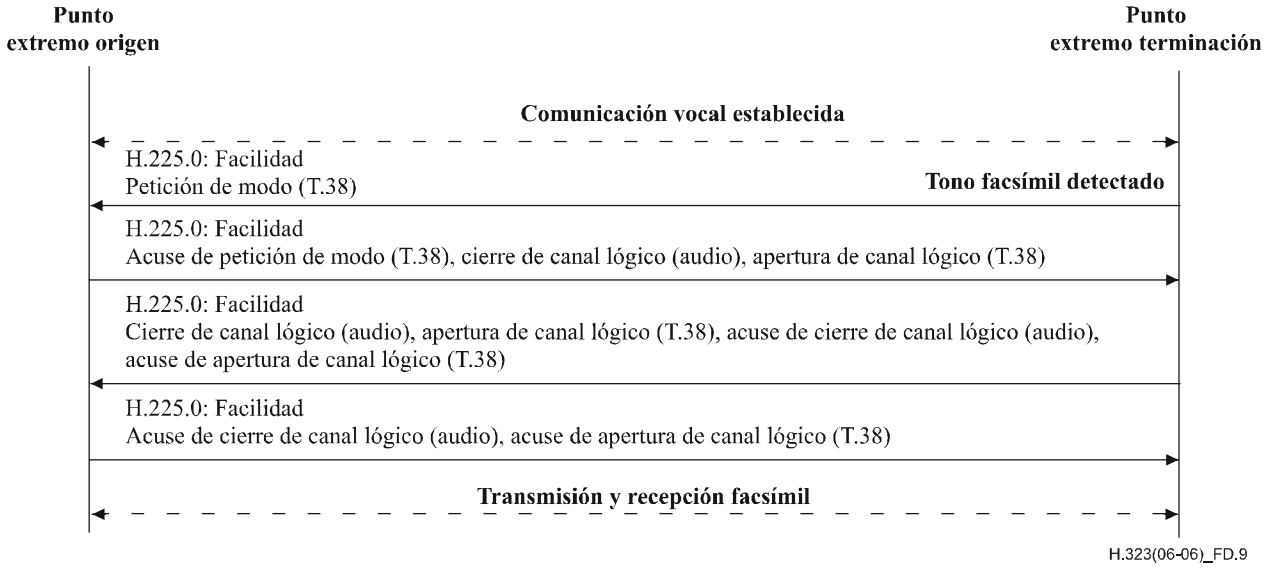


Figura D.9/H.323 – Conmutación exitosa de una llamada vocal existente a T.38 utilizando dos canales de medios unidireccionales con tunelización

Cuando se utiliza un canal facsímil bidireccional (sólo para TCP), la instrucción petición de modo no resulta necesaria: el punto extremo que ha detectado el tono cerrará sus canales abiertos, pedirá que el otro punto extremo cierre los canales inversos y abrirá un canal T.38 bidireccional. Cuando se recibe la instrucción petición de cierre de canal, el extremo distante cerrará su canal de audio. Después de que se hayan recibido los acuses de recibo para cada uno de los canales lógicos T.38 abiertos, se realiza la transmisión y recepción facsímil.

En la figura D.10 se muestra una transición exitosa de voz a facsímil cuando ya se ha abierto un canal H.245 separado para un canal de medios bidireccional.

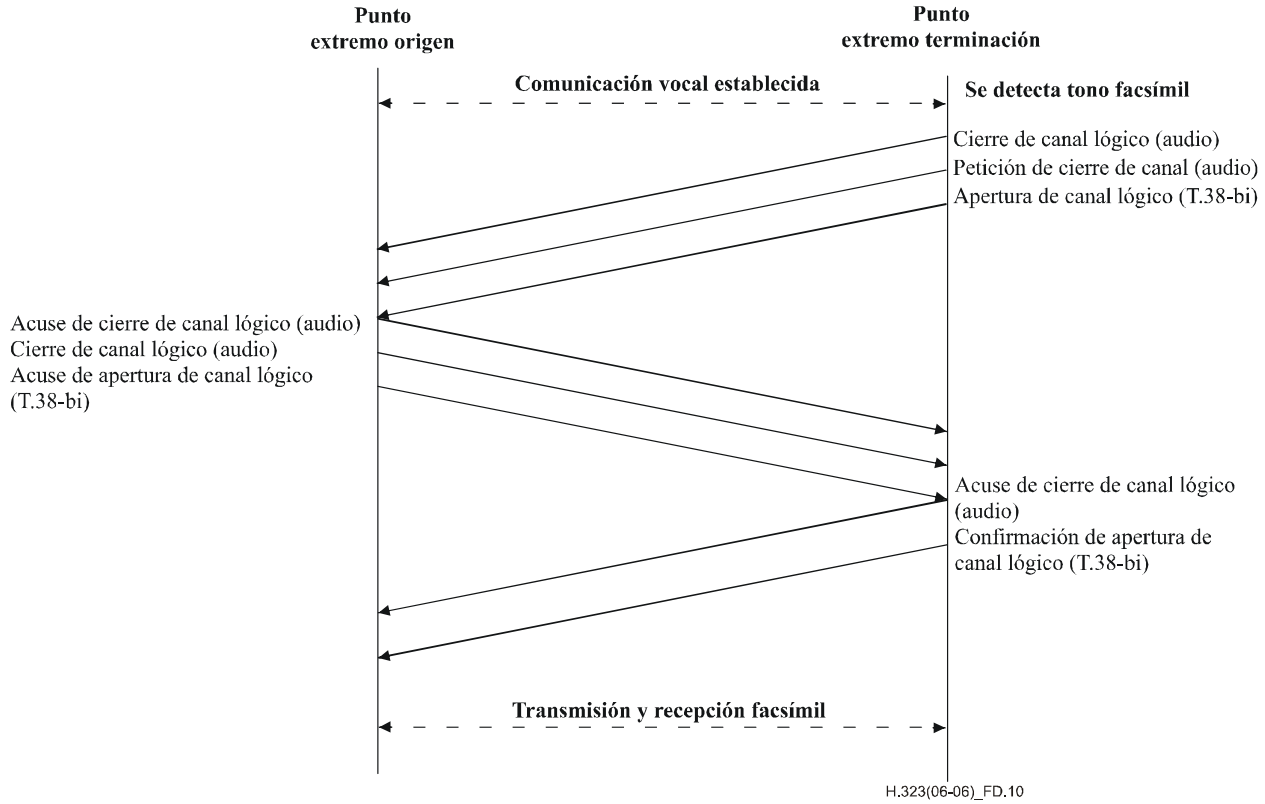


Figura D.10/H.323 – Transición exitosa de una llamada vocal existente a T.38 utilizando un canal de medios bidireccional (TCP) sin tunelización

En la figura D.11 se muestra una transición exitosa de voz a facsímil utilizando tunelización H.245 para un canal de medios bidireccional.

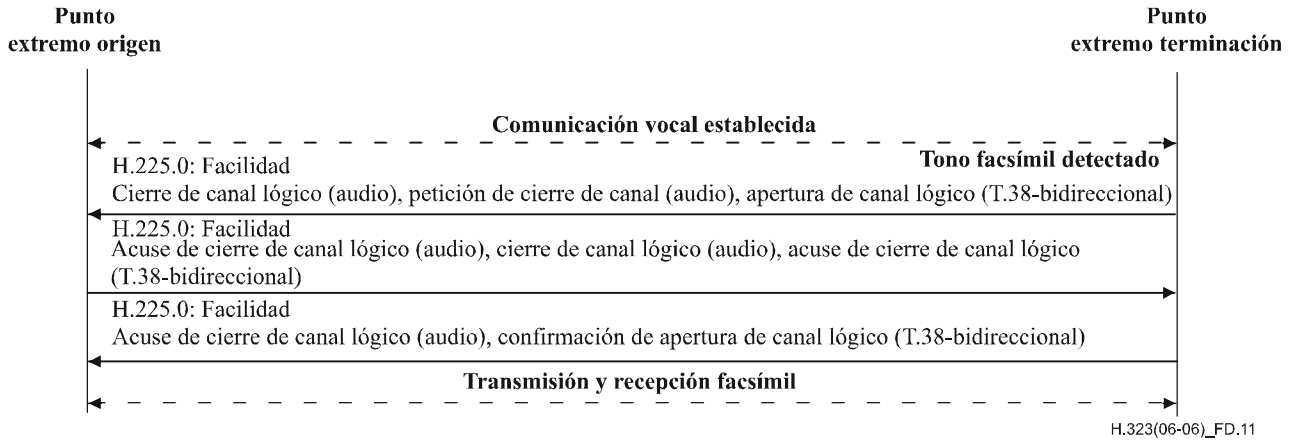


Figura D.11/H.323 – Transición exitosa de una llamada vocal existente a T.38 utilizando un canal de medios bidireccional (TCP) con tunelización

Si cualquiera de los puntos extremos desea volver a la situación de llamada de audio una vez que haya terminado la transmisión facsímil, se iniciará el procedimiento de petición de modo utilizando como parámetro un códec de audio. El procedimiento anterior también se aplica a los casos tradicionales de señalización de canal lógico H.245, si la conexión rápida no puede establecerse entre los dos puntos extremos.

D.6 Utilización de la velocidad máxima de bits (maxBitRate)/anchura de banda (bandWidth) en los mensajes

Cuando se utiliza el TCP para una transmisión fax a través del terminal T.38, la **bandWidth** (**anchura de banda**) en el ARQ/BRQ no incluye la velocidad de datos de fax, y si se desconecta un enlace de voz cuando comienza la transmisión de fax, deberá utilizarse un BRQ para indicar al controlador de acceso que la anchura de banda ha cambiado. Cuando se utiliza el UDPTL o el RTP para la transmisión de fax a través del terminal T.38, la **bandWidth** en el ARQ/BRQ incluye la velocidad de bits necesaria para la transmisión de fax. El punto extremo (terminal, pasarela) enviará BRQ al controlador de acceso si es necesario que la anchura de banda cambie durante la llamada. Se señala que la **maxBitRate** en el elemento **apertura de canal lógico** del mensaje Establecimiento durante la conexión rápida es diferente de la **bandWidth** en ARQ/BRQ y hace referencia a la máxima velocidad de bits que utilizará la llamada fax.

D.7 Interacciones con pasarelas y dispositivos del anexo B/T.38

Se debe considerar el caso siguiente:

Dispositivo del anexo D/H.323 (con señales vocales) <–> dispositivo del anexo B/T.38 (sin señales vocales).

Obsérvese que estos dispositivos pueden ser terminales o pasarelas; esa disyuntiva no afecta al análisis. Una llamada facsímil llega del lado "sin señales vocales", pero el lado con señales vocales debe generar una llamada vocal saliente no conectada a nada aunque se reproduzcan tonos o locuciones. En el sentido opuesto, el dispositivo del anexo D/H.323 no puede ofrecer una llamada vocal a un dispositivo "sin señales vocales", ya que éste no puede recibir voz.

La pasarela del anexo D/H.323 puede enviar un elemento **OpenLogicalChannel** de señales vocales y facsímil en el mensaje Establecimiento. Si encuentra un dispositivo T.38 sólo se abrirá el canal facsímil en caso de que ambos sean propuestos. Si la llamada encuentra por error un dispositivo H.323 no facsímil, no se abrirá el puerto facsímil. Esto es el equivalente a un aparato facsímil que llamara a un teléfono.

El dispositivo del anexo D/H.323 es consciente de que está hablando con un dispositivo del anexo B/T.38 por la siguiente secuencia de eventos:

1) Los dispositivos del anexo B/T.38 no indican ningún puerto H.245 en el mensaje Conexión ni en el mensaje Establecimiento.

2) El dispositivo del anexo D/H.323 utiliza el mensaje facilidad descrito en 8.2.3 y transmite un mensaje **FACILIDAD** con un **FacilityReason** de **startH245** (**comienzo de H245**) y proporciona su dirección H.245 en el elemento **H245Address** (**dirección H245**). El punto extremo del anexo B/T.38 que reciba un mensaje **FACILIDAD** cuyo **FacilityReason** sea **startH245**, responderá con un mensaje **FACILIDAD** cuyo **FacilityReason** sea **noH245**. En este punto, el dispositivo del anexo D/H.323 deberá cesar cualquier tentativa de abrir el canal H.245.

Anexo E

Marco y protocolo de redes alámbricas para el transporte de la señalización de llamadas multiplexadas

E.1 Alcance

En este anexo se describen un formato de paquetización y un conjunto de procedimientos (algunos de los cuales son facultativos) que pueden utilizarse para implementar protocolos basados en UDP y TCP. En la primera parte de este anexo se describen el marco de señalización y el protocolo de redes alámbricas, y en las cláusulas siguientes se detallan casos de usos específicos. El único perfil actualmente especificado en esta revisión es para transportar mensajes de señalización de llamada H.225.0.

Este anexo está concebido para ser utilizado en redes proyectadas y utiliza los servicios de seguridad proporcionados por H.323 (por ejemplo, IPSec H.235.0). Este anexo no debe utilizarse por la Internet pública por razones de seguridad y de tráfico.

E.1.1 Introducción

E.1.1.1 Transporte multiplexado

En este anexo se proporciona una capa de transporte multiplexado que puede utilizarse para transmitir múltiples protocolos (con fiabilidad facultativa) en la misma PDU. Los protocolos utilizados frecuentemente tienen puntos de código específicos (denominados también "tipos de cabida útil"). Pueden transportarse e identificarse otros protocolos utilizando las cabidas útiles del tipo ID de objeto.

E.1.1.2 Múltiples cabidas útiles en una sola PDU

Las PDU anexo E pueden contener múltiples "cabidas útiles", cada una con un protocolo diferente y destinadas a diferentes sesiones (la definición de una "sesión" depende del protocolo). Se señala que no existe una relación implícita entre las cabidas útiles cuando llegan en la misma PDU.

E.1.1.3 Opciones de encabezamiento flexible

Las PDU y los encabezamientos de cabida útil anexo E son configurables. El tamaño mínimo del encabezamiento es de 8 octetos y el máximo de 20 octetos cuando todos los campos facultativos están presentes.

E.1.1.4 Mensaje de acuse de recibo (Ack)

Los mensajes transportados utilizando un UDP pueden perderse. Si la aplicación necesita la garantía de que el mensaje enviado ha llegado con éxito, puede pedir un mensaje de acuse de recibo (Ack) de la PDU.

El emisor especificará en el campo <ackRequested> si desea recibir el mensaje Ack de una PDU que se haya enviado, y el receptor responderá con una parte útil Ack si se ha fijado el campo <ackRequested>.

NOTA – Los mensajes Ack serán enviados por la capa de transporte anexo E, y no por la aplicación utilizando la pila anexo E. El comportamiento específico de los Ack está dictado por el modelo de señalización que la pila anexo E ha encargado que utilice la aplicación.

E.1.1.5 Mensaje de acuse de recibo negativo (Nack*)*

Los mensajes de acuse de recibo negativo Nack se utilizarán para indicar errores. Dichos errores pueden ser la incapacidad de soportar un tipo específico de cabida útil, la llegada de una PDU mal formada u otros. Estos mensajes pueden tener o no como consecuencia la interrupción de una llamada en curso.

NOTA – Los mensajes Nack han de ser enviados por la capa de transporte anexo E, y no por la aplicación utilizando la pila del presente anexo.

E.1.1.6 Política relativa al número de secuencia de emisor

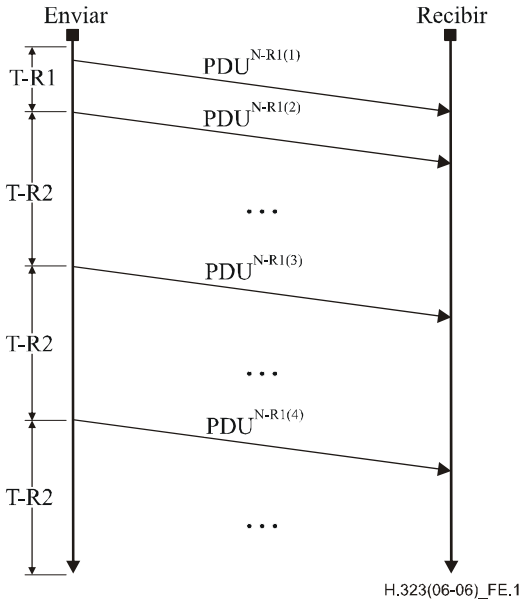
Asignadas por dirección del anfitrión y puerto de origen, el envío de las capas anexo E comenzará por un valor aleatorio que aumentará en 1 en cada PDU enviada. Si el número de secuencia llega a 2^{24} (16 777 216), volverá a 0.

E.1.1.7 Política relativa al número de secuencia de receptor

Al recibir un paquete de UDP, la capa anexo E deberá comprobar la dirección del anfitrión, puerto de origen y número de secuencia para reconocer los mensajes duplicados. La capa anexo E puede reordenar los mensajes según los números de secuencia y reconocer la pérdida de paquetes si detecta ausencias entre los números de secuencia.

E.1.1.8 Retransmisiones

Cuando se pierda un mensaje (y se hubiera pedido un Ack que no se ha recibido), el emisor puede retransmitir el mensaje. La retransmisión tiene por objeto remediar la pérdida del primer mensaje retransmitiéndolo rápidamente, pero si este otro mensaje se pierde también, se pide al emisor que reduzca el retardo de retransmisión aplicando un factor superior a dos. Véase la figura E.1.



Temporizadores y contadores de retransmisión:

Ítem	Valor	Comentarios
T-R1	500 ms	Se ha elegido aquí un valor razonablemente pequeño para compensar la posible pérdida del primer paquete
T-R2	(T-R1 | T-R2) × N-R2	Si se pierde el primer paquete retransmitido, aplíquese una cierta reducción. Si hay disponible un valor T-R2 anterior, utilícese el lugar del valor inicial (T-R1).
N-R1	8	Número máximo de retransmisiones antes de abandonar la conexión
N-R2	2,1	Multiplicador a utilizar para la reducción

Figura E.1/H.323 – Retransmisión de PDU

Cuando se conoce el valor de intervalo del mensaje de ida y vuelta por una transmisión anterior, el temporizador T-R1 debe ponerse al valor de dicho intervalo de mensaje de ida y vuelta +10%.

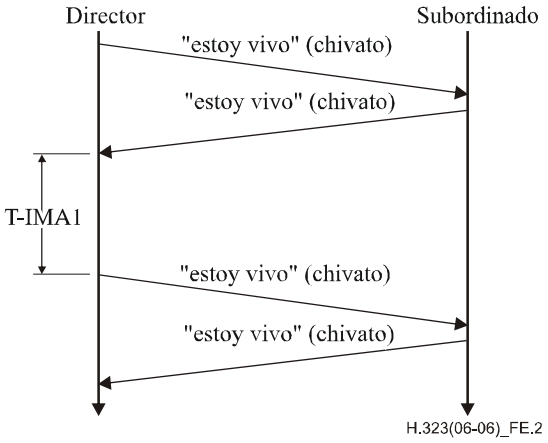
E.1.1.9 Conexión keep-alive (mantener vivo)

Cuando se activa un TCP, la presencia de una conexión TCP persistente puede garantizar que un lado conoce los fallos del lado distante (observando los fallos del TCP). Cuando se activa un UDP, no existe ese "estado" asociado, y debe utilizarse otro procedimiento.

La solución es que un extremo de la llamada (normalmente el extremo "servidor" o "director", si tal clasificación es pertinente) envíe un mensaje "estoy vivo" ("I-Am-Alive") al otro extremo, para que la aplicación distante sepa que el anfitrión todavía está activo. El lado distante responderá con un mensaje "estoy vivo" como prueba de que también está activo. El originador de la secuencia "estoy vivo" puede proporcionar un chivato (cookie) que, de estar disponible, se devolverá en la respuesta "estoy vivo".

El temporizador de retransmisión de los mensajes "estoy vivo" puede ser reiniciado al recibir otro mensaje pertinente, ya que ello prueba al extremo distante que está activo. Así se ahorra anchura de banda, porque los mensajes "estoy vivo" sólo se enviarán cuando realmente sean necesarios. Esta capacidad se decide protocolo por protocolo.

La generación de mensajes "estoy vivo" es facultativa, pese a lo cual todas las entidades deberán disponer de la capacidad de responder a mensajes "estoy vivo" (lo cual quiere decir que la capacidad y el requisito de responder a un mensaje "estoy vivo" no son facultativos, y siempre que se reciba este tipo de mensajes deberá responderse de acuerdo con los procedimientos definidos en el presente anexo). Véase la figura E.2.



Temporizadores "estoy vivo"

Ítem	Valor	Comentarios
T-IMA1	6 segundos	Intervalo de transmisión de "estoy vivo" (nota)
N-IMA1	6	Número de mensajes "ESTOY VIVO" consecutivos a los que no se ha respondido después de que el par distante es declarado muerto
NOTA – Estos temporizadores deben ajustarse a los valores recomendados en el anexo R cuando entre estas dos entidades se utilice también el anexo R.		

Figura E.2/H.323 – Transmisión "estoy vivo"

E.1.1.10 Corrección de errores sin canal de retorno

Los mensajes anexo E pueden enviarse más de una vez para permitir la corrección de errores sin canal de retorno. Si la llegada de un mensaje es crucial, la capa anexo E puede optar por enviar el mismo mensaje dos veces (sin incrementar el número de secuencia). Si llegan ambos mensajes, el segundo será tratado según los procedimientos normales de duplicación de mensajes.

E.1.1.11 Sugerencias de respuesta

Es conveniente que los implementadores anexo E añadan un pequeño retardo antes de devolver un mensaje Ack, para que la aplicación pueda adjuntar una cabida útil de protocolo que acompañe a la cabida útil del Ack. Se dispone de una opción de encabezamiento que permite a los emisores indicar a la capa de transporte distante que se espera la respuesta a un mensaje determinado.

NOTA – Por ejemplo, si se envía un mensaje ESTABLECIMIENTO H.225.0, la pila puede retardar ligeramente la respuesta de cabida útil Ack cuando se haya fijado a 1 el bit de indicación de respuesta para asegurar que la aplicación tendrá tiempo de proporcionar la cabida útil CONEXIÓN de retorno (por ejemplo). La PDU que se devuelva contendrá entonces un Ack (del mensaje ESTABLECIMIENTO) y la cabida útil CONEXIÓN.

E.1.1.12 Puerto conocido y generación de puerto

El presente anexo soporta un puerto conocido principal (puerto 2517 UDP/TCP). Cuando las aplicaciones que soportan operaciones anexo E, reciben una cabida útil que el puerto conocido principal no soporta (identificada utilizando el tipo de cabida útil estático o el tipo de cabida útil ID de objeto) pueden responder con un mensaje Nack que ordena al emisor que envíe ese tipo específico de cabida útil a un puerto y una dirección IP diferentes.

E.1.2 Modelos de señalización

La señalización puede seguir muchos modelos. Toda implementación de protocolo que utilice el presente anexo deberá soportar uno de los modelos que se describen a continuación o el elegir un modelo diferente de señalización que corresponda a sus necesidades.

E.1.2.1 Modelo en tiempo real

Según el modelo en tiempo real, si se pierde una PDU, es inútil volver a enviar la PDU, porque la información puede ser ya irrelevante. Un ejemplo de ese protocolo es el RTP cuando se utiliza para flujo continuo de audio o vídeo en tiempo real. Para tales protocolos, el retardo causado por la retransmisión es peor que la pérdida de la información.

Cuando se emplee este modelo, deberá ponerse a 0 siempre la bandera Ack.

E.1.2.2 Modelo en serie

En el modelo en serie, cuando se envía una PDU, la capa anexo E espera hasta que se devuelve una respuesta positiva para el mismo identificador de sesión. Este comportamiento se utiliza con protocolos que no pueden aceptar la llegada de mensajes de fuera de servicio y requieren operaciones en tiempo real mientras se envían pequeñas cantidades de información. Un ejemplo de este tipo de protocolos es el de Q.931.

Cuando se emplee este modelo, deberá fijarse siempre la bandera Ack para los mensajes de tipo estático. A menos que se especifique lo contrario, las implementaciones anexo E utilizarán los temporizadores (**T-R1** y **T-R2**) y el contador (**N-R1**) de retransmisión por defecto.

E.1.2.3 Modelo mixto

El modelo mixto quizás conlleve el entrelazado de la máquina de estados de protocolos y la máquina de estados anexo E. Tales implementaciones pueden utilizar el bit Ack cuando así convenga.

Cuando se emplee este modelo, la utilización de la bandera Ack puede estar prohibida, ser facultativa o ser obligatoria, según prescriba el protocolo.

E.1.2.4 Anexo E con TCP

Es posible hacer uso del presente anexo aplicando el TCP. Cuando así sea, no se utilizará el mensaje Ack. Además, se fijará el bit L en el encabezamiento de la PDU, lo que hará que pueda disponerse de los campos de cuenta de cabida útil o longitud de PDU.

E.1.3 Campos facultativos de cabida útil

E.1.3.1 Identificador de sesión

Las cabidas útiles anexo E soportan un campo facultativo de sesión que puede utilizarse para identificar una sesión en el transporte multiplexado al que pertenece la cabida útil. El campo sesión tiene una longitud de 16 bits.

NOTA – Este campo puede utilizarse, por ejemplo, para transportar el CRV (es decir, valor de referencia de llamada, que se define en la Rec. UIT-T Q.931) en mensajes H.225.0. La interpretación del campo de sesión depende del protocolo.

E.1.3.2 Identificador de dirección fuente/destino

Las cabidas útiles anexo E soportan un campo de fuente/destino facultativo que puede utilizarse para identificar la fuente, el destino (o ambos) de la cabida útil. El campo de fuente/destino tiene una longitud de 32 bits.

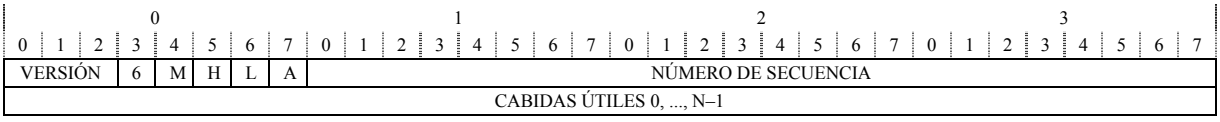
NOTA – Este campo puede utilizarse, por ejemplo, en la Rec. UIT-T H.283 para expresar la dirección [<M><T>] que identifica el nodo fuente del paquete, y la dirección [<M><T>] que identifica el nodo destino del paquete. La interpretación del campo de fuente/destino depende del protocolo.

E.1.4 Protocolo de redes alámbricas

El transporte anexo E utiliza la codificación binaria que se define en el resto de esta subcláusula. Las estructuras y campos de multiocteto deberán utilizar ordenación de octetos de red (por ejemplo de grandes extremos (big-endian)).

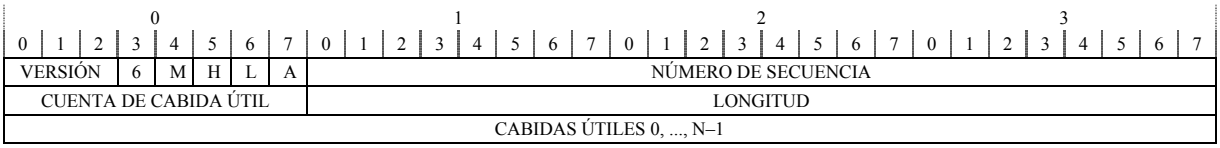
E.1.4.1 Estructura de encabezamiento

Para codificar el encabezamiento anexo E se utilizará la siguiente estructura. Si el bit L se pone a 0 (y por lo tanto no hay indicación de cuenta de cabida útil o de la longitud de la PDU), la longitud de las cabidas útiles dentro del mensaje, así como su número pueden deducirse, del tamaño del mensaje, del que informa la capa de transporte. Véanse las figuras E.3 y E.4.



Campo	Contenido de los campos	Bits
VERSIÓN	Entero sin signo; los emisores deberán fijar este campo a cero. La versión número 7 está reservada para uso experimental y deberá ignorarse en implementaciones comerciales	3
6	Cuando se ha liberado, significa que todas las direcciones IP cumplen IPv4 (utilizando 32 bits). Cuando se fija, significa que todas las direcciones IP cumplen IPv6 (utilizando 128 bits)	1
M	Bit de multidifusión. Si se fija, la PDU se envía utilizando multidifusión, si se libera, la PDU era unidifusión. Los emisores deberán enviar este bit si la PDU era multidifusión, o en otro caso deberán liberar el bit	1
H	Bit de indicación de respuesta – Cuando se fija, este mensaje genera una respuesta, por ejemplo, el mensaje Ack deberá retardarse para dar a la aplicación la oportunidad de proporcionar una cabida útil de respuesta con la cabida útil de Ack	1
L	Indicador de longitud. Si está presente, hay 4 OCTETOS adicionales que contienen el número de cabidas útiles de la PDU (8 bits) y la longitud total (en OCTETOS) de la PDU (24 bits)	1
A	Booleano: VERDADERO indica que se pide un Ack de esta PDU	1
NÚMERO DE SECUENCIA	Entero sin signo entre 0 y 16 777 215: el número de secuencia de esta PDU	24
CABIDA(S) ÚTIL(ES)	Secuencia de estructuras de cabida útil	$8 \times n$

Figura E.3/H.323 – Estructura de encabezamiento cuando el bit L está puesto a 0



Campo	Contenido de los campos suplementarios del bit L	Bits
CUENTA DE CABIDA ÚTIL	Número total de cabidas útiles de PDU −1 (por ejemplo, 0 significa que hay una cabida útil, 1 significa que hay dos, etc.)	8
LONGITUD	Longitud total en OCTETOS de todas las cabidas útiles (excluido el encabezamiento)	24

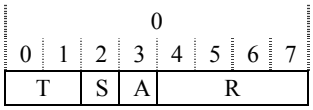
Figura E.4/H.323 – Estructura de encabezamiento cuando el bit L está fijado

E.1.4.2 Estructura de cabida útil

Deberán utilizarse las siguientes estructuras para codificar las cabidas útiles anexo E.

E.1.4.2.1 Banderas de encabezamiento de cabida útil

Cada cabida útil comienza con un OCTETO de banderas, que describe los campos facultativos que hay en el encabezamiento de cabida útil. Véase la figura E.5.



Campo	Contenido de los campos	Bits
T	Dos bits que definen el tipo de identificación de cabida útil: **00**: mensajes de transporte anexo E **10**: mensajes de tipo cabida útil estática **01**: mensajes de tipo IDENTIFICADOR DE OBJETO **11**: reservada para uso futuro	2
S	Indica la presencia de un campo de sesión	1
A	Indica la presencia de un campo de dirección de fuente/destino	1
R	Reservada para uso futuro, los emisores deberán fijarla a 0	4

Figura E.5/H.323 – Banderas de cabida útil

E.1.4.2.2 Mensajes de transporte anexo E

Los bits T del OCTETO de banderas de encabezamiento de cabida útil se pondrán a 0 (cero) en todos los mensajes de transporte anexo E. El octeto siguiente indicará el mensaje de transporte anexo E que sigue. Los bits S y los bits A se pondrán a 0. Véase la figura E.6.

Valor	Interpretación
0	Mensaje "estoy vivo"
1	Mensaje Ack
2	Mensaje Nack
3	Mensaje de rearranque
4..255	Reservados para uso futuro

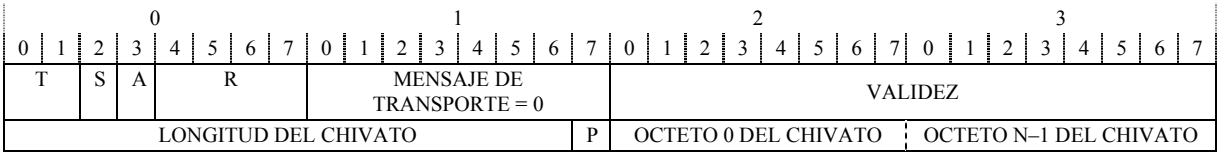
Figura E.6/H.323 – Mensajes de transporte del presente anexo

E.1.4.2.2.1 Mensaje "estoy vivo"

Se utilizará la siguiente estructura para codificar las cabidas útiles de los mensajes "estoy activo" anexo E. El octeto de mensaje de transporte se fijará a 0 (cero). El periodo de validez se expresa en centenas de milisegundos.

- Si el bit respuesta pedida (**P**) está fijado, el receptor deberá responder con un mensaje de "estoy vivo" con el chivato (si se dispone de él).
- Respuesta pedida no es lo mismo que Ack pedido en el encabezamiento de la PDU, que genera un mensaje Ack. Respuesta pedida genera un mensaje "estoy vivo".
- Si el periodo de validez se ha fijado a 0 (cero), deberá utilizarse el temporizador **T-IMA1**.
- Las PDU que contengan sólo una cabida útil de "estoy vivo" pondrán a 0 el bit Ack en el encabezamiento de PDU.

Véase la figura E.7.

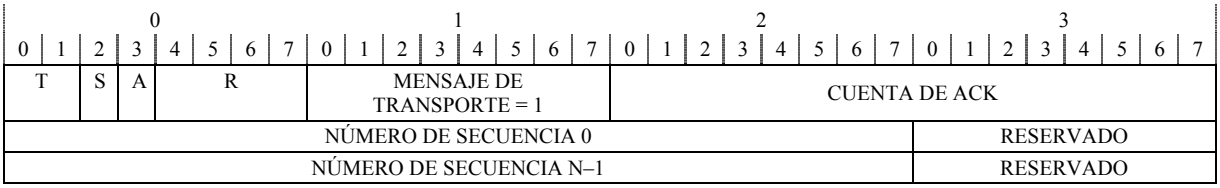


Campo	Contenido de los campos	Bits
VALIDEZ	Entero sin signo: tiempo, expresado en centenas de milisegundos, durante el cual es válido este mensaje "estoy vivo"	16
LONGITUD DEL CHIVATO	Longitud (en BYTES u OCTETOS) del campo del CHIVATO	15
P	Respuesta pedida	1
CHIVATO	BYTES u OCTETOS del chivato	8 × n

Figura E.7/H.323 – Mensaje "estoy vivo"

E.1.4.2.2.2 Mensaje de acuse de recibo (Ack)

Se utilizará la siguiente estructura para codificar los mensajes Ack. El octeto de mensaje de transporte se fijará a 1 (uno). Las PDU que contengan sólo una cabida útil Ack pondrán a 0 el bit Ack en el encabezamiento de PDU. Véase la figura E.8.

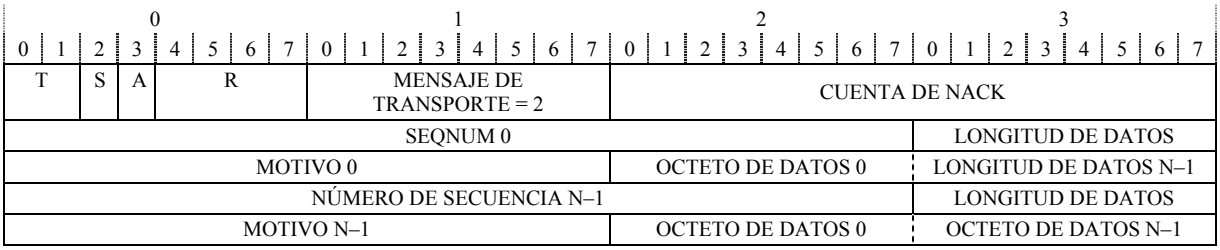


Campo	Contenido de los campos	Bits
CUENTA DE ACK	Número de campos de NÚMERO DE SECUENCIA que siguen a continuación	16
NÚMERO DE SECUENCIA 0, ... , N–1	Números de secuencia de las PDU de las que se hace acuse de recibo	24 × n
RESERVADO	Reservado para uso futuro	8 × n

Figura E.8/H.323 – Cabida útil de Ack

E.1.4.2.2.3 Mensaje de acuse de recibo negativo (Nack)

Se utilizará la siguiente estructura para codificar los mensajes Nack. El octeto de mensaje de transporte se fijará a 2 (dos). El mensaje deberá utilizarse para señalar errores transitorios, o errores más serios, tales como la llegada de un mensaje mal formado. Deberán ignorarse los mensajes Nack inesperados (como los que tienen números de secuencia ilegales). Véase la figura E.9.



Campo	**Contenido de los campos**	**Bits**
CUENTA DE NACK	Número de campos de NÚMERO DE SECUENCIA que siguen a continuación	16
NÚMERO DE SECUENCIA 0, ... , N–1	Números de secuencia de las PDU de las que se hace ACUSE DE RECIBO NEGATIVO	24 × n
LONGITUD 0, ... , N–1	Longitud de los datos específicos del Nack	8 × n
MOTIVO 0, ... , N–1	Motivo del NACK	16 × n
OCTETOS	Octetos de los datos específicos del Nack	8 × n

Motivo Valor	**Significado del motivo del Nack**	**Longitud de los datos del Nack en octetos**	**Datos**
0	Motivo no normalizado	1 + n	OCTETO DE LONGITUD seguido por OCTETOS DE IDENTIFICADOR DE OBJETO
1	Se pide al emisor que utilice un puerto alternativo para el tipo de cabida útil estático especificado	8	Los definidos en la figura E.10
2	Se pide al emisor que utilice un puerto alternativo para el tipo de cabida útil de ID de objeto	1 + n + 6	Los definidos en la figura E.11
3	Cabida útil de transporte no soportada	1	Entero sin signo
4	Tipo de cabida útil estático no soportado	1	Entero sin signo; cabida útil definida en el protocolo de tipo estático que no es soportado
5	Cabida útil de ID de objeto no soportada	1 + n	OCTETO DE LONGITUD seguido por OCTETOS DE IDENTIFICADOR DE OBJETO
6	Cabida útil alterada	1	Número de la cabida útil del mensaje que está alterada
7.. 65535	Reservado para uso futuro		

Figura E.9/H.323 – Mensaje Nack

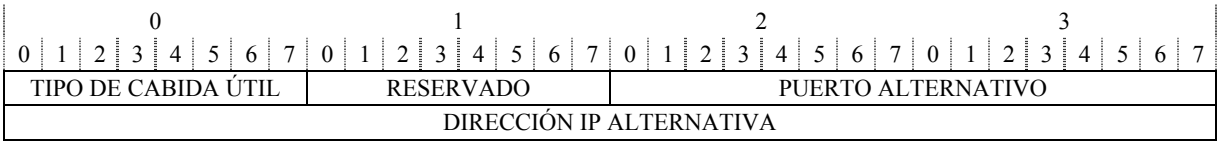


Figura E.10/H.323 – Estructura del motivo 1 de Nack

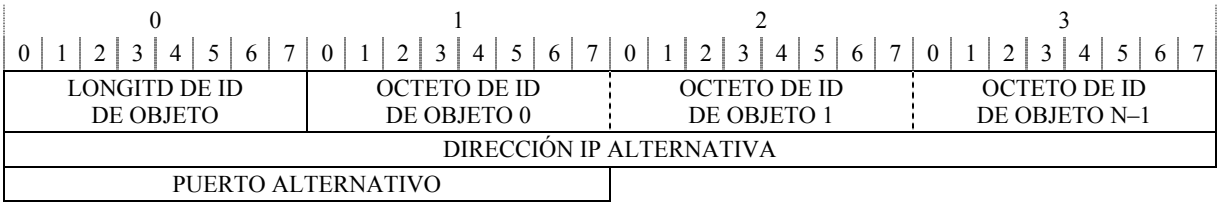


Figura E.11/H.323 – Estructura del motivo 2 de Nack

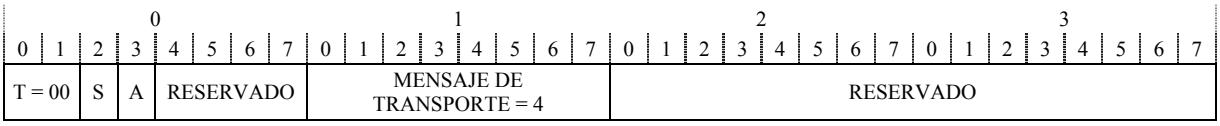
Si la dirección IP se ha fijado a cero, deberá utilizarse la dirección IP del emisor (identificada por la capa TCP/IP). Si el puerto UDP se ha fijado a cero, deberá utilizarse el puerto desde el que se transmite (identificado por la capa TCP/IP).

E.1.4.2.2.4 Mensaje de rearranque

Deberá utilizarse la siguiente estructura para codificar las cabidas útiles de rearranque anexo E. El octeto de mensaje de transporte se pondrá a 3. Las cabidas útiles de rearranque se utilizan para indicar al par distante que el remitente ha rearrancado. La cabida útil de rearranque debe enviarse integrada en el primer mensaje destinado a la entidad distante. Cuando el receptor reciba la cabida útil de rearranque reiniciará su intervalo de números de secuencia de receptor y considerará obsoleto, e ignorará, cualquier mensaje que llegue del anterior intervalo de números de secuencia.

El receptor deberá terminar las llamadas existentes o iniciar procedimientos de recuperación dependiendo del campo "action" de la cabida útil de rearranque.

Si un rearranque no afecta a las llamadas en curso, es invisible a la capa anexo E por lo que no deberá ser señalado. Véase la figura E.12.



Campo	**Contenido del campo**	**Bits**
acción	Acción deseada por el receptor de la cabida útil de rearranque	8

Valor de acción	Explicación
0	No específica
1	Terminar llamadas
2	Iniciar procedimientos de recuperación
3..	Reservado para el futuro

Figura E.12/H.323 – Estructura del mensaje de rearranque

E.1.4.3 Mensajes de tipo estático

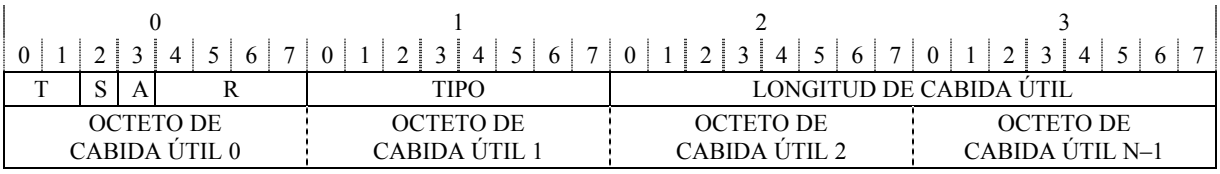
El primer bit T del OCTETO de banderas de encabezamiento de cabida útil se pondrá a 1 (uno) en todos los mensajes de tipo estático. El segundo bit T del OCTETO de banderas de encabezamiento de cabida útil se pondrá a 0 (cero) en todos los mensajes de tipo estático. El octeto siguiente indicará la cabida útil estática que está presente (véase la figura E.13):

Valor	Interpretación
0	El tren de octetos contiene un mensaje de señalización de llamada definido en la Rec. UIT-T H.225.0
1..255	Reservado para uso futuro

Figura E.13/H.323 – Cabidas útiles de tipo estático

E.1.4.3.1 Mensaje básico de tipo estático (bit S y bit A puestos a 0)

Cuando los bits S y A estén puestos a 0, se utilizará el siguiente formato de cabida útil (véase la figura E.14):

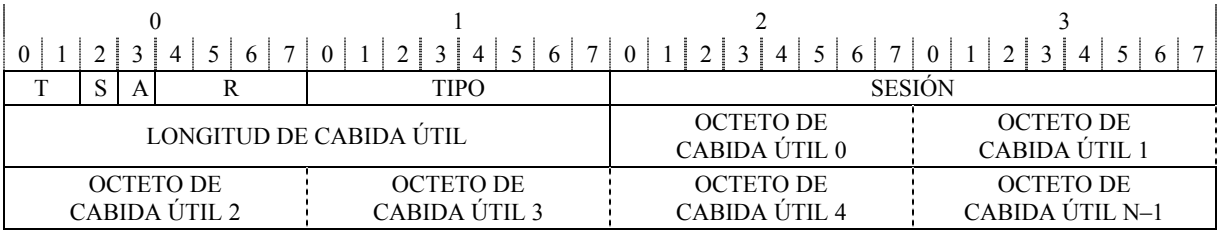


Campo	Contenido de los campos	Bits
TIPO	Entero sin signo: tipo de cabida útil definido en la figura E.13	8
LONGITUD	Entero sin signo: longitud de los datos de cabida útil (en OCTETOS)	16
DATOS	OCTETOS reales de los datos de cabida útil	8 × n

Figura E.14/H.323 – Cabida útil básica de tipo estático

E.1.4.3.2 Mensaje ampliado-1 de tipo estático (bit S puesto a 1 y bit A puesto a 0)

Cuando el bit S esté puesto a 1 y el bit A esté puesto a 0, se utilizará el siguiente formato de cabida útil. El bit S indica la presencia de un campo de SESIÓN. Véase la figura E.15.

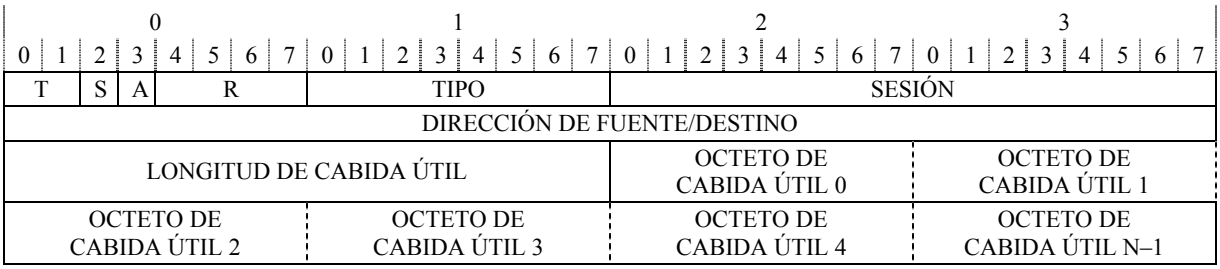


Campo	Contenido de los campos	Bits
TIPO	Entero sin signo: tipo de la cabida útil, definido en la figura E.13	8
SESIÓN	Entero sin signo: el significado del campo de sesión depende del protocolo	16
LONGITUD DE CABIDA ÚTIL	Entero sin signo: longitud (en OCTETOS) de los datos de cabida útil	16
DATOS	OCTETOS reales de los datos de cabida útil	8 × n

Figura E.15/H.323 – Formato ampliado-1 de cabida útil

E.1.4.3.3 Mensaje ampliado-2 de tipo estático (bit S y bit A fijados)

Cuando los bits S y A estén fijados, se utilizará el siguiente formato de cabida útil. El bit A indica la presencia de un campo de dirección de fuente/destino. Véase la figura E.16.



Campo	Contenido de los campos	Bits
TIPO	Entero sin signo: tipo de la cabida útil, definido en la figura E.13	8
SESIÓN	Entero sin signo: el significado del campo de sesión depende del protocolo	16
DIRECCIÓN DE FUENTE/DESTINO	Entero sin signo: el significado del campo de dirección de fuente/destino depende del protocolo	32
LONGITUD DE CABIDA ÚTIL	Entero sin signo: longitud (en OCTETOS) de los datos de cabida útil	16
DATOS	OCTETOS reales de los datos de cabida útil	$8 \times n$

Figura E.16/H.323 – Formato ampliado-2 de cabida útil

E.1.4.3.4 Mensaje ampliado-3 de tipo estático (bit S puesto a 0, bit A puesto a 1)

Cuando el bit S esté puesto a 0 y el bit A esté puesto a 1, se utilizará el siguiente formato de cabida útil. El bit A indica la presencia de un campo de dirección de fuente/destino. Véase la figura E.17.

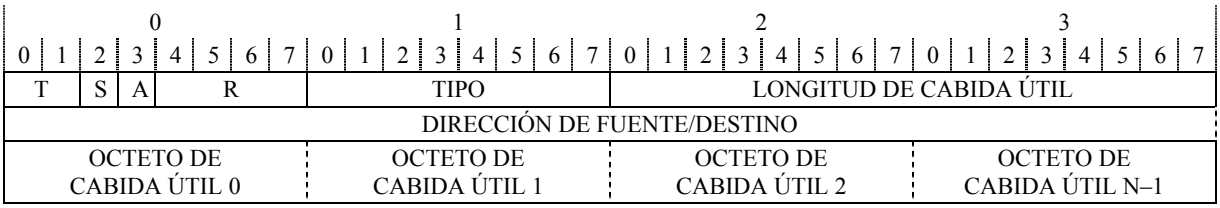


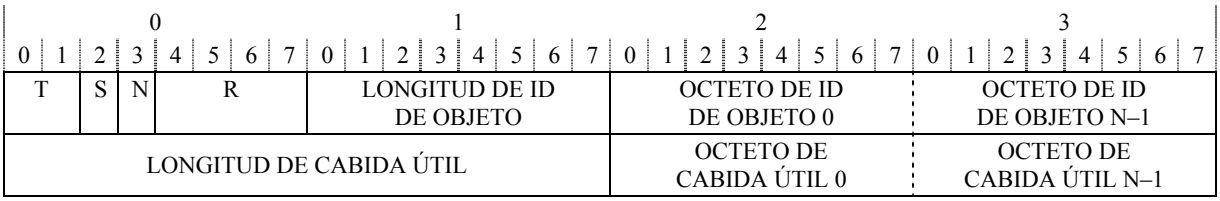
Figura E.17/H.323 – Formato ampliado-3 de cabida útil

E.1.4.4 Mensajes de tipo ID de objeto

El primer bit T del OCTETO de banderas de encabezamiento de cabida útil se pondrá a 0 (cero) en todos los mensajes de tipo ID de objeto. El segundo bit T del OCTETO de banderas de encabezamiento de cabida útil se pondrá a 1 (uno) en todos los mensajes de tipo ID de objeto. Los dos octetos siguientes indicarán la longitud del ID de objeto que sigue.

E.1.4.4.1 Mensaje básico de tipo ID de objeto (bit S y bit A puestos a 0)

Cuando los bits S y A estén puestos a 0, se utilizará el siguiente formato de cabida útil. Véase la figura E.18.

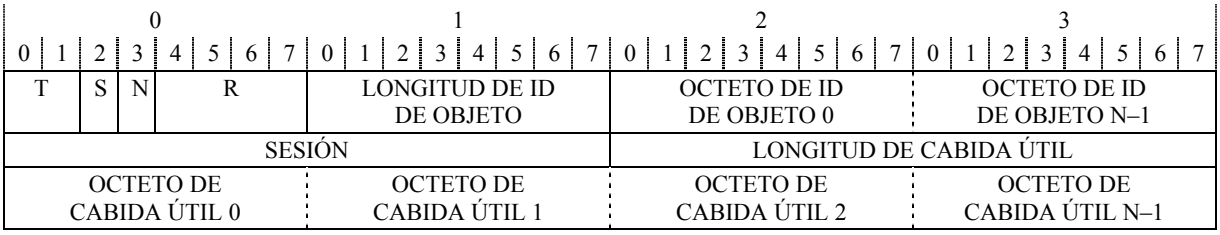


Campo	Contenido de los campos	Bits
LONGITUD DE ID DE OBJETO	Entero sin signo: longitud en OCTETOS del identificador de objeto	8
ID DE OBJETO	OCTETOS del identificador de objeto	8 × n
LONGITUD	Entero sin signo: longitud (en OCTETOS) de los datos de cabida útil	16
DATOS	OCTETOS reales de los datos de cabida útil	8 × n

Figura E.18/H.323 – Cabida útil básica de tipo ID de objeto

E.1.4.4.2 Mensaje de tipo ObjectID ampliado-1 (bit S puesto a 1 y bit A puesto a 0)

Cuando el bit S esté puesto a 1 y el bit A esté puesto a 0, se utilizará el siguiente formato de cabida útil. El bit S indica la presencia de un campo de SESIÓN, el cual es utilizado por la aplicación para asociar las cabidas útiles con una sesión específica. La definición de la sesión depende del protocolo. Véase la figura E.19.

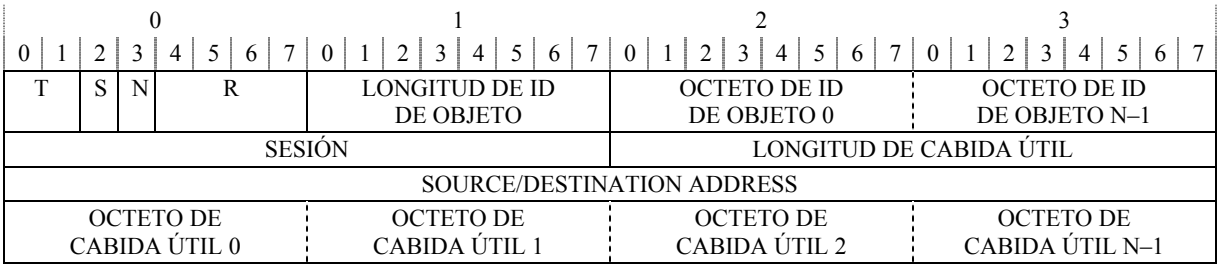


Campo	Contenido de los campos	Bits
LONGITUD DE ID DE OBJETO	Entero sin signo: longitud en OCTETOS del siguiente identificador de objeto	8
ID DE OBJETO	OCTETOS del identificador de objeto	8 × n
SESIÓN	Entero sin signo: el significado del campo de sesión depende del protocolo	16
LONGITUD	Entero sin signo: longitud (en OCTETOS) de los datos de cabida útil	16
DATOS	OCTETOS reales de los datos de cabida útil	8 × n

Figura E.19/H.323 – Formato ampliado-1 de cabida útil de tipo ID de objeto

E.1.4.4.3 Mensaje ampliado-2 de tipo ID de objeto (bit S y bit A fijados)

Cuando los bits S y A estén fijados, se utilizará el siguiente formato de cabida útil. El bit A indica la presencia de un campo de dirección de fuente/destino. Véase la figura E.20.



Campo	Contenido de los campos	Bits
LONGITUD DE ID DE OBJETO	Entero sin signo: longitud en OCTETOS del siguiente identificador de objeto	8
ID DE OBJETO	OCTETOS del identificador de objeto	8 × n
SESIÓN	Entero sin signo: el significado del campo de sesión depende del protocolo	16
LONGITUD	Entero sin signo: longitud (en OCTETOS o BYTES) de los datos de cabida útil	16
DIRECCIÓN DE FUENTE/DESTINO	Entero sin signo: el significado del campo de dirección de fuente/destino depende del protocolo	32
DATOS	OCTETOS reales de los datos de cabida útil	8 × n

Figura E.20/H.323 – Formato ampliado-2 de cabida útil de tipo ID de objeto

E.1.4.4.4 Mensaje ampliado-3 de tipo ID de objeto (bit S puesto a 0, bit A puesto a 1)

Cuando el bit S esté puesto a 0 y el bit A esté puesto a 1, se utilizará el siguiente formato de cabida útil. El bit A indica la presencia de un campo de dirección de fuente/destino. Véase la figura E.21.

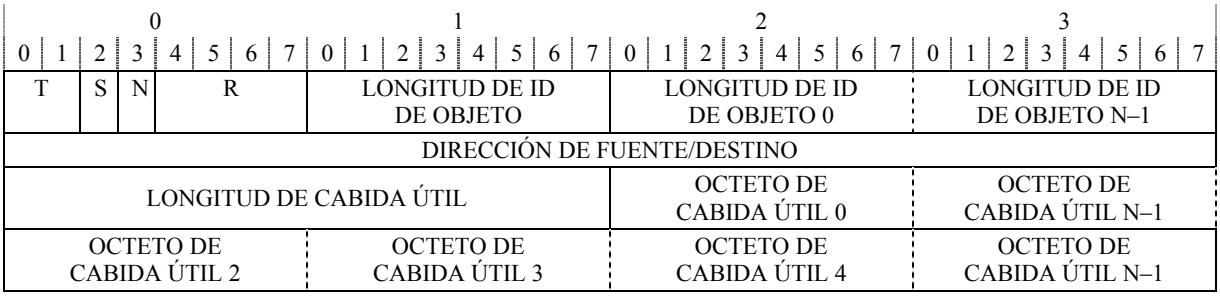


Figura E.21/H.323 – Formato ampliado-3 de cabida útil de tipo ID de objeto

E.2 Señalización de llamada H.225.0 según las especificaciones sobre anexo E

En esta cláusula se describe cómo cursar mensajes de señalización de llamada H.225.0 utilizando el transporte especificado en anexo E, con UDP. Las especificaciones anexo E se utilizan para proporcionar un transporte "UDP fiable", que permita a las implementaciones H.225.0 aplicar las especificaciones anexo E prácticamente sin cambios.

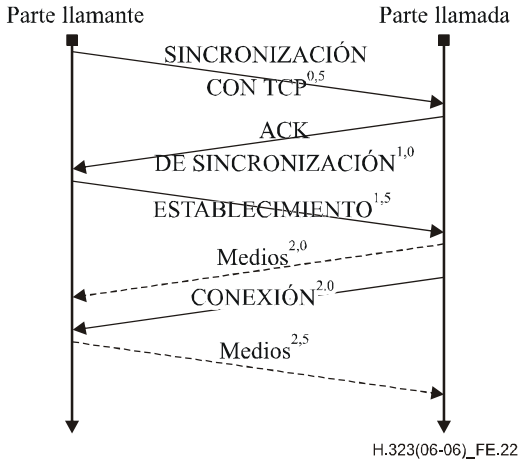
E.2.1 Fundamentos

La versión 2 de la Rec. UIT-T H.323 (1998) introduce el concepto de "conexión rápida" que permite el acceso rápido a los medios en tan sólo 2 idas y vueltas de la parte llamada a la parte llamante (incluidos mensajes TCP) y en 2,5 idas y vueltas de la parte llamante a la parte llamada.

Lo anterior puede reducirse a una ida y vuelta y 1,5 idas y vueltas respectivamente utilizando UDP para el transporte de mensajes H.323 en vez de TCP. Esto es especialmente importante cuando se hace uso del modelo encaminado por el controlador de acceso.

E.2.2 Establecimiento de comunicación H.323 utilizando las especificaciones del presente anexo

La versión 2 de la Rec. UIT-T H.323 (1998) utiliza el transporte TCP para cursar mensajes H.225.0, lo que significa que el número más pequeño de posible idas y vueltas para conseguir el acceso rápido a los medios es 2 de la parte llamada a la parte llamante, y 2,5 de la parte llamante a la parte llamada. Véase la figura E.22.



NOTA – En aras de la claridad, se han omitido algunos mensajes en el procedimiento de entrada en contacto TCP.

Figura E.22/H.323 – Flujo de información de la conexión rápida de la versión 2 de H.323 (1998)

E.2.2.1 Procedimiento basado en UDP

Para conseguir un acceso a los medios más rápidos, es posible utilizar el UDP en el transporte de señalización de llamada, lo que permite efectivamente un acceso rápido a los medios con una sola ida y una sola vuelta (véase la figura E.23):

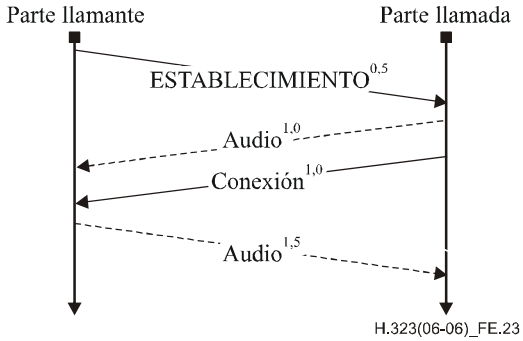


Figura E.23/H.323 – Flujo de información para el establecimiento de comunicación basado en UDP

Las capas anexo E deberán retransmitir un paquete perdido si no obtienen una respuesta después de un cierto tiempo. El procedimiento preciso de retransmisión se describe con detalle en E.1.1.8.

E.2.2.2 Procedimiento mixto TCP-UDP

Los procedimientos de establecimiento de comunicación basados en TCP y en UDP no se excluyen mutuamente. Si el establecimiento de comunicación basado en UDP y TCP se lleva a cabo en paralelo, deberá utilizarse el procedimiento de esta cláusula. En el procedimiento mixto, el originador transmite el mensaje ESTABLECIMIENTO por UDP, y simultáneamente establece una conexión TCP. Si el originador no ha recibido una respuesta al ESTABLECIMIENTO UDP cuando se establece la conexión, transmite también entonces los mensajes ESTABLECIMIENTO por la conexión TCP. Si el llamado recibe el mismo mensaje ESTABLECIMIENTO por UDP y por TCP deberá entonces responder utilizando uno de esos protocolos de transporte (normalmente el que llegó primero) pero no ambos.

Si el originador recibe una respuesta por UDP, deberá entonces liberar la conexión TCP y la comunicación continúa por UDP. Si el originador recibe una respuesta por TCP (por ejemplo, porque el par distante no soporta los procedimientos anexo E), la comunicación continúa entonces por TCP, y la comunicación basada en UDP no deberá utilizarse más para esta llamada.

Un llamado que soporta el presente anexo deberá seleccionar el protocolo de transporte con el que llega primero: mensaje de establecimiento TCP o mensaje de establecimiento UDP. Téngase en cuenta que estos mensajes pueden reordenarse en la entrega. Se notifica al llamante la selección según protocolo de transporte con el que ha llegado el mensaje subsiguiente (por ejemplo, conexión). Véase la figura E.24.

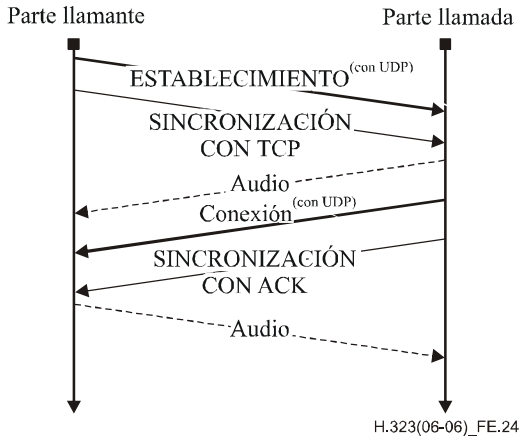


Figura E.24/H.323 – Flujo de información para el procedimiento mixto TCP y UDP

De esta manera se garantiza que si el procedimiento UDP falla, pueden aplicarse inmediatamente los procedimientos habituales basados en TCP (véase la figura E.25).

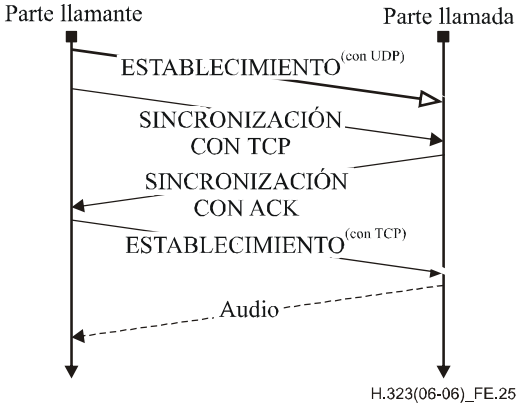


Figura E.25/H.323 – Flujo de información cuando no se soporta UDP

Esto significa que la retrocompatibilidad cuando se llama a entidades de la versión 1 (1996) o 2 (1998) de la Rec. UIT-T H.323 es transparente, ya que la aplicación H.323 v1/v2 no sabrá nada del paquete UDP.

NOTA – Es recomendable que las entidades que inician una llamada y no saben si el lado distante soporta las operaciones anexo E, utilicen el procedimiento detallado más arriba. Si la entidad llamante sabe por cualquier medio que la parte llamada distante soporta operaciones basadas en UDP, puede utilizar un establecimiento de comunicación con UDP solamente.

E.2.3 Especificaciones

E.2.3.1 Identificación de mensajes

Para H.225.0 a través de las cabidas útiles sobre anexo E se utilizará el tipo **0** (cero) de cabida útil estático.

E.2.3.2 Puerto conocido

Se utilizará el puerto UDP **2517** como puerto conocido. Las entidades pueden transmitir desde cualquier puerto aleatorio. Una entidad singular H.323 de un dispositivo físico utilizará un puerto singular UDP independiente como puerto anunciado para la recepción de mensajes. No obstante, puede utilizar un puerto distinto en cada interfaz si el dispositivo físico tuviera varias interfaces de red.

La entidad llamante deberá enviar todos los mensajes anexo E correspondientes a una llamada al puerto de destino anunciado de la entidad llamada. La entidad llamada deberá enviar todos los mensajes anexo E relativos a dicha llamada a la dirección IP y puerto de los que se recibiera el mensaje anexo E inicial correspondiente a la llamada. La entidad llamada deberá enviar todos los mensajes anexo E utilizando el mismo puerto por el que recibiera la PDU H.225.0 inicial del llamador.

La entidad llamante puede transmitir mensajes desde cualquier puerto al azar, pero deberá utilizar el mismo puerto durante toda la llamada.

E.2.3.3 Modelo de señalización

H.225.0 por medio de las especificaciones sobre anexo E utilizará el **modelo en serie** descrito en E.1.2.2.

E.2.3.4 Temporizadores

H.225.0 a través de las especificaciones sobre anexo E utilizará temporizadores y valores por defecto. El temporizador **T-IMA1** se restablecerá cuando se reciba un mensaje cualquiera de señalización de llamada (pero no cuando se reciban paquetes RTP).

E.2.3.5 Campo de sesión

El campo de sesión estará presente en todas las cabidas útiles. El valor de sesión contendrá el CRV de los mensajes de señalización de llamada H.225.0. De manera específica, deberá incluirse la bandera de referencia de llamada como bit más significativo del valor de referencia de llamada (CRV). Ello restringe el CRV real a la gama de 0 a 32 767 inclusive.

E.2.3.6 Campo de dirección de fuente/destino

La utilización del campo de fuente/destino es facultativa, pero deberá estar presente en todos los mensajes que se originen en una MCU o vayan destinados a ella, o cuando un controlador de acceso actúa como MC.

E.2.3.7 MTU

Los mensajes de señalización que requieren el envío de grandes cantidades de datos (como los de autenticación y autorización de certificados) deberán utilizar TCP para el establecimiento de comunicación ya que utilizarlos por el presente anexo podría causar fragmentación debido a que los mensajes son más largos que la MTU del trayecto.

E.2.3.8 H.245

Se transmitirá H.245 utilizando los procedimientos de tunelización H.245 de la versión 2 de la Rec. UIT-T H.323 (1998).

E.2.3.9 Política de números de secuencia del receptor para H.225.0 sobre anexo E

Cuando una entidad reciba un mensaje H.225.0 sobre anexo E, deberá verificar la dirección de anfitrión, el puerto de origen y el número de secuencia para detectar si se trata de un mensaje duplicado. La entidad transmisora utiliza el modelo serie para el mismo identificador de sesión y asigna números de secuencia para cada dirección de anfitrión y puerto de origen. Como no es posible que los mensajes para una única llamada H.323 estén desordenados, la capa anexo E no intentará ordenar los mensajes por número de secuencia. Aunque haya saltos en el números de secuencia, cosa que es posible, la entidades no deberá identificarlos como pérdida de paquetes.

Anexo F

Tipos de punto extremo simples

F.1 Introducción

Los tipos de punto extremo simple, es decir, dispositivos fabricados para un solo uso, pueden abarcar una parte significativa del conjunto general de sistemas de extremo con capacidades H.323. En contraste con los dispositivos H.323 totalmente equipados (cuyas implementaciones se basan muy a menudo en un PC), los denominados tipos de punto extremo simple (SET, *simple endpoint types*) pueden implementarse en aparatos autónomos poco costosos, de los que el ejemplo más notable es el simple teléfono.

NOTA – Ejemplos de configuraciones de aplicación de tales sistemas son los siguientes:

1) un ordenador de bolsillo con capacidades de comunicaciones de audio (voz, transferencia de ficheros, fax, etc.);
2) un teléfono con un conector RJ-45;
3) teléfonos con texto (que utilizan la Rec. UIT-T T.140);
4) un teléfono celular IP;
5) un sistema móvil con comunicaciones integradas de voz y datos (UMTS, IMT-2000).

Todos estos sistemas tienen en común el hecho de que soportan un conjunto de funcionalidades relativamente específico: voz y/o prestaciones rudimentarias de comunicaciones de datos (es decir, no T.120). Conviene señalar que los objetivos de los sistemas no exigen funcionalidades más amplias: un aparato telefónico sin una (compleja) pantalla no tiene que ofrecer la funcionalidad de vídeo, ni capacidades de comunicación de datos en conferencia.

Todos estos sistemas tienen una cantidad limitada de recursos disponibles (por ejemplo, capacidad de procesamiento, anchura de banda para la comunicación, memoria).

En el presente anexo se describe el alcance de los dispositivos SET en general y se definen los detalles de procedimiento y de protocolo de los dispositivos simples de audio (SET de audio). En este anexo se define, en particular, la línea funcional básica de todos los tipos de punto extremo simple; por ello, cualesquiera otros SET se habrán de definir refiriéndose al presente anexo y especificando tan solo adiciones a los procedimientos y convenios expuestos en el mismo.

En este anexo se define un subconjunto de la funcionalidad H.323, identificándose explícitamente cualquier desviación con respecto a la presente Recomendación. Cualesquiera procedimientos no descritos explícitamente en este anexo quedan cubiertos por el texto principal de esta Recomendación.

El desarrollo de dispositivos SET puede tener repercusiones en otros dispositivos H.323: en particular, los MC (y las MCU) y las pasarelas tienen que conocer su potencial soporte mínimo de la funcionalidad H.323 (1998), a fin de proporcionar a los dispositivos SET audio un acceso continuo a servicios mejorados de la H.323, tales como las conferencias multipunto y los servicios suplementarios. Alternativamente, pueden proporcionarse dispositivos externos que actúen cubriendo el vacío existente entre las diferentes gamas funcionales de los dispositivos SET y los puntos extremos H.323 (1998) que disponen de todas las capacidades. Las cuestiones de interfuncionamiento se tratan con más detalle en F.9.

F.2 Convenios de especificación

En el presente anexo se especifican únicamente aquellos servicios, procedimientos, mensajes de protocolo, etc., que son obligatorios para la implementación de un dispositivo SET, que es un subconjunto de las funcionalidades obligatorias de un sistema H.323 (1998). Ello implica que los dispositivos SET no asumirán ninguna funcionalidad de otro dispositivo SET que no esté especificada como obligatoria en el presente anexo.

Además de los componentes obligatorios, en varias cláusulas de este anexo se especifican servicios, procedimientos, mensajes de protocolo, etc., obligatorios en ciertas condiciones, basándose en el concepto de bloques funcionales, que son facultativos globalmente. Sin embargo, si se decide que un dispositivo SET implemente un bloque funcional particular, dicho dispositivo debe soportar todos los componentes definidos como obligatorios para dicho bloque; pueden soportarse componentes facultativos.

Las demás características definidas en esta Recomendación son, por definición, facultativas, y su implementación en un dispositivo SET depende enteramente del fabricante.

F.3 Alcance

En el presente anexo se especifican ciertas reglas sobre cómo utilizar esta Recomendación para hacer posible la implementación sencilla de tipos de punto extremo simple. Está previsto que el UIT-T normalice la siguiente lista (no exhaustiva) de tipos de punto extremo simple:

1) **teléfono simple (dispositivo simple de audio)** – definido en este anexo;
2) **teléfono simple con capacidades de seguridad** – queda en estudio;
3) **terminal de conversación mediante texto** – queda en estudio;
4) **dispositivo fax** – queda en estudio.

En este anexo se define el teléfono simple. El teléfono simple de seguridad, el terminal de texto y el terminal de fax simple son tipos de punto extremo simple que quedan en estudio. Los perfiles de los tipos de punto extremo simple pueden dividirse en las siguientes categorías:

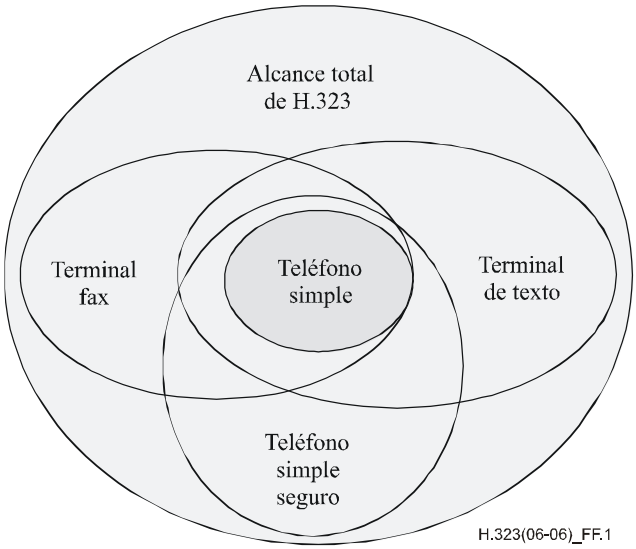


Figura F.1/H.323 – Diagrama de Venn en el que se muestran las gamas funcionales de los diferentes dispositivos SET

La figura F.1 representa una imagen esquemática de los diferentes tipos de punto extremo simple que están siendo definidos en el contexto de los 'perfiles' H.323, organizada en lo que se denomina un diagrama de Venn. En dicho diagrama se ilustra la relación entre los SET. La elipse más amplia muestra el contexto de un sistema que cumple totalmente las especificaciones H.323. En la figura se indica, a título de ejemplo, el teléfono simple. Se trata a todas luces de un subconjunto del sistema totalmente conforme con la H.323, por lo que queda completamente dentro de su alcance. El teléfono simple de seguridad, que contiene además capacidades de seguridad, comprende las capacidades del teléfono simple (por ejemplo, los mismos códecs de audio, el mismo establecimiento de comunicación, etc.). El interfuncionamiento entre una implementación SET de teléfono simple y un teléfono simple de seguridad estará, por consiguiente, garantizado.

Los dispositivos SET están definidos de forma que pueden interfuncionar sin discontinuidades entre sí y con los dispositivos H.323 (1998) que soportan el procedimiento de conexión rápida, así como con todos los puntos extremos H.323 que tienen en cuenta los SET.

NOTA – Aunque los dispositivos SET están definidos pensando en dispositivos sencillos, es asimismo posible construir pasarelas basadas en la especificación SET respectiva. No se requieren definiciones adicionales para otros tipos de dispositivos.

F.4 Referencias normativas

Se aplican todas las referencias normativas de la parte principal de esta Recomendación y de la Rec. UIT-T H.225.0 (2003).

F.5 Abreviaturas

En este anexo se utilizan las siguientes siglas.

SET audio de seguridad	Tipo de punto extremo de audio simple de seguridad (*secure simple audio endpoint type*)
SET audio	Tipo de punto extremo de audio simple (*simple audio endpoint type*)

SET fax	Tipo de punto extremo de facsímil simple (*simple facsimile endpoint type*)
SET texto	Tipo de punto extremo de telefonía de texto simple (*simple text telephony endpoint type*)
SET	Tipo de punto extremo simple (*simple endpoint type*)

F.6 Tipo de punto extremo (audio) simple – Aspectos generales de la funcionalidad de los sistemas

Las características siguientes son las correspondientes a los tipos de punto extremo simple (dispositivos SET audio):

Capacidades de medios

- Capacidad de voz
  - obligatoria: G.711 (ley A y ley μ);
  - opciones recomendadas: G.723.1, G.729, GSM;
  - opciones recomendadas: codificación de redundancia de audio con cualquier combinación de los códecs anteriores.
- Los dispositivos SET audio soportarán únicamente el funcionamiento audio simétrico.
- Sin capacidad de datos.
- Capacidad DTMF obligatoria; transmisión obligatoria de mensajes de información H.225.0; la transmisión como parte útil de RTP queda en estudio.
- Sin capacidad de vídeo.
- Sin capacidad T.120.
- Distribución de medios: soporte de unidifusión obligatoria.

Las capacidades de medios obligatorias y facultativas se definirán separadamente para otros tipos de punto extremo simple.

Capacidades de control

Las siguientes capacidades mínimas de control serán aplicables por igual a todos los tipos de punto extremo simple.

- Secuencia de conexión rápida de la Rec. UIT-T H.323 (1998) obligatoria.

NOTA – Los dispositivos SET audio son capaces por defecto de participar en conferencias multipunto, aunque obviamente están limitados a las comunicaciones audio.

La mayoría de las capacidades de control restantes son facultativas, en particular:

- La conexión rápida basada en UDP según el anexo E/H.323, facultativa.
- Los servicios suplementarios (únicamente basados en H.450.x), facultativos.
- El soporte de mensajes y procedimientos H.245, facultativo.
- El soporte de más de una llamada/conferencia al mismo tiempo, facultativo.

Algunas capacidades de control no están permitidas en el caso de los dispositivos SET audio.

- Funcionalidad MC prohibida.

F.7 Procedimientos para tipos de punto extremo simple

En esta cláusula se especifica, para todos los protocolos requeridos por esta Recomendación, el nivel detallado de soporte de los dispositivos SET en general y los requisitos para dispositivos SET audio:

- señalización de registro, admisión y situación (RAS) (H.225.0), véase F.7.1;
- señalización de llamada (H.225.0), véase F.7.2;
- señalización de control de sistemas multimedia (H.245), véase F.7.3;
- paquetización y transporte de medios (RTP, H.225.0), véase F.7.4;
- servicios suplementarios (H.450.x), véanse F.7.5 y F.7.6;
- funcionamiento de conferencia multipunto, véase F.7.7;
- conferencias de bajo grado de acoplamiento (H.332), véase F.7.8;
- bases de información de gestión, véase F.7.9.

En F.8 se analizan los servicios de seguridad especificados en la Rec. UIT-T H.235.0 para crear dispositivos SET audio de seguridad.

F.7.1 Señalización RAS (RAS H.225.0)

Los dispositivos SET deberán ser conformes a los procedimientos RAS definidos en las Recs. UIT-T H.323 (1998) y H.225.0 (1998), aplicándose las siguientes modificaciones.

Un dispositivo SET deberá utilizar los procedimientos de petición de admisiones (ARQ, *admissions request*) tal como se especifica en la Rec. UIT-T H.225.0 (1998,) y deberá poder determinar si una petición de llamada entrante se recibe de su controlador de acceso. Un controlador de acceso que tenga en cuenta los SET deberá soportar los procedimientos de ARQ concedidos previamente y deberá conceder por adelantado la realización y recepción de llamadas con encaminamiento de las mismas a través del controlador de acceso de los dispositivos SET (lo que se debe indicar en el componente preGrantedARQ). Si un controlador de acceso con el que se establece contacto no soporta ARQ concedido previamente o no soporta la concesión por adelantado antes mencionada, el dispositivo SET deberá registrarse en otro controlador de acceso.

Los dispositivos SET deberán soportar como mínimo los siguientes mensajes RAS: transmisión de GRQ, RRQ, URQ, UCF y XRS y recepción de GCF, GRJ, RCF, RRJ, URQ, UCF, URJ y XRS. Los dispositivos SET pueden soportar mensajes RAS adicionales.

Un terminal SET deberá incluir el componente "set" del tipo de punto extremo H.225.0 cuando comunique con un controlador de acceso y fije los bits como se indica a continuación.

Bit 0: = 1 si el dispositivo tiene la funcionalidad SET audio.

Bit 1: = 0 si el dispositivo no tiene en cuenta la funcionalidad de conferencia.

Bit 1: = 1 si el dispositivo tiene en cuenta la funcionalidad de conferencia.

La utilización de los otros bits se definirá mediante especificaciones de SET adicionales.

F.7.2 Señalización de la llamada (control de la llamada H.225.0)

Los dispositivos SET deberán atenerse a los procedimientos de control de la llamada definidos en las Recs. UIT-T H.323 (1998) y H.225.0 (1998). Los dispositivos SET no cerrarán el canal de señalización de la llamada después del establecimiento de la comunicación.

Los dispositivos SET deberán implementar los procedimientos de conexión rápida especificados en la Rec. UIT-T H.323 (1998). Cuando origine una llamada, el dispositivo SET utilizará la conexión rápida.

Los dispositivos SET deberán soportar los mensajes de información H.225.0 en el canal de señalización de la llamada. Tales mensajes deberán utilizarse para, pero sin limitarse al transporte de entrada de usuario en el elemento de información teclado.

Los dispositivos SET deberán utilizar los mensajes de consulta de estado y estado de la Rec. UIT-T H.225.0 para estimar tiempos de ida y vuelta con su par.

Los dispositivos SET pueden implementar el establecimiento de comunicaciones basado en UDP, tal como se describe en el anexo E. Si se implementa el establecimiento de comunicación basado en UDP, el dispositivo SET debe, en primer lugar, tratar de llamar a otro punto extremo en aplicación del procedimiento de establecimiento de comunicación basado en UDP.

La implementación de servicios suplementarios de H.450.x es facultativa para los dispositivos SET. Éstos deberán poder ignorar sin riesgo alguno los mensajes de Facilidad H.225.0 que no comprendan.

Los dispositivos SET deberán incluir el componente "set" del tipo de punto extremo H.225.0 cuando intercambien las PDU de señalización de llamada con su par. Los bits de los componentes "set" se fijarán como se define en F.7.1.

F.7.3 Señalización de control de sistemas multimedia (H.245)

F.7.3.1 Canal de control H.245

Se utilizará el procedimiento de conexión rápida para el establecimiento de la conexión. Se utilizará la transmisión repetida del elemento fastStart en los mensajes de señalización de llamada H.225.0 para reconfigurar o reencaminar trenes de medios.

Los dispositivos SET no abrirán una conexión H.245 independiente:

a) Limitarán la señalización H.245 a la estructura de **apertura de canal lógico** en la secuencia de conexión rápida junto con la determinación implícita principal-subordinado.

b) Si se necesita señalización adicional H.245, se realizará la tunelización definida en la Rec. UIT-T H.225.0 (1998).

Los dispositivos SET deberán utilizar la sintaxis de la Rec. UIT-T H.245 (1998) o versiones posteriores.

No se definen procedimientos específicos para mensajes H.245. Si los dispositivos SET implementan funcionalidades H.245, deberán seguir los procedimientos definidos en las Recomendaciones UIT-T H.323, H.225.0 y H.245.

F.7.3.2 Determinación principal-subordinado

Los dispositivos SET deberán asumir implícitamente el cometido de subordinado en cualquier relación de comunicación sin un canal de control H.245.

Si se establece un túnel H.245, siguiendo las reglas de 6.2.8.4/H.323 (1998), el dispositivo SET indicará un valor de 40 para el **terminalType**. Así se garantiza que en el caso de que un dispositivo SET se conecte con un terminal totalmente equipado de H.323 (1998), este último ganará la determinación principal-subordinado.

F.7.3.3 Intercambio de capacidad de terminal

Aunque la gama de funcionalidades que soportan los dispositivos SET es, por definición, restringida, no puede evitarse un procedimiento de intercambio de capacidad que permita un mínimo de diversidad en los dispositivos. No obstante, la gama de posibles capacidades que pueden ser indicadas por un punto extremo SET se limita a lo definido a continuación, y los procedimientos de intercambio de capacidad deberán seguir las reglas establecidas en esta subcláusula.

El procedimiento de intercambio de capacidad para tipos de medios y modos de transmisión se llevará a cabo siguiendo las reglas del procedimiento de conexión rápida, utilizando múltiples estructuras de apertura de canal lógico como parte de las posibilidades ofrecidas por la parte llamante, de las que la parte llamada elige un subconjunto para enviar y recibir.

En la siguiente subcláusula se enumeran las capacidades que es necesario que comprenda la parte receptora (llamada) y que puede transmitir la parte emisora (llamante) para dispositivos SET audio.

F.7.3.3.1 Capacidad de audio

- G.711 (ley μ, ley A, 56 kbit/s, 64 kbit/s)

  Se soportarán las alternativas siguientes:

```
AudioCapability.g711Alaw64k          ≥ 20     number of frames
AudioCapability.g711Alaw56k          ≥ 20     number of frames
AudioCapability.g711Ulaw64k          ≥ 20     number of frames
AudioCapability.g711Ulaw56k          ≥ 20     number of frames
```

- G.723.1 (supresión o no de silencio, velocidad baja y alta)

  Un SET que soporte G.723.1 debe soportar como mínimo:

```
AudioCapability.g7231
  maxAl-sduAudioFrames               ≥ 1      number of frames
  silenceSuppression                          True/False as appropriate
```

- G.729 (completa o anexo A)

  Un SET que soporte G.729 debe soportar como mínimo:

```
AudioCapability.g729                 ≥ 1      number of frames
AudioCapability.g729AnnexA           ≥ 1      number of frames
```

- GSM (velocidad máxima, velocidad máxima mejorada, velocidad media)

  Un SET que soporte GSM debe soportar como mínimo:

```
AudioCapability.gsmFullRate          GSMAudioCapability,
AudioCapability.gsmHalfRate          GSMAudioCapability,
AudioCapability.gsmEnhancedFullRate GSMAudioCapability
```

  siendo GSMAudioCapability definido según convenga para cada una de estas velocidades:

```
GSMAudioCapability.audioUnitSize     ≥ 1      number of frames
GSMAudioCapability.comfortNoise              True/False as appropriate
GSMAudioCapability.scrambled                 True/False as appropriate
```

F.7.3.3.2 Capacidad de vídeo

Los dispositivos SET audio no soportan la capacidad de vídeo.

F.7.3.3.3 Capacidad de datos

Los dispositivos SET audio no soportan la capacidad de datos.

F.7.3.3.4 Capacidad de conferencia

Se supone que los dispositivos SET se conectan a través de intermediarios en conferencias centralizadas con distribución de datos centralizada (véase F.7.7).

F.7.3.3.5 Capacidad de entrada de usuario

Los dispositivos SET deberán soportar la transmisión de multifrecuencia bitono (DTMF), como elementos de información teclado en la conexión de señalización de llamada H.225.0 (por ejemplo, utilizando mensajes información).

F.7.3.3.6 Capacidad de seguridad

La seguridad para los dispositivos SET, es decir, la definición de un dispositivo SET seguro queda en estudio. Véase también F.8.

F.7.3.3.7 maxPendingReplacementFor

Los dispositivos SET audio deberán soportar este parámetro. Se asumirá implícitamente un valor igual a "1":

```
maxPendingReplacementFor = 1
```

Por consiguiente, el parámetro **maxPendingReplacementFor** no se indicará de manera explícita.

F.7.3.3.8 Capacidad no normalizada

Se evitará en la medida de lo posible la utilización de capacidades no normalizadas, tanto en el nivel superior de la estructura de capacidades como dentro de las categorías de capacidades mencionadas más arriba.

F.7.3.3.9 Normas adicionales para la utilización de capacidades

Para dispositivos SET audio, las capacidades audio se indicarán únicamente en aplicación del procedimiento de conexión rápida y en el intercambio repetido de estructuras de **OpenLogicalChannel** utilizando la conexión rápida.

Las capacidades de vídeo, de datos, de conferencia, de seguridad y de criptación h233 (h233encryption) no serán utilizadas.

Se supondrán los siguientes valores de las entradas del cuadro MultiplexCapability de un dispositivo SET audio:

```
maximumAudioDelayJitter                  ≥ 250 ms
receiveMultipointCapability,
transmitMultipointCapability, and
receiveAndTransmitMultipointCapability
    multicastCapability                  TRUE/FALSE as appropriate,
                                         default FALSE[1]
    multiUnicastConference               TRUE/FALSE as appropriate,
                                         default FALSE[1]
    mediaDistributionCapability
        centralizedControl               TRUE
        distributedControl               FALSE
        centralizedAudio                 TRUE
        distributedAudio                 TRUE/FALSE as appropriate,
                                         default FALSE[1]
        centralizedVideo                 FALSE
        distributedVideo                 FALSE
        centralizedData                  ABSENT
        distributedData                  ABSENT
mcCapability
    centralizedConferenceMC              FALSE
    decentralizedConferenceMC            FALSE
```

[1] Los dispositivos SET audio para conferencias pueden soportar multidifusión, multiunidifusión y audio distribuido.

```
rtcpVideoControlCapability                ABSENT
mediaPacketizationCapability              ABSENT
...,
transportCapability                       ABSENT
redundancyEncodingCapability              Audio redundancy encoding only
                                          (if any)
logicalChannelSwitchingCapability         FALSE
t120DynamicPortCapability                 FALSE
```

Las capacidades indicadas por el lado distante que no se comprendan serán ignoradas.

F.7.3.4 Mensajes de señalización de canal lógico

La apertura de canales lógicos se atendrá a las especificaciones de conexión rápida de la Rec. UIT-T H.323 (1998).

Además, los dispositivos SET soportarán la reconfiguración de trenes de medios en todo momento durante una llamada. Las estructuras de apertura de canal lógico se tunelizarán en mensajes de señalización de llamada H.225.0, siguiendo los procedimientos definidos en las Recs. UIT-T H.225.0 (1998) y H.323 (1998), reutilizando el elemento comienzo rápido del mensaje de señalización de la llamada H.225.0. Fuera del procedimiento de conexión rápida se utilizarán estructuras de apertura de canal lógico para alterar los parámetros de trenes de medios, con el fin de proporcionar una base para servicios suplementarios. Cuando se reciban, las estructuras de apertura de canal lógico se interpretarán de la forma siguiente:

- Si el número de canal lógico coincide con un canal lógico abierto en esos momentos, el canal correspondiente será reconfigurado conforme a los principios del procedimiento de conexión rápida si el componente **tipo de datos** no es "nulo" ("null"). Si el componente **tipo de datos** es "nulo", lo que indica un "canal nulo" ("NullChannel"), el canal lógico correspondiente se considerará cerrado y cesará la transmisión de medios por el mismo.
- Si el número de canal lógico no coincide con un número de un canal lógico abierto en esos momentos, se abrirá un nuevo canal lógico siguiendo los principios del procedimiento de conexión rápida.

A continuación se describen las restricciones impuestas a la petición de apertura de canal lógico:

```
OpenLogicalChannel
   forwardLogicalChannelNumber          LogicalChannelNumber
   forwardLogicalChannelParameters
      portNumber                        ABSENT
      dataType                          a valid audio data type
                                        (see F.7.3.3.1)
      multiplexParameters               CHOICE:h2250LogicalChannelParameters
      forwardLogicalChannelDependency   ABSENT,
      replacementFor                    used if another Logical Channel is
                                        to be replaced

   reverseLogicalChannelParameters
      dataType                          a valid audio data type
                                        (see F.7.3.3.1)
      multiplexParameters               CHOICE:h2250LogicalChannelParameters
      reverseLogicalChannelDependency   LogicalChannelNumber OPTIONAL,
      replacementFor                    used if another Logical Channel is
                                        to be replaced
   separateStack                        ABSENT
   encryptionSync                       ABSENT for Audio SET devices; FFS.
```

La estructura **H2250LogicalChannelParameters** tiene las restricciones siguientes:

```
H2250LogicalChannelParameters
   nonStandard                    should be ABSENT
```

```
sessionID                          INTEGER(0..255)
associatedSessionID                ABSENT
mediaChannel                       TransportAddress - should be a unicast
                                   address
mediaGuaranteedDelivery            ABSENT
mediaControlChannel                PRESENT - reverse RTCP channel
mediaControlGuaranteedDelivery     FALSE
silenceSuppression                 as appropriate
destination                        typically ABSENT
dynamicRTPPayloadType              as appropriate,
mediaPacketization                 as appropriate; may only specify the
                                   payload format used
    rtpPayloadType
    payloadDescriptor              should refer to an rfc-number
    payloadType                    (dynamic) payload type value to be used

transportCapability
    nonStandard                    should be ABSENT
    qOSCapabilities                should be ABSENT (may only contain RSVP
                                   parameters)
    mediaChannelCapabilities       should be ABSENT (may indicate "ip-udp")

redundancyEncoding                 optional; only audio redundancy is
                                   allowed
source                             typically ABSENT
```

F.7.4 Intercambio de medios

Para el intercambio de medios, los dispositivos SET deberán seguir los procedimientos H.323 y H.225.0 utilizando RTP/UDP/IP para transportar los trenes de medios. Se utilizarán los formatos de paquetización de medios apropiados.

F.7.5 Servicios suplementarios (H.450.x)

El soporte de servicios suplementarios de conformidad con las Recomendaciones de la serie H.450.x es facultativo.

NOTA – Si el dispositivo SET no proporciona la funcionalidad H.450.x, deberá implementar la funcionalidad de rechazo de mensaje (APDU Interpretación) de H.450.1 para que su par pueda determinar rápidamente la no disponibilidad de servicios suplementarios por parte del dispositivo SET. Si el rechazo de mensaje H.450.1 no se ha implementado, el dispositivo par dependerá de una temporización.

Queda en estudio la línea básica del soporte de los servicios suplementarios por los dispositivos SET.

F.7.6 Pausa y reencaminamiento iniciados por terceras partes

El soporte de la pausa y el reencaminamiento iniciados por terceras partes es similar a los procedimientos descritos en 8.4.6/H.323 (1998), con las modificaciones que se describen a continuación.

F.7.6.1 Parte iniciadora

Para reencaminar una llamada conectada a un dispositivo SET, su par, normalmente un controlador de acceso, transmitirá una especificación NullChannel en el elemento arranque rápido de un mensaje del canal de señalización de llamada.

A continuación, la entidad iniciadora transmitirá nuevamente (para el nuevo par) las estructuras apropiadas **OpenLogicalChannel**, similares a la negociación de capacidad y al establecimiento del tren de medios en el procedimiento de conexión rápida, e incluirá las nuevas direcciones de transporte para redireccionar el tren de medios originado por el dispositivo SET. Las estructuras **OpenLogicalChannel** se transportan en un mensaje de señalización de llamada H.225.0.

La estructura **OpenLogicalChannel** deberá ofrecer las mismas codificaciones de audio que se ofrecieron en la llamada inicial.

F.7.6.2 Parte receptora (dispositivo SET)

Al recibir una especificación NullChannel en un elemento fastStart, el dispositivo SET dejará inmediatamente de transmitir los trenes de medios y se preparará para tratar interrupciones en los trenes de medios recibidos. El dispositivo SET esperará un intercambio repetido de capacidad y direcciones de transporte según los principios del procedimiento de conexión rápida.

Al recibir una estructura **OpenLogicalChannel** transportada en un mensaje de señalización de llamada H.225.0, el dispositivo SET seleccionará una codificación de medios aceptable entre las ofrecidas por la entidad iniciadora, siguiendo las reglas del procedimiento de conexión rápida. A continuación, el dispositivo SET arrancará la transmisión de sus trenes de medios a las direcciones de transporte recién indicadas en las estructuras **OpenLogicalChannel**.

F.7.7 Funcionamiento en modo conferencia

Los dispositivos SET pueden participar en conferencias multipunto de dos formas diferentes:

- siendo introducidos en la conferencia por medio de un dispositivo externo especializado, tal como un MC con reconocimiento del SET combinado con un MP adecuado o una entidad intermediaria específica del SET, tal como se describe en F.7.7.1 como modo de funcionamiento por defecto de los dispositivos SET; o
- implementando los procedimientos necesarios de los protocolos H.225.0 y H.245, tal como se describe en esta cláusula. Este modo de funcionamiento se define en F.7.7.2.

F.7.7.1 Dispositivos SET que no tienen en cuenta la funcionalidad de conferencia

El modo de funcionamiento por defecto de los dispositivos SET no requiere ninguna capacidad para la funcionalidad de conferencia en el propio terminal. Se supone que, en vez de ello, una entidad externa intermedia actúa entre lo que sería un dispositivo H.323 totalmente equipado y un dispositivo SET. Esta entidad lógica puede ser un dispositivo representativo autónomo o puede ser parte de un MC (o una MCU), una pasarela o un controlador de acceso.

NOTA – La funcionalidad de una entidad lógica intermedia puede ser la siguiente:

- ocultar la existencia de instrucciones H.245 relacionadas con la conferencia y responder apropiadamente en dirección del dispositivo H.323 totalmente equipado;
- adaptar la capacidad y la señalización de canal lógico H.245 incluyendo instrucciones en modo multipunto;
- combinar varios trenes de audio entrantes para proporcionar un solo tren al dispositivo SET;
- traducir las direcciones de transporte para el tren de audio;
- transcodificar los trenes de audio; y
- ofrecer acceso a las funciones de control de la conferencia a través de medios de entrada sencillos (como la señalización DTMF) al dispositivo SET.

F.7.7.2 Dispositivos SET que tienen en cuenta la funcionalidad de conferencia

La especificación de los dispositivos SET que tienen en cuenta la funcionalidad de conferencia queda en estudio.

No obstante, los dispositivos SET pueden seguir los procedimientos completos de funcionamiento en modo conferencia definidos en las Recomendaciones de la serie H.323.

F.7.8 Soporte de conferencias de bajo grado de acoplamiento (Rec. UIT-T H.332)

El soporte de conferencias de bajo grado de acoplamiento de conformidad con la Rec. UIT-T H.323 es facultativo:

- La participación como miembro del panel es facultativa; se facilita si se soportan el funcionamiento en modo conferencia y la distribución de medios a través de la multidifusión, o si una combinación apropiada de MC/MP oculta todas las instrucciones de conferencia al terminal SET y presenta un solo tren de audio.
- La participación como miembro de la audiencia es facultativa; es posible si el dispositivo SET soporta la recepción de información multidifusión y puede recibir e interpretar anuncios de sesión H.332.

F.7.9 Bases de datos de información de gestión (MIB, *management information base*)

La implementación de bases de datos de información de gestión (MIB) es facultativa para los dispositivos SET. Si se incluyen las MIB en la configuración, deberán implementarse las siguientes MIB relacionadas con H.323:

- Señalización de llamada.
- Entidad del terminal.
- RAS.
- Protocolo en tiempo real (RTP).

Los detalles quedan en estudio.

F.8 Extensiones de seguridad

Los dispositivos SET sencillos no soportan los servicios de seguridad H.235.0. Los dispositivos SET seguros, en cambio, son una extensión simple de los dispositivos SET que cubre la funcionalidad de seguridad utilizando un subconjunto de mecanismos especificados en la Rec. UIT-T H.235.0.

Los detalles de los dispositivos SET seguros están cubiertos por el anexo J.

F.9 Consideraciones relativas al interfuncionamiento

El presente anexo especifica que el dispositivo SET es un subconjunto bien definido de la funcionalidad completa H.323.

Los dispositivos SET deben utilizarse siempre en combinación con controladores de acceso que tengan en cuenta a dichos dispositivos. Tales controladores de acceso efectuarán ARQ concedido previamente y emplearán el modelo de llamada encaminada por el controlador de acceso para garantizar el interfuncionamiento pleno con otros dispositivos H.323 (1996) y H.323 (1998).

Además, el reconocimiento de los SET puede estar incorporado en los MC (o las MCU) o en las pasarelas para conseguir un interfuncionamiento continuo.

En el cuadro F.1 se presenta una visión general del interfuncionamiento alcanzado entre dispositivos SET y otros puntos extremos H.323.

Cuadro F.1/H.323 – Interfuncionamiento de dispositivos SET con otros dispositivos H.323

	H.323 (1996)	H.323 (1998)	H.323 (1998) con conexión rápida	Dispositivo SET
H.323 (1996)	√	√	√	√(GK)
H.323 (1998)	√	√	√	√(GK)
H.323 (1998) con conexión rápida	√	√	√	√a)
Dispositivo SET	√(GK)	√(GK)	√a)	√

(GK) Indica que se necesita un controlador de acceso que tenga en cuenta el SET para el interfuncionamiento.

a) El redireccionamiento facultativo de canales de medios requiere la ejecución repetida de la conexión rápida en ambos puntos extremos.

F.10 Notas sobre la implementación (informativo)

En esta cláusula se da información sobre la codificación simple de la mayoría de los mensajes H.245 necesarios sin que se requieran codificadores/decodificadores específicos ASN.1.

NOTA – Todos los mensajes se transmiten como mensajes H.245 tunelizados, es decir, que las configuraciones de bits resultantes son codificadas como una sola CADENA DE OCTETOS de la SECUENCIA del componente fastStart de una PDU-UU H323. En los cuadros que se muestran a continuación, el octeto más a la izquierda (octeto #0) de la primera línea (palabra #0) es el primer octeto de la cadena de octetos, y va seguido por el octeto #1 de la primera línea, y así sucesivamente. El octeto #3 de la palabra #n va seguido del octeto #0 de la palabra #(n+1).

Si los números han de codificarse, para números negativos se utiliza la codificación con complemento a 2. De otro modo, se utiliza la codificación binaria simple. La codificación de números que abarcan múltiples octetos se realiza de forma que el bit más significativo del valor codificado se encuentre en el primer octeto del valor (orden de octetos de la red).

F.10.1 Apertura de canal lógico

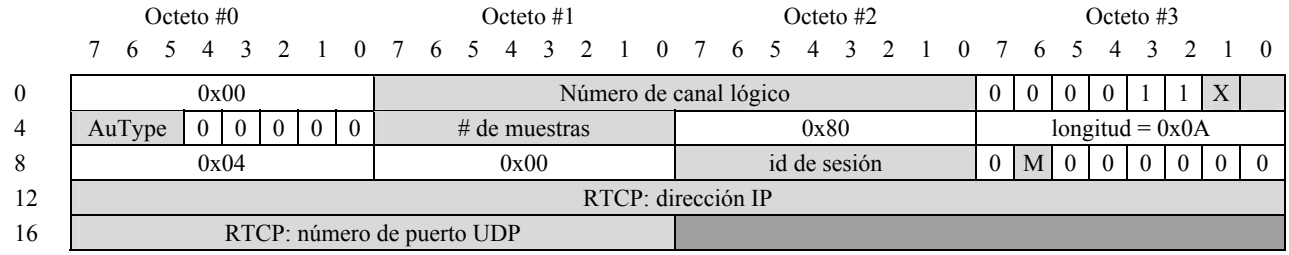
Las estructuras de **apertura de canal lógico** son utilizadas por los dispositivos SET durante el procedimiento de conexión rápida para indicar sus capacidades y abrir canales de medios simultáneamente en ambos sentidos y reconfigurar trenes de medios durante una conferencia. Por definición, las estructuras de **apertura de canal lógico** contienen solamente parámetros de canal lógico hacia adelante o parámetros de canal lógico hacia atrás.

F.10.1.1 Parámetros de canal lógico hacia adelante

Una estructura de apertura de canal lógico que contiene solamente parámetros de **ForwardLogicalChannel** puede ser codificada de tres maneras diferentes, dependiendo del tipo de audio (AuType) y del bit X.

F.10.1.1.1 Recs. UIT-T G.711 y G.729

La estructura más común es la siguiente (Recs. UIT-T G.711, G.729 y anexo A/G.729):



Número de canal lógico: Este campo contiene el número del canal lógico H.245 – 1.

Bit X: Se utiliza para distinguir entre tipos de audio básico y ampliado. Si $X = 0$, es aplicable AuType (véase el campo siguiente); de no ser así ($X = 1$), son aplicables los tipos de audio ampliados descritos más adelante (GSM principalmente) junto con una estructura de paquete diferente.

AuType: Identifica el códec de audio que se ha de utilizar. Los valores siguientes son aceptables para AuType. El bit situado más a la izquierda es el bit 1 del octeto #3 anterior, el bit situado más a la derecha es el bit 5 del octeto #4.

N.º	Descripción de códec	Valor de AuType
1	G.711, ley A a 64 kbit/s	0001
2	G.711, ley A a 56 kbit/s	0010
3	G.711, ley μ a 64 kbit/s	0011
4	G.711, ley μ a 56 kbit/s	0100
5	G.723.1	1000
6	G.729	1010
7	Anexo A/G.729	1011
8	GSM y otros (véase más adelante)	X = 1

muestras: Para los códecs 1, 2, 3, 4, 6 y 7, este componente contiene el número de muestras –1 por paquete de audio, como se define en la Rec. UIT-T H.245.

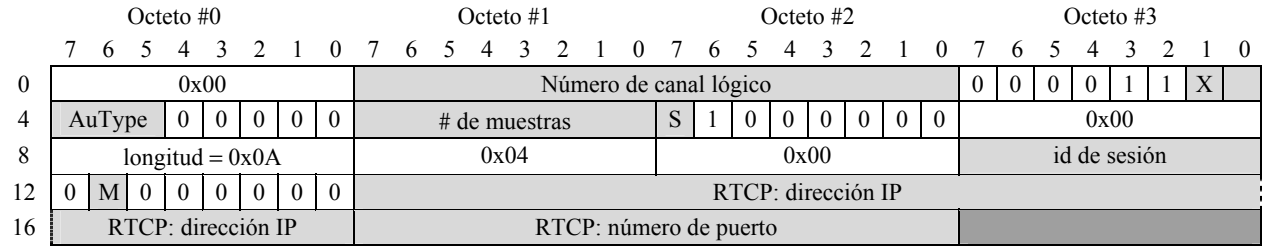
id de sesión: Contiene el parámetro id de sesión que se ha de utilizar junto con RTP/RTCP.

Bit M: Bit de dirección de multidifusión: indica que la dirección siguiente es una dirección de multidifusión. Aunque se definen muchos tipos de dirección además de IPv4 (incluidas IPv6 e IPX), las estructuras que aquí se muestran sólo son válidas para direcciones IPv4.

dirección/puerto IP de RTCP: Contiene la dirección de transporte para RTCP a la que se han de enviar los informes del receptor.

F.10.1.1.2 Códec G.723.1

Para la Rec. UIT-T G.723.1, la estructura difiere ligeramente, como se muestra a continuación:

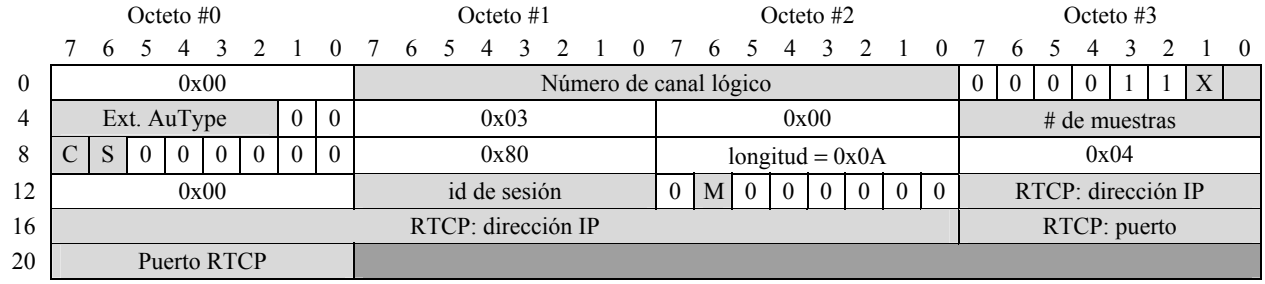


El significado de los campos es idéntico al definido para el formato anterior. Además, son importantes los campos siguientes:

Bit S: Indica soporte de la supresión del silencio si S = 1.

F.10.1.1.3 GSM

Para GSM, identificado por el bit 1 del octeto 3 fijado a X = 1, la estructura tiene el aspecto siguiente:



Los campos tienen el mismo significado que en los formatos de paquetes anteriores. Además se definen los siguientes campos para GSM:

Ext. AuType: Identifica el códec de audio ampliado:

GSM velocidad máxima = 000 0011

GSM velocidad media = 000 0100

GSM velocidad máxima mejorada = 000 0101

Bit C: C = 1 indica soporte/uso del ruido confortativo

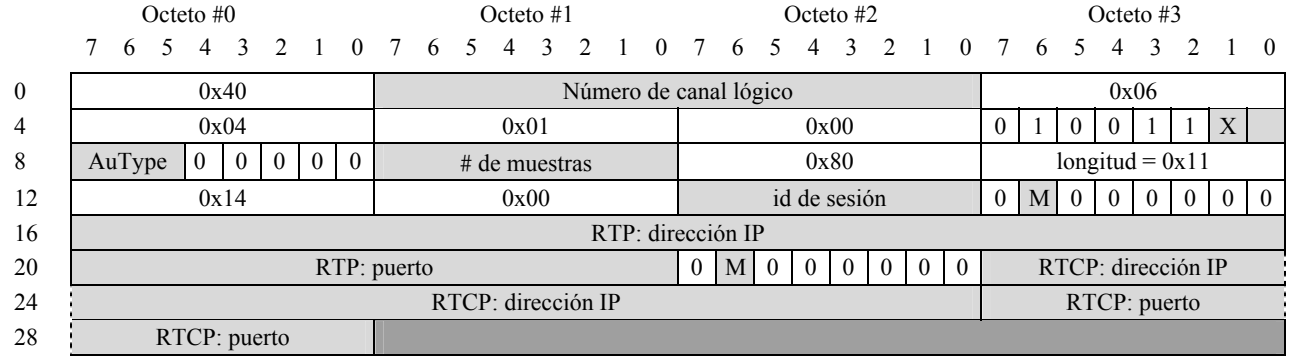
Bit S: S = 1 indica soporte/uso de la aleatorización

F.10.1.2 Parámetros de canal lógico inverso

Los mensajes de apertura de canal lógico que contienen parámetros de **canal lógico inverso** se codifican como se describe en esta subcláusula.

F.10.1.2.1 Recs. UIT-T G.711 y G.729

La estructura más común es la siguiente (Recs. UIT-T G.711, G.729 y anexo A/G.729):



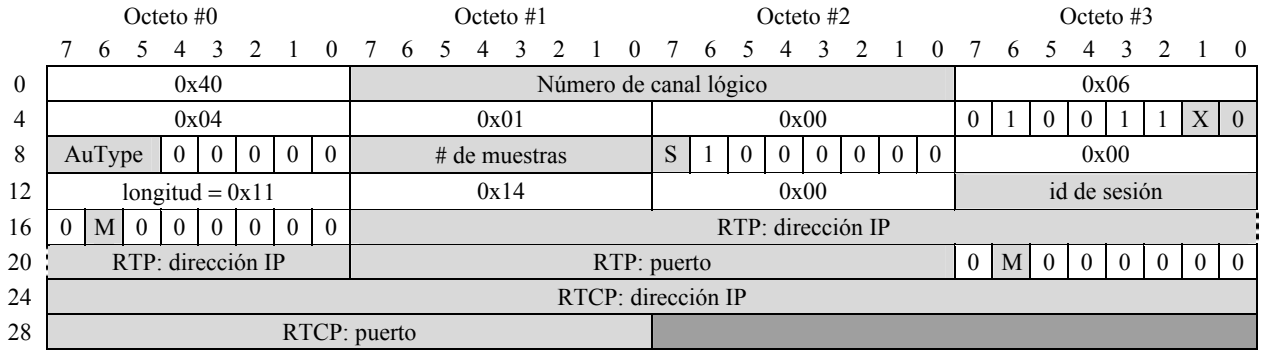
Los campos tienen el mismo significado que antes. Además, se definen los siguientes campos:

dirección/puerto IP de RTP: Dirección de transporte objetivo a la que se ha de enviar el tren de audio RTP.

dirección/puerto IP de RTCP: Dirección de transporte objetivo a la que se han de enviar los informes del emisor RTCP.

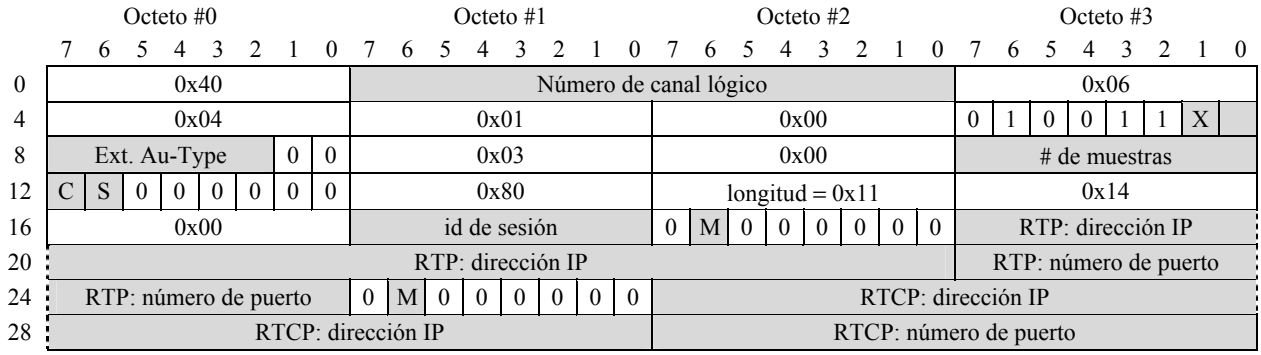
F.10.1.2.2 Rec. UIT-T G.723.1

Para la Rec. UIT-T G.723.1, la estructura difiere ligeramente de la anterior, como se muestra a continuación:



F.10.1.2.3 GSM

Para GSM identificado por el bit #1 del octeto #7 fijado a X = 1, la estructura tiene el aspecto siguiente:



Ex. AuType: Identifica el códec de audio (GSM) ampliado y se ha utilizar como sigue:

GSM velocidad máxima = 000 0011

GSM velocidad media = 000 0100

GSM velocidad máxima mejorada = 000 0101

Anexo G

Conversación mediante texto y SET mediante texto

G.1 Introducción

En todas las redes es necesario disponer de facilidades de conversación mediante texto normalizadas orientadas a los caracteres. Cuando se establecen facilidades de conversación mediante texto en protocolo multimedia, se crea una oportunidad de utilizar en una conversación una combinación de texto, vídeo y voz. La iniciativa de normalizar esta combinación surge de la necesidad que tienen las personas con discapacidades de comunicación. La disponibilidad de tener tres medios distintos de conversación ofrece mayores oportunidades de comunicación sobre cualesquiera de los medios por separado. Toda persona considerará altamente estimable la adición de conversación mediante texto normalizado, de disponibilidad común, a los servicios de conversación multimedia, mejorando así la telefonía de vídeo para obtener "conversación total".

Considerando que H.323 es un marco en que los componentes se pueden incluir cuando se requiera, los terminales mediante texto de función simple así como los terminales de texto y voz, pueden constituir elementos útiles del terminal de conversación total. Estos subconjuntos corresponden a los teléfonos con texto disponibles para la RTPC.

El protocolo de conversación mediante texto se especifica en la Rec. UIT-T T.140 [G1]. Este protocolo constituye un nivel de presentación común adecuado para conversación mediante texto directo en tiempo real en servicios multimedia y en telefonía con texto. Está basado en el código de caracteres ISO/CEI 10646 que es adecuado a cualquier idioma. Se introduce a través de los protocolos multimedia de la serie H.

Esta especificación describe cómo se agregan facilidades de conversación mediante texto al entorno multimedia H.323 en redes de paquetes.

La facilidad de conversación mediante texto está establecida en un canal de datos o un canal de voz (a los que se llama colectivamente "canales de medios") identificados por el mensaje **OpenLogicalChannel** H.245. En un canal de datos se utiliza la misma identificación para la apertura de canales de conversación mediante texto en H.324. Sólo difiere el protocolo y los procedimientos del canal de datos para transportar el protocolo T.140. El interfuncionamiento entre los sistemas H.324 y H.323 supone que los dispositivos utilizarán un canal de datos para transportar texto. Por ello, se recomienda que todos los dispositivos H.323 que apliquen el presente anexo soporten el transporte de texto por el canal de datos.

Por lo tanto, la conversación total obtiene una aplicación uniforme a través de diferentes redes. La complejidad de pasarelas y otros componentes de red se puede mantener baja.

G.2 Alcance

El alcance de este anexo es especificar los procedimientos H.323 para establecer y efectuar sesiones de conversación mediante texto en tiempo real a través de redes de paquetes en un entorno multimedia H.323. Asimismo, se especifican reglas sobre la utilización de los procedimientos H.323 que permiten a los dispositivos del tipo de punto extremo simple de

conversación mediante texto (text SET, *text conversation simple endpoint type devices*) sean creados como superconjuntos de los dispositivos de tipo punto extremo simple de audio especificados en el anexo F. La especificación SET mediante texto describe un dispositivo que se puede utilizar para conversaciones en audio y texto simultáneamente en tiempo real a través de redes de paquetes.

G.3 Referencias

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

[G1] Recomendación UIT-T T.140 (1998), *Protocolo de conversación mediante texto para aplicaciones multimedia* más enmienda 1 (2000).

[G2] RFC 4103 (2005), *RTP payload for text conversion*.

[G3] RFC 4351 (2006), *RTP payload for text conversion interleaved in an audio stream*.

G.4 Definiciones

En este anexo se definen los términos siguientes.

G.4.1 conversación total: Servicios de conversación que ofrecen comunicaciones en vídeo, texto y audio en tiempo real.

G.4.2 T140PDU: Unidad de protocolo de datos de T.140 = colección de datos para transmisión presentados en formato T.140.

G.5 Anuncio de capacidades para texto en H.323

El soporte para la comunicación de textos se puede anunciar utilizando dos capacidades diferentes incluidas en H.323. La primera es la capacidad **DataApplicationCapability.application.t140** que se encuentra en la especificación H.245. Esta capacidad es un medio de abrir un canal de datos que soporte la transmisión de texto. Corresponde al tipo MIME " text/t140" que se describe en [G2]. Aunque [G2] sólo describe el transporte de texto a través de RTP, la capacidad **DataApplicationCapability.application.t140** también puede utilizarse con TCP en contraposición a RTP.

Esta capacidad **DataApplicationCapability.application.t140** era el identificador de capacidad original añadido a H.245 para soportar texto. Cuando se aportaron nuevas mejoras a la especificación RTP para transportar texto ([G2]), se añadió un nuevo parámetro a fin de aportar un dispositivo que indique el número de caracteres por segundo que puede recibir. Las mejoras también se introdujeron para permitir el transporte de texto a través de un tren RTP separado o intercalado con otra información de audio, que correspondiese al tipo MIME "audio/t140c" en [G3]. La capacidad para transportar texto intercalado con audio se introdujo a fin de permitir a las pasarelas de la RTPC extraer señales de teléfono con texto de la RTPC y transportarlas dentro de la misma RTP como el tren de audio.

Para soportar los más recientes parámetros de [G2] y [G3] y todas las revisiones subsiguientes, así como para soportar el transporte de texto intercalado con audio, se definen aquí dos nuevas capacidades genéricas para H.245. Cuando se utilizan capacidades genéricas con parámetros, las entidades H.323 simplemente ignorarán todos los parámetros que no entiendan. Este anexo reserva identificadores de parámetros **normalizados** de 0 a 99. Los valores de parámetros **normalizados** de 100 a 127 se reservan para otras Recomendaciones del UIT-T.

Se considerará que el campo **maxBitRate** de la capacidad **DataApplicationCapability.application.t140** y las capacidades genéricas definidas en las subcláusulas siguientes están en unidades de bits por segundo, a diferencia de los 100 bits/segundo que habitualmente se utilizan en H.245. Esa misma interpretación de las unidades se aplicará a todos los mensajes H.245 que contengan un parámetro de velocidad binaria y que esté relacionado con esas capacidades de texto, incluidas la petición de modo, la instrucción de control de flujo y la indicación de control de flujo. A título de ejemplo, un valor de 192 representa 192 bits por segundo (aproximadamente 6 caracteres por segundo cuando los caracteres son de 3 octetos cada uno).

Como [G2] y [G3] utilizan T.140, donde se especifica una codificación de carácter que requiere entre 1 y 3 octetos por carácter, la utilización de parámetros en "bits por segundo" puede no ser tan útil como en "caracteres por segundo", conforme a lo que se especifica en G.5.3. No obstante, los sistemas H.323 están diseñados para indicar en velocidades binarias y no en velocidades de caracteres por segundo. De esta manera, las entidades H.323 calcularán el valor en bits por segundo anunciado que se ha de utilizar sobre la base de 3 octetos por carácter, incluso si se requiere un solo octeto para la transmisión de un carácter. Eso permite a los sistemas establecer una adecuada correspondencia entre bits por segundo y caracteres por segundo, lo que es particularmente importante ya que esos dispositivos pueden utilizar, por ejemplo, la instrucción de control de flujo para controlar adecuadamente la velocidad de transmisión desde el otro sistema y obtener resultados coherentes. De todas maneras, el parámetro caracteres por segundo sigue siendo útil cuando se utiliza como parte de un tren de cabida útil múltiple, ya que cada elemento no transportará un valor de velocidad binaria separado en el mensaje de canal lógico abierto.

NOTA – La velocidad binaria máxima anunciada en el mensaje de conjunto de capacidad de terminal puede diferir del valor de la velocidad binaria máxima utilizado en el mensaje de canal lógico abierto. Cualquier valor anunciado en un mensaje de canal lógico abierto o en instrucciones de limitación de velocidad (por ejemplo, instrucción de control de flujo) tiene prioridad con respecto a los valores en un mensaje de conjunto de capacidad de terminal.

G.5.1 Capacidades de texto por canal de datos

La capacidad original **DataApplicationCapability.application.t140** no está obsoleta y, cuando se anuncia con el UDP seleccionado como transporte, se tratará como equivalente a la nueva capacidad de texto por canal de datos que se define a continuación, pero desprovista de todo parámetro. Si bien existe una preferencia por la nueva definición de capacidad, debe mantenerse la retrocompatibilidad con los sistemas existentes, por lo que se hace la siguiente recomendación: los dispositivos que implementen este anexo anunciarán la capacidad **DataApplicationCapability.application.t140** y anunciarán la nueva capacidad genérica definida en la presente cláusula.

Para el transporte de texto por un canal de datos que corresponde al tipo MIME "text/t140" especificado en [G2], se define la siguiente capacidad genérica:

Nombre de la capacidad:	Datos T140
Clase de capacidad:	Capacidad de aplicación de datos
Tipo de identificador de capacidad	Normalizado.
Valor de identificador de capacidad	itu-t (0) recommendation (0) h (8) 323 annex(1) g (7) data(0)
maxBitRate	Se incluirá el campo maxBitRate y se indicará el valor máximo de bits por segundo. Cuando se utilice la instrucción de control de flujo u otras señales relativas a esta capacidad, de considerará que las unidades de todos los campos maxBitRate estarán en bits/s, a diferencia de las típicas unidades 100 bits/s utilizadas en H.245. Ello se debe a que la velocidad binaria de la comunicación de texto en tiempo real es naturalmente baja.
nonCollapsing	Este campo no se incluirá y se ignorará si es recibido.
nonCollapsingRaw	Este campo no se incluirá y se ignorará si es recibido.
transport	Este campo no se incluirá.

G.5.2 Capacidad de texto por canal de audio

Para el transporte de texto por un canal de audio, se define la capacidad genérica siguiente correspondiente al tipo MIME "audio/t140c" especificado en [G3].

Nombre de la capacidad:	Datos T140
Clase de capacidad:	Capacidad de audio
Tipo de identificador de capacidad	Normalizado.
Valor de identificador de capacidad	itu-t (0) recommendation (0) h (8) 323 annex(1) g (7) data(0)
maxBitRate	Se incluirá el campo maxBitRate y se indicará el valor máximo de bits por segundo. Cuando se utilice la instrucción de control de flujo u otras señales relativas a esta capacidad, de considerará que las unidades de todos los campos maxBitRate estarán en bits/s, a diferencia de las típicas unidades 100 bits/s utilizadas en H.245. Ello se debe a que la velocidad binaria de la comunicación de texto en tiempo real es naturalmente baja, incluidas las velocidades binarias bajas utilizadas por numerosos protocolos de teléfono con texto de la RTPC.
nonCollapsing	Este campo no se incluirá y se ignorará si es recibido.
nonCollapsingRaw	Este campo no se incluirá y se ignorará si es recibido.
transport	Este campo no se incluirá.

G.5.3 Parámetro genérico en caracteres por segundo

Cuando se utilizan, ya sea una capacidad de audio genérica o una capacidad de datos genérica para señalizar texto, un punto extremo puede también anunciar tanto en el conjunto de capacidades del terminal, como en el canal lógico abierto, o en ambos, la capacidad para recibir un número específico de caracteres por segundo. Este parámetro se define en [G2] y [G3] y se señaliza de la siguiente manera:

Nombre del parámetro:	cps
Descripción del parámetro:	Ésta es una capacidad desplomable. Indica el número máximo de caracteres por segundo que se pueden recibir en una sesión. Cuando se transporta dentro de un OLC, indica la velocidad máxima de transmisión que el otro punto extremo puede utilizar si abre una sección de texto correspondiente.
Valor de identificador de parámetro:	normalizado: 0
Estado del parámetro:	Opcional
Tipo de parámetro:	unsignedMin
Reemplaza:	–

G.6 Procedimientos para la apertura de canales para conversación mediante texto conforme a T.140

Los requisitos de sesión del protocolo T.140 se reflejan en la siguiente especificación para el establecimiento de canal utilizando la estructura de mensaje de canal lógico abierto H.245 en el entorno H.323.

Para establecer la sesión T.140 como un canal de datos se puede seleccionar un canal fiable (TCP) o no fiable (UDP). El canal no fiable estará siempre soportado. Este canal se puede seleccionar en los casos en que se espera que el terminal participe en sesiones en las que el canal fiable no es favorable o es imposible de utilizar.

- En el intercambio de capacidades, cuando se usa un canal fiable, especifíquese:

```
DataApplicationCapability.application = t140
DataProtocolCapability = tcp
```

- En las capacidades de intercambio, cuando se utiliza un canal no fiable, especifíquese:

```
DataApplicationCapability.application = t140
DataProtocolCapability = udp
```

o

```
DataApplicationCapability.application = genericDataCapability
   (La capacidad de datos genérica se debe especificar de conformidad con
   G.5.1)
```

o

```
AudioCapability = genericAudioCapability
   (La capacidad de datos genérica se debe especificar de conformidad con
   G.5.2)
```

- En el procedimiento de canal lógico abierto, especifíquese:

```
OpenLogicalChannel.forwardLogicalChannelParameters = dataType
DataType = data
```

Y selecciónese un canal fiable o no fiable para la transferencia de datos T.140 especificando las capacidades **`DataApplicationCapability`** y **`DataProtocolCapability`** como se indica anteriormente.

o

```
OpenLogicalChannel.forwardLogicalChannelParameters = dataType
DataType = audioData
```

La selección de los **dataType**, ya sea **audioData** o **data**, depende de las capacidades soportadas y preferidas.

Se pueden utilizar los procedimientos de conexión rápida o los procedimientos normales de señalización de canal lógico H.245.

Los conceptos de nodo de destino y nodo de origen que figuran en la Rec. UIT-T T.140 se hacen corresponder con los dos puntos extremos H.323.

El identificador de usuario T.140 es un alias para el punto extremo H.323 lejano.

G.7 Encuadre de trama y almacenamiento en memoria tampón de los datos T.140

La transmisión de datos T.140 se efectuará de acuerdo con las siguientes especificaciones, de manera diferente para los canales fiable y no fiable.

NOTA – En esta cláusula y las subsiguientes, "datos" se refiere a los datos T.140, independientemente de si son transportados por un canal de "datos" o un canal de "audio". Las expresiones "canal de datos" o "canal de audio" se utilizarán explícitamente cuando sea necesario establecer una distinción.

G.7.1 Consideraciones comunes

Los datos T.140 se pueden almacenar en una memoria tampón antes de la transmisión en el canal. En canales de baja velocidad binaria se recomienda esta memorización intermedia para reducir la tara de paquete. Por defecto se recomienda el almacenamiento de datos en memoria intermedia en intervalos de 300 ms.

En recepción, se extrae el contenido del canal de medios y se utiliza como datos T.140.

G.7.2 Utilización de canales fiables

Cuando para la transmisión del protocolo T.140 se selecciona un canal fiable, se utiliza TCP, y los datos T.140 se transmiten en el canal sin ulterior alineación de trama.

G.7.3 Utilización de canales no fiables

Cuando para la transmisión del protocolo T.140 se especifica un canal no fiable, se utiliza RTP. Los detalles del formato de cabida útil RTP "T140" figuran en [G2] y [G3]. Se deben utilizar los procedimientos recomendados en [G2] y [G3]. La atribución del tipo de cabida útil es dinámica. A menos que se señale explícitamente, el formato de cabida útil "T140", se utiliza el tipo de cabida útil 96 y el tipo de cabida útil para paquetes de redundancia, será el tipo de cabida útil 98.

Los procedimientos ofrecen la posibilidad de incluir un número de T140PDU ya transmitidos en el paquete. Esto se efectúa para incluir datos redundantes con objeto de reducir los riesgos de pérdida de datos.

La estación de transmisión puede seleccionar un número de generaciones T.140 PDU para retransmitir en cada paquete. Un número elevado introduce mejor protección frente a la pérdida de texto. Si las condiciones de la red no son conocidas, se recomienda utilizar dos generaciones. Asimismo, se recomienda utilizar no más de seis generaciones.

Se debe utilizar RTCP para supervisar la pérdida de paquetes, de modo tal que se debe efectuar una decisión sobre el número de generaciones de datos redundantes que se ha de transmitir.

G.8 Interacción con facilidades de conversación mediante texto en otros dispositivos

La información de esta cláusula no es normativa y se proporciona sólo a fines de información, y está fuera del alcance de este anexo.

La Rec. UIT-T T.140 se establece como protocolo de conversación mediante texto a través de una diversidad de protocolos multimedia de la serie H, conferencia de datos T.120 y para teléfonos con texto conforme a la Rec. UIT-T V.18. Los canales de medios son específicos a cada entorno.

Cuando se establecen las pasarelas a estos diferentes entornos, el canal T.140 en el entorno H.323 se pone en correspondencia con el canal T.140 en el otro entorno. Los datos del canal T.140 se pueden transferir en forma transparente a través de la pasarela.

Cuando se establecen pasarelas para otros protocolos de conversación mediante texto, los mecanismos de protocolo y de datos de ese protocolo se pondrán en correspondencia con un canal de conversación mediante texto T.140 en la pasarela. Estas funciones de correspondencia se pueden denominar ecualizadores T.140. Las funciones de pasarela a los diferentes sistemas de teléfono con texto implican la utilización de ecualizadores T.140.

La figura G.1 presenta un panorama de servicios de pasarela y protocolos de conversación mediante texto.

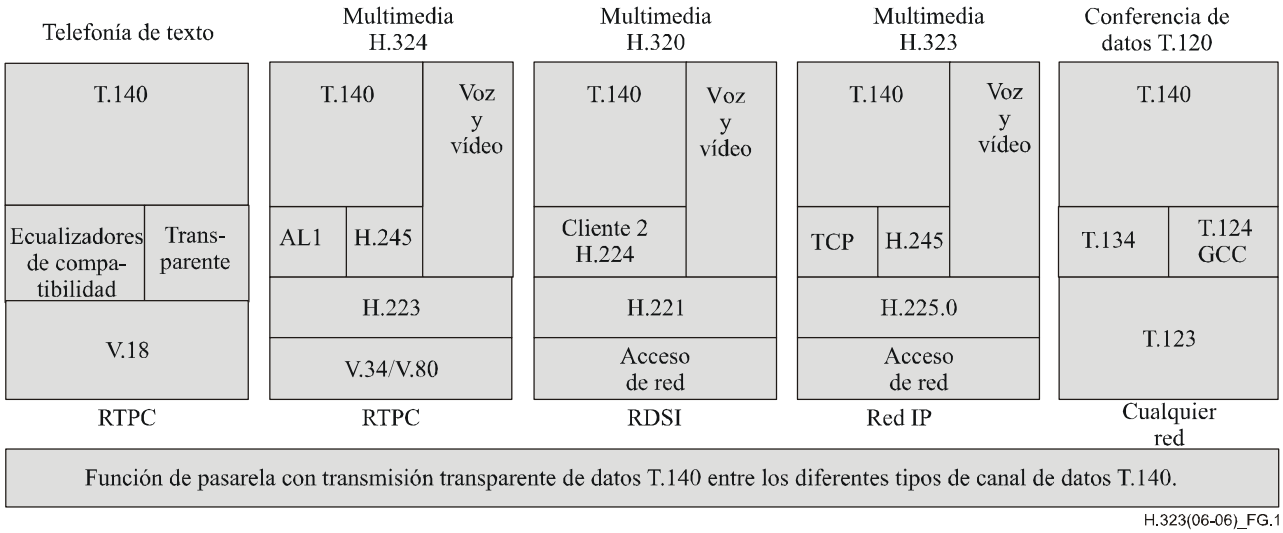


Figura G.1/H.323 – Recomendaciones multimedia de conversación mediante texto en tiempo real y necesidades de interfuncionamiento

G.9 Consideraciones multipunto

Sin nuevas especificaciones, existen tres alternativas opcionales para puntos extremos H.323 con conversación mediante texto T.140 para participar en conversaciones mediante texto multipunto.

Alternativas:

- Se establece un canal T.140 separado para cada punto extremo H.323 distante. Los trenes de texto pueden ser coordinados para indicación visual a través de una interfaz de usuario que tiene en cuenta conversaciones multipunto, que también transmite datos T.140 a todos los puntos extremo conectados.
- Una MCU coordina el tren de datos T.140 al punto extremo H.323 para contener datos procedentes de una serie de puntos extremos distantes.
- En lugar de los procedimientos descritos en este anexo, se utiliza el miembro de aplicación T.134 de conferencia de datos T.120 como el canal para datos T.140. Las sesiones multipunto se coordinan a través de los conceptos T.120.

G.9.1 Situaciones para conversación mediante texto multipunto

Para aclarar la utilización de la conversación mediante texto, y especialmente los diferentes casos multipuntos, se presentan los siguientes ejemplos de esquemas y aplicaciones posibles sin ser normativos.

G.9.1.1 Persona a persona

El caso de una persona con otra representa una conversación directa mediante texto entre dos partes, donde el texto introducido en un punto extremo se presenta visualmente carácter por carácter o en pequeños grupos de caracteres a medida que se van registrando en el otro extremo. Ejemplos típicos son situaciones como la tradicional telefonía con texto en la RTPC y aplicaciones de conversación multimedia con vídeo, texto y datos utilizados para llamadas de persona a persona. Véase la figura G.2.

Anne	Eve
Hola, soy Anne ¿Te has enterado que iré a París en noviembre?	¡Hola Anne, estoy contenta de que me hayas llamado! No, no sabía nada. ¿Qué es lo que te trae por aquí?

Figura G.2/H.323 – Posible presentación visual de una llamada de texto de persona a persona

G.9.1.2 Muchos participantes entre sí

Todos los usuarios pueden escribir, presentando una conferencia no gestionada.

La indicación visual se puede disponer como se especifica en la Rec. UIT-T T.140 con una ventana para cada participante. Véase la figura G.3.

Anne	Eve
Hola, soy Anne. ¿Te has enterado que iré a París en noviembre?	¡Hola muchachos! ¿Cómo estás Steve?
Steve	**Bill**
Hola, soy Steve. Estoy bien.	¡Hola Anne! ¡Me alegro que estén en el gran Internet!

Figura G.3/H.323 – Posible presentación visual de una sesión de texto no gestionada en la que intervienen cuatro participantes en conferencia

La indicación visual de una conferencia que intervienen muchos participantes se puede presentar en una ventana con etiquetas para cada inserción de un participante (estilo IRC) (véase la figura G.4):

Steve > ¡Hola!
Anne > ¿Te has enterado que iré a París en noviembre?
Bill > ¡Hola Anne! ¡Me alegro que estés en el gran Internet!
Eve > ¡Hola muchachos! ¿Cómo estás Steve?
Steve > Estoy bien.

Figura G.4/H.323 – Modo de presentación visual posible de una sesión de texto con cuatro participantes

G.9.1.3 Un participante con muchos participantes con derecho gestionado a escribir

Un participante por vez tiene derecho a transmitir texto a varios participantes. El derecho a escribir puede pasar a otros participantes en una reunión gestionada.

Una aplicación típica de este caso se efectúa en educación a distancia en la que el profesor tiene normalmente el derecho de escribir, pero puede transferir esa facilidad a un participante.

G.9.1.4 Un participante con muchos participantes con derecho fijo a escribir

Un participante envía texto en la sesión desde un punto extremo fijo y los otros puntos extremos presentan la indicación visual en una ventana de recepción. El derecho a escribir no se puede transferir.

Una aplicación típica de este caso se encuentra en discursos subtitulados.

Los terminales de usuario pueden ser puntos extremos de bajo grado de acoplamiento H.332. Véase la figura G.5.

Estamos muy satisfechos de anunciarles hoy un nuevo sistema superior para viajes intergalácticos

Figura G.5/H.323 – Ejemplo de una sesión de texto de un usuario con muchos participantes

G.10 SET mediante texto: Dispositivos de tipo punto extremo simple de conversación mediante texto

Esta parte del anexo especifica los dispositivos de tipo punto extremo simple de conversación mediante texto que funciona utilizando un subconjunto bien definido de protocolos H.323. Estos dispositivos son adecuados para aplicaciones de telefonía con texto IP a la vez que mantienen el interfuncionamiento con dispositivos regulares H.323, versión 2 (1998) o posterior. Esta especificación añade facilidades de conversación mediante texto en tiempo real conforme a la Rec. UIT-T T.140 a la telefonía vocal IP como se especifica en el anexo F, para integrar el teléfono con texto IP con prestaciones simultáneas de voz y texto.

G.10.1 Introducción a los dispositivos SET mediante texto

El procedimiento y detalle del protocolo de un dispositivo de teléfono con texto de tipo punto extremo simple para redes IP se define en términos de modificaciones y adiciones a la especificación SET audio que figura en el anexo F. El dispositivo se denomina en este documento SET mediante texto.

Los conceptos generales de dispositivos de tipo punto extremo simple (SET) se describen en el anexo F. El presente dispositivo constituye una serie de modificaciones a la especificación SET audio que comprende lo que es necesario para añadir funcionalidad de conversación de texto al SET audio. Este anexo indica el número de apartado del original.

G.10.2 Aspectos generales de la funcionalidad del sistema SET mediante texto (véase F.6)

En **Capacidades de medios**, modifíquese:

- capacidad de datos obligatoria; T.140.

G.10.3 Procedimientos para dispositivos SET mediante texto (véase F.7)

Modifíquese el punto paquetización y transporte de medios como sigue:

- paquetización y transporte de medios (H.225.0, RTP, TCP, T.140) – Véase F.7.4.

G.10.4 Señalización RAS (RAS H.225.0 – Véase F.7.1)

Como para SET audio, se utiliza código tipo punto extremo H.225.0 SET preservado para SET mediante texto.

Bit 2 = 1 Indica que el dispositivo tiene capacidades para SET mediante texto.

Bit 2 = 0 Indica que el dispositivo no tiene capacidades para SET mediante texto.

NOTA – Los protocolos del controlador de acceso se deben diseñar de modo tal que permitan sesiones de voz únicamente con un dispositivo SET mediante texto.

G.10.5 Señalización de la llamada (control de la llamada H.225.0 – Véase F.7.2)

El bit 2 del código tipo de punto extremo H.225.0 SET se utiliza para indicar una función SET mediante texto.

G.10.6 Capacidad de datos (véase F.7.3.3.3)

Se especificará capacidad de datos T.140.

DataApplicationCapability.application = t140.

G.10.7 Normas adicionales para la utilización de capacidades (véase F.7.3.3.9)

Las capacidades de audio y de datos se indicarán únicamente en aplicación del procedimiento de conexión rápida y el intercambio repetido de estructuras de **apertura de canal lógico**, como se especifica en el anexo F.

Se supondrán los siguientes valores de las entradas del cuadro **MultiplexCapability** como para SET audio con las siguientes excepciones:

```
mediaDistributionCapability
centralizedDataVERDADERO
distributedDataVERDADERO/FALSO, según proceda, FALSO por defecto
```

G.10.8 Mensaje de señalización de canal lógico (véase F.7.3.4)

Añádase en la petición de apertura de canal lógico.

```
OpenLogicalChannel.forwardLogicalChannelParameters.DataType.data = t140
MultiplexParameters     según corresponda para el tipo de canal fiable o no
                        fiables seleccionado.
```

G.10.9 Intercambio de medios (véase F.7.4)

Para el intercambio de texto, los terminales SET deberán seguir los procedimientos especificados en este anexo.

G.10.10 Parte iniciadora (véase F.7.6.1)

Añádase:

La estructura **apertura de canal lógico** ofrecerá la misma codificación de datos para texto que la que fuera ofrecida en la llamada inicial.

G.10.11 Terminales SET mediante texto que no tienen en cuenta la funcionalidad de conferencia (véase F.7.7.1)

Añádanse los siguientes puntos de funcionalidad:

- Fusionar diversas sesiones de texto entrantes al dispositivo SET mediante texto.
- Traducir las direcciones de transporte para el tren de texto.
- Transferir y, posiblemente, transcodificar trenes de datos de texto.

G.10.12 Soporte de conferencias de bajo grado de acoplamiento (Rec. UIT-T H.332) (véase F.7.8)

Un dispositivo SET mediante texto puede participar en una conferencia de bajo grado de acoplamiento utilizando los procedimientos H.332 siempre que la conferencia se amplíe para incluir texto y el canal para la transmisión de texto se seleccione para utilizar un canal no fiable.

Anexo J

Seguridad para el anexo F

J.1 Introducción

Este anexo describe la seguridad para los tipos de punto extremo simple del anexo F. El perfil de seguridad especificado se basa en H.235v2 y utiliza el perfil de seguridad básico descrito en el anexo D/H.235v2. El perfil de seguridad presentado en el anexo J aplica la Rec. UIT-T H.235v2 para los fines de los tipos de punto extremo simple y sus requisitos de seguridad específicos. El perfil de seguridad selecciona las características apropiadas de H.235 con su rico conjunto de opciones.

El texto descrito contiene una sinopsis del perfil de seguridad; el anexo D/H.235v2 incluye todos los detalles técnicos y de implementaciones.

Básicamente, un **tipo de punto extremo simple de seguridad (SET de seguridad)** es un SET definido por el anexo F, que implementa además ciertas características de seguridad de este anexo.

Actualmente, este anexo se limita solamente a un "SET audio de seguridad (SASET)" y deja cualesquiera otros tipos de punto extremo simple de seguridad (por ejemplo, SET FAX, terminal de texto de seguridad, SET vídeo de seguridad, etc.) en estudio.

J.2 Convenios de especificación

Conviene dar algunas explicaciones para entender los términos utilizados en este anexo:

El anexo se aplica al **perfil de seguridad básico** para un SASET (**terminal de punto extremo simple de audio seguro**). El perfil de seguridad básico proporciona la seguridad básica por medios sencillos utilizando técnicas criptográficas basadas en contraseñas seguras; la funcionalidad proporcionada debe ser implementada por cada SASET. El perfil de seguridad básico puede ser utilizado en el **perfil de seguridad de criptación de la voz** para conseguir confidencialidad de la voz, si es necesario. Queda en estudio si habrá otros perfiles de seguridad más sofisticados para los SASET.

Para evitar referencias a una marca registrada (RC2®), este anexo hace realmente referencia a un algoritmo de criptación "compatible con la RC2".

Este anexo utiliza términos de seguridad conocidos tales como clave, gestión de claves y SET, que tienen diferentes significados en otros contextos (por ejemplo, teclado táctil, gestión de claves de características Q.931/Q.932, y protocolo de transacción electrónica segura).

J.3 Alcance

Este anexo describe la seguridad para tipos de punto extremos simples. Como se indica en F.3 actualmente incluye:

- **Terminal telefónico simple seguro** (tipo de punto extremo simple de audio seguro) – Definido en el presente anexo (véase J.6).

Cualesquiera otros SET de seguridad quedan en estudio.

J.4 Abreviaturas

En este anexo se utilizan las siguientes siglas.

DES Norma de criptación de datos (*data encryption standard*)

GK Controlador de acceso (*gatekeeper*)

HMAC Código de autenticación de mensaje troceado (*hashed message authentication code*)

MAC Código de autenticación de mensaje (*message authentication code*)

RAS Registro, admisión y situación (*registration, admission & status*)

RTP Protocolo en tiempo real (*real time protocol*)

SASET Tipo de punto extremo de audio simple de seguridad (*secure audio simple endpoint type*)

SET Tipo de punto extremo simple (*simple endpoint type*)

SHA Algoritmo troceado asegurado (*secure hash algorithm*)

UIT Unión Internacional de Telecomunicaciones

J.5 Referencias normativas

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

– Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes*.

– Recomendación UIT-T H.235 (2000), *Seguridad y criptado para terminales multimedia de la serie H (basados en las Recomendaciones H.323 y H.245)*.

– Recomendación UIT-T H.245 (2006), *Protocolo de control para comunicación multimedia*.

– IETF RFC 2268 (1998), *A Description of the RC2® Encryption Algorithm*.

J.6 Tipo de punto extremo de audio simple de seguridad (SASET)

En este anexo se describen los aspectos básicos de los **tipos de punto extremo de audio simple de seguridad (SASET)**. Ejemplos de un SASET es un teléfono simple de seguridad.

J.6.1 Hipótesis

El perfil de seguridad básico impone el modelo con encaminamiento por controlador de acceso para los SET del anexo F. Los SASET y otras entidades H.323 que implementan este perfil de seguridad (por ejemplo, los controladores de acceso) se supone que implementan el procedimiento de conexión rápida.

De acuerdo con el anexo F, el perfil de seguridad básico impone el procedimiento de conexión rápida con elementos de gestión integrada de claves, pero no soporta la tunelización H.245. Por tanto, el perfil básico no provee medios de actualización de claves y de sincronización utilizando mensajes H.245 (tunelizados). Los SASET que implementan sólo el perfil de seguridad básico pero que siguen necesitando algún mecanismo de actualización de claves deben detener la llamada, y reconectar, y obtener por tanto una nueva clave de sesión.

J.6.2 Sinopsis

La seguridad básica es aplicable en entornos administrados con claves/contraseñas simétricas asignadas entre las entidades (SASETs-controlador de acceso, controlador de acceso-controlador de acceso).

El cuadro J.1 resume todos los procedimientos definidos en el anexo D/H.235v2.

Cuadro J.1/H.323 – Sumario de tipos de punto extremo de audio simple de seguridad (véase el anexo D/H.235v2)

Servicios de seguridad	**Funciones de llamada**						
	RAS	**H.225.0**		**H.245 (nota)**	**RTP**		
Autenticación	*Contraseña HMAC-SHA1-96	*Contraseña HMAC-SHA1-96		*Contraseña HMAC-SHA1-96			
No repudio							
Integridad	*Contraseña HMAC-SHA1-96	*Contraseña HMAC-SHA1-96		*Contraseña HMAC-SHA1-96			
Confidencialidad					♦DES de 56 bits	♦RC2 de 56 bits compa-tible	♦DES triple de 168 bits
Control de acceso							
Gestión de claves	*Asignación de claves por abono	*Asigna-ción de claves por abono	♦Inter-cambio de claves Diffie-Hellman autenti-cado	♦Gestión de claves de sesión H.235 integrada (distribu-ción de claves, actualización de claves utilizando DES de 56 bits/ RC2 de 56 bits compatible/DES triple de 168 bits)			

* Área azul: Esquema basado en contraseñas

♦ Área verde: Perfil de seguridad de criptación de la voz

NOTA – H.245 incluida en H.225.0 conexión rápida.

Para la autenticación y la integridad, el usuario utilizará un esquema basado en contraseñas (área azul en el cuadro J.1). El esquema basado en contraseñas se recomienda vivamente para la autenticación debido a su simplicidad y facilidad de implementación. El troceo de los campos en los mensajes H.225.0 es el método recomendado para la integridad de los mensajes (también utilizando el esquema de contraseñas). Los SASET realizan la autenticación en unión de la integridad utilizando el mismo mecanismo de seguridad común.

Los SASET, cuando introducen el perfil de seguridad de criptación de la voz (área verde en el cuadro J.1) implementará la DES de 56 bits como algoritmo de criptación por defecto; los SASET pueden implementar la DES triple de 168 bits mientras que los SASET que aplican criptación exportable pueden implementar RC2 compatible de 56 bits.

Para la confidencialidad de la voz, el esquema sugerido es la criptación utilizando RC2 compatible, DES o tipo DES triple basada en el modelo comercial y en el requisito de exportabilidad. Algunos entornos que ofrecen cierto grado de confidencialidad pueden no requerir criptación de la voz. En este caso, el acuerdo de claves Diffie-Hellman y otros procedimientos de gestión de claves tampoco son necesarios.

Los medios de control de acceso no se describen explícitamente; pueden introducirse localmente sobre la información recibida transportada dentro de campos de señalización H.235 (ClearTokem, CryptoToken).

Esta Recomendación no describe procedimientos de asignación de contraseñas/claves secretas en régimen de abono con gestión y administración. Dichos procedimientos pueden producirse por medios que no son parte de este anexo.

Los SASET pueden utilizar los servicios de extremo posterior con arreglo al procedimiento descrito en I.4.6/H.235v2.

Anexo K

Canal de transporte de control de servicio basado en HTTP

K.1 Introducción

En este anexo se describe una forma opcional de controlar servicios suplementarios en un entorno H.323. Mediante la apertura de una conexión separada que transporta un protocolo de control de servicio independiente, se pueden desarrollar y desplegar nuevos servicios sin realizar actualizaciones de los puntos extremos H.323.

El canal de control del servicio tiene por objeto ser utilizado en una amplia gama de servicios, algunos de los cuales requiere la utilización de señalización H.450 u otra delegada (por ejemplo, como en el apéndice III) para la invocación/ejecución. Puesto que dicho canal es independiente del servicio, no se definen servicios específicos ni se preconiza ninguno en concreto. Los intercambios de datos en este canal tienen por objetivo ser informativos (en la interfaz de usuario) y deben ser seguidos de las acciones adecuadas (por ejemplo, invocaciones H.450) en el plano de señalización cuando ello sea necesario. Aunque algunas aplicaciones del lado del servidor requieran soportar servicios H.450 para interfuncionamiento, el presente anexo es totalmente independiente de las Recomendaciones de la serie H.450.x.

El canal de control de servicio puede ser utilizado para servicios relacionados con la llamada y servicios no relacionados con la llamada. Puede estar abierto entre el terminal y la red o entre dos puntos extremos (de una llamada, o con una conexión independiente de la llamada).

Si bien pueden utilizarse diversos protocolos, en este anexo se describe la utilización del protocolo de transferencia de hipertexto (HTTP, *hypertext transfer protocol*). HTTP es un protocolo abierto, flexible, con una sistema de protección amigable y que resulta bien conocido. Cualquier dispositivo que declare que soporta el anexo K soportará el protocolo HTTP como una forma de transporte para el control del servicio y opcionalmente el protocolo S-HTTP para aplicaciones que requieren seguridad. El protocolo de aplicación de servicio real es dinámico y se identifica utilizando tipos MIME en la señalización HTTP. Algunos ejemplos de aplicaciones incluyen páginas XML que pueden incluir Java™ y guiones, la descarga de tonos y locuciones que deben reproducirse al cliente, la carga de guiones de procesamiento de llamadas desde los clientes a un controlador de acceso, etc. Aunque este anexo se centra en servicios suplementarios dirigidos por el usuario, este canal de control también puede ser utilizado para otros fines. Por ejemplo, podría utilizarse para potenciar el soporte lógico o para lanzar publicidad a los clientes.

En la cláusula K.2 se describe la utilización de esta Recomendación para proporcionar el URL de la conexión HTTP entre el proveedor de servicio y el cliente, en la cláusula K.3 se ilustra la utilización de HTTP y en la cláusula K.4 se presentan algunos ejemplos de posibles servicios y la correspondiente señalización.

La interfaz entre el plano de control del servicio y el plano de control de la llamada en el cliente o en el proveedor de servicio no está en el alcance de este anexo, pero podría incluir etiquetas HTML o XML tales como "enviar correo electrónico a" o URL de elementos H.323. Véase la figura K.1.

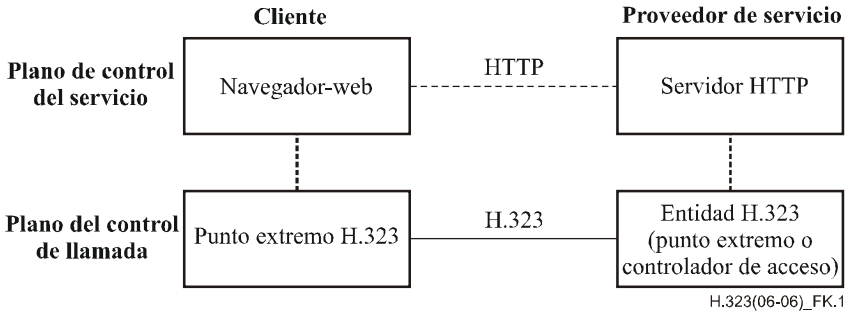


Figura K.1/H.323 – Visión general del sistema para el control de servicio basado en HTTP

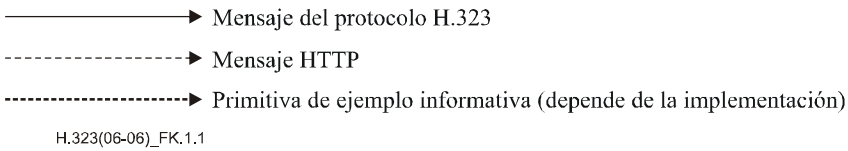
En general, la definición e implementación de las funciones de control y de los servicios que presenta un URL determinada son cuestiones que dependen del proveedor del URL (pueden soportarse servicios normalizados o no normalizados). Si el control del servicio interactúa con el procesamiento de llamada H.323, el proveedor del URL debe establecer las vinculaciones entre el servicio HTTP y los servicios H.323/H.450 que soporta el controlador de acceso o el punto extremo.

Puesto que el canal de control de servicio HTTP carece de estados y desconoce los servicios, no tiene en cuenta los problemas de las interacciones entre servicios. Sin embargo, una aplicación que utilice este canal de control de servicio debe tener un cuidado especial en que ello sea tenido en cuenta.

Los diagramas de secuencias o las referencias a la señalización H.323 que se incluyen en este anexo son sólo ejemplos informativos que describen posibles interacciones con el control del servicio y el control de llamada. No redefinen las reglas de señalización H.323, pues en aras de la brevedad, la mayoría están muy simplificados.

K.1.1 Notación

Se utiliza la notación siguiente:



Los mensajes HTTP y RAS se escriben en mayúsculas (HTTP:GET, RAS:ARQ) y los mensajes de señalización de llamada H.225.0 se escriben con la primera letra mayúscula (Establecimiento). Los puntos de código ASN.1 de H.225.0 se escriben en negrita (**ServiceControlAddress** (**dirección de control de servicio**)).

K.2 Control de servicio en H.323

En esta cláusula se describe cómo se utilizan los mensajes H.323 para mantener las sesiones de control de servicio.

K.2.1 Sesión de control de servicio

Una sesión de control del servicio es una relación unidireccional entre la entidad cliente y el proveedor de servicio, tal como ocurre en el caso de una sesión HTTP. Se inicia desde el cliente después de la recepción del URL **ServiceControlAddress** en mensajes H.225.0. el URL puede ser recibida a través de dos canales de señalización H.323 diferentes:

- Una estructura **ServiceControlSession** (**dirección de control de servicio**) que contiene un URL se recibe en un mensaje en el canal RAS. Si no hay ningún mensaje apropiado que enviar, se puede enviar el mensaje indicación de control de servicio (SCI) al punto extremo en cualquier momento.
- Una estructura **ServiceControlSession** que contenga un URL se recibe en un mensaje del canal de señalización de la llamada H.225.0.

La sesión de control del servicio se identifica con un **sessionId** (**identificador de sesión**) inequívoco del canal de señalización. Los **sessionId** recibidos a través del RAS y de la señalización de llamada pueden superponerse pues un emisor desconoce la existencia de los demás.

Un proveedor de servicio que desee iniciar una nueva sesión de control de servicio lo hace enviando al cliente una estructura **ServiceControlSession**. Ésta contiene un nuevo **sessionId**, el URL correspondiente al servicio y el campo motivo puesto a "**apertura**" ("**open**"). El cliente puede abrir una conexión con dicha dirección y solicitar el recurso al URL, pero el cliente no envía ningún acuse de recibo en el plano de señalización de la llamada. Si el usuario desea dar por terminada la sesión, por ejemplo, cerrando una ventana de la sesión, lo hace sin enviar notificación alguna al proveedor.

Si un proveedor de servicio necesita notificar a un punto extremo nuevos servicios o eventos relacionados con una sesión previamente abierta, lo puede hacer emitiendo una nueva estructura **ServiceControlSession** en el RAS o canal de señalización de la llamada (tal como se ha hecho en la secuencia "apertura"). La estructura contendrá el mismo **sessionId** que antes (para reutilizar el mismo recurso, por ejemplo, la ventana en pantalla), un nuevo URL que debe ser cargado y el motivo puesto a "**refresh**" (**refresco**).

Si el proveedor de servicio necesita terminar la sesión, puede enviar una estructura **ServiceControlSession** con el mismo **sessionId** y el motivo puesto a "**cierre**". Si el cliente aún tiene la sesión abierta, debería cerrar todos los recursos, como por ejemplo, ventanas dedicadas a la sesión.

El motivo por el que deben soportarse múltiples sesiones es que otros nodos de proveedores de servicio que no están relacionados con éstos pueden utilizar los mismos mecanismos de notificación, por ejemplo, el canal de señalización de la llamada. Las aplicaciones de servicio que utilicen lo especificado en este anexo, deben evitar sobreutilizar el número de sesiones, pues numerosas notificaciones emitidas muy rápidamente pueden confundir a un usuario final. A los clientes que soportan este anexo no se les exige que soporten más de dos sesiones, una relacionada con la llamada y la otra no.

K.2.2 Control de servicio no relacionado con la llamada

Para proporcionar servicios relacionados con la sesión de registro, y no con una llamada en particular, el controlador de acceso puede devolver una estructura **ServiceControlSession** que contenga un URL en el mensaje RCF. El URL devuelta debería ser completa en términos de definición del protocolo, servidor y recursos, es decir, <protocol>://<server-address>/<resource>. El punto extremo puede cargar este URL y mostrar los servicios y funciones de control de servicios tal como son proporcionados por los datos de dicho URL (por ejemplo, una página web con menús y enlaces).

Si la red necesita informar al punto extremo sobre eventos relacionados con los servicios durante una llamada o durante el registro, puede emitir a dicho punto extremo un mensaje Indicación de control de servicio (SCI, *service control indication*) con un URL. Para indicar que ese URL está relacionada con una sesión de control de servicio no relacionada con la llamada que ya se encuentra activa, el **sessionId** coincidirá con el anterior y el campo **callSpecific** (**específico de llamada**) no estará presente. El punto extremo puede entonces cargar dicho URL y ser actualizado con servicios y funciones de control de servicio. Un punto extremo que reciba dicho mensaje SCI responderá con un mensaje Respuesta de control de servicio (SCR, *service control response*) para evitar retransmisiones del mensaje SCI desde el proveedor. El mensaje SCR sólo constituye un acuse de recibo de la recepción del mensaje SCI y no necesariamente una respuesta en el ámbito de la aplicación.

El mensaje Indicación de control de servicio también puede utilizarse para abrir una nueva sesión o para cerrar la sesión.

Si una entidad distinta del controlador de acceso local desea abrir una sesión de control de servicio no relacionado con la llamada hacia un punto extremo, puede hacerlo abriendo una conexión de señalización independiente de la llamada hacia el punto extremo, y enviando un mensaje Establecimiento con una estructura **ServiceControlSession** incluyendo un URL. El parámetro **conferenceGoal** deberá fijarse a **callIndependentSupplementaryService** y el elemento de información de capacidad portadora del mensaje Establecimiento deberá fijarse tal como se define para una conexión independiente de la llamada en 7.2.2.1.2/H.225.0. De otro modo, se aplican los mismos procedimientos que en K.2.2 con la estructura **ServiceControlSession** transportada en mensajes de señalización de llamada, sin presencia de medios en la conexión.

K.2.3 Control de servicio relacionado con la llamada

Existen dos métodos para abrir sesiones de control de servicio relacionadas con una llamada en particular:

1) La sesión de control de servicio se abre entre un punto extremo y su controlador de acceso con un URL incluida en un mensaje RAS relacionado con la llamada, especialmente en el caso de controladores de acceso que utilizan llamadas con encaminamiento directo. Si se utiliza el mensaje SCI, el campo **callSpecific** del mismo contendrá el **callIdentifier** (**identificador de llamada**), el **conferenceId** (**identificador de conferencia**) y el campo **answerCall** (**llamada de respuesta**) tal como han sido utilizados en la señalización previa de esta llamada. Se utilizará un nuevo **sessionId**. Tal como en el caso de K.2.2, esta sesión no debería afectar a la sesión de control de servicio no relacionada con la llamada.

2) Las sesiones de control de servicio se abren entre un punto extremo y un controlador de acceso, o entre dos puntos extremos cuyo campo **ServiceControlSession** contiene un URL en los mensajes de señalización de llamada.

Si un proveedor de servicio debe notificar a un punto extremo sobre nuevos servicios o eventos de una sesión ya existente, puede hacerlo mediante datos de refresco de un URL que haya sido cargada previamente (por ejemplo, diálogos de aplicativo/servlet) o puede emitir un mensaje H.225.0 (Facilidad o SCI) con uno nuevo URL, cuyo motivo sea "**refresh**" y que tenga el mismo **sessionId** al anteriormente especificado para la sesión. El punto extremo que reciba dicho mensaje Facilidad debería cargar dicho URL y hacer una representación de los datos que le son presentados sobre el mismo recurso (por ejemplo, una ventana en pantalla), tal como se utilizó en primera instancia para esta sesión.

Si una entidad proveedora de servicios desea iniciar una nueva sesión después de que la llamada haya sido conectada, puede utilizar también el mensaje Facilidad/SCI con una **ServiceControlSession** que incluya un nuevo **sessionId**, el URL de interés y cuyo motivo sea "**open**". Los mensajes H.225.0 que no incluyan **ServiceControlSession** no influyen en la sesión HTTP, excepto el mensaje Liberación Completa, que sin un URL indica que se han terminado todas las sesiones para la llamada en cuestión. Esta señalización debe contemplarse de forma separada para cada una de las sesiones abiertas (no relacionadas con la llamada, relacionadas con la llamada y con mensajes SCI y de señalización durante la llamada).

Los controladores de acceso que utilizan el control de servicio HTTP deben tener especial cuidado de no interactuar con el control de servicio extremo a extremo. Éste es en concreto el caso de las llamadas no encaminadas por un controlador de acceso, en las que los controladores de acceso desconocen los mensajes y estados del control de la llamada. Para aliviar este problema, se recomienda que los puntos extremos utilicen distintas ventanas de visualización para cada una de las sesiones de control de servicio. Los dispositivos intermedios tales como controladores de acceso o MCU que apliquen este anexo, deben ser conscientes de la posibilidad de que se produzcan conflictos con otras entidades que proporcionen servicios en el trayecto de señalización de la llamada. Los mensajes (de señalización de llamada u otros, por ejemplo, un LCF con datos de control de servicio que pueden ser enviados al cliente en un ACF) pueden llegar al cliente con un **ServiceControlSession** que utilice el mismo **sessionId** que el anteriormente utilizado entre el proveedor intermedio y el cliente del servicio. Si el dispositivo intermedio decide pasar **ServiceControlSession**, debe poder establecer una relación entre el **sessionId** y un número singular para el cliente. Otra posibilidad es multiplexar estas dos sesiones en el mismo protocolo de nivel de presentación.

Para proporcionar servicios relacionados con la llamada entre zonas o dominios diferentes, una entidad de terminación puede devolver una estructura **ServiceControlSession** que contenga un URL en mensajes ajenos al canal de señalización de la llamada (por ejemplo, LCF/LRJ). El reenvío hacia el cliente de la estructura **ServiceControlSession** recibida en los mensajes correspondientes (por ejemplo, ACF/ARJ) depende del controlador de acceso local. Las aplicaciones que necesiten

información detallada sobre el estado de la llamada, la posibilidad de llevar a cabo acciones en el plano de control de la llamada o la posibilidad de actualizar la sesión posteriormente no deberán emplear este mecanismo, sino utilizar más bien el canal de señalización de llamada para transportar la estructura **ServiceControlSession**.

K.3 Utilización del HTTP

K.3.1 Canal de control de servicios no relacionado con la llamada

El protocolo HTTP se define en RFC 2068. En esta cláusula se hace una indicación de carácter informativo sobre cómo podría utilizarse el protocolo HTTP para proporcionar el protocolo de control de servicio descrito.

Para servicios no relacionados con la llamada, al punto extremo se facilita un URL que puede recuperar mediante el método GET (OBTENER) normalizado. Los datos se recopilan y se presentan conforme a los procedimientos normales de un agente-usuario[2] HTTP. El ejemplo siguiente (figura K.2) ilustra el flujo:

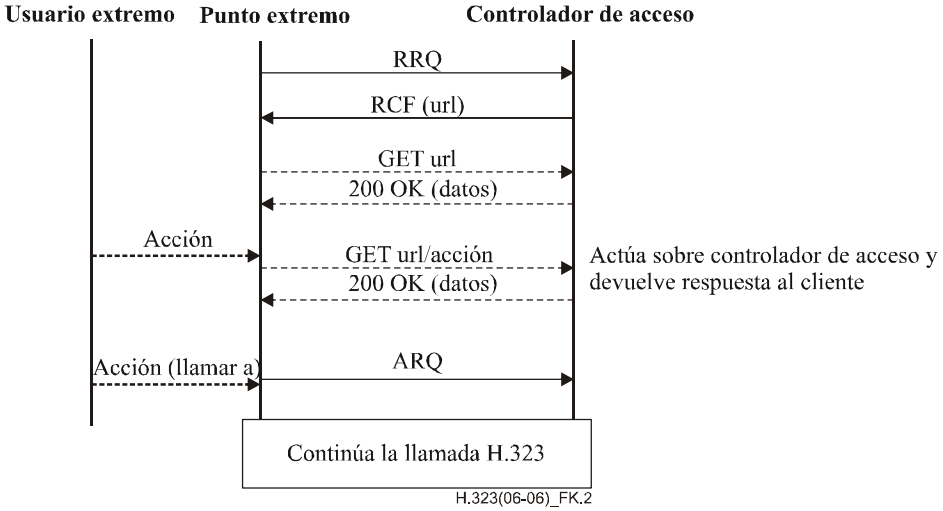


Figura K.2/H.323 – Ejemplo de control de servicio no relacionado con la llamada

K.3.2 Canal de control de servicios relacionado con la llamada

A fin de soportar el control de servicios relacionado con la llamada, se transporta un URL en los distintos mensajes H.225.0, tal como en K.2.3. Cuando un punto extremo que soporte este anexo reciba dicho URL, debe solicitar un usuario-agente HTTP normalizado para abrir y representar dicho URL.

El usuario-agente HTTP debería representar el URL dado y soportar hojas de estilo, guiones e imágenes conforme a lo definido para HTTP en RFC 2068. Las acciones definidas y realizadas por el contenido de este URL se podrían ejecutar localmente (por ejemplo, mediante enlaces "enviar correo electrónico a") o de forma distante en cualquier servidor HTTP con el que se disponga de un enlace, por ejemplo, que esté implementado o que esté relacionado con un punto extremo o un controlador de acceso. A continuación (véase la figura K.3) se presenta un ejemplo en el que el punto extremo es un proveedor de servicio, mientras que en el ejemplo 2 de la figura K.4 el proveedor de servicio es el controlador de acceso.

---

[2] El término "agente de usuario HTTP" utilizado en este anexo hace referencia a un proceso que implementa la parte cliente del protocolo HTTP (normalmente representado por un navegador web).

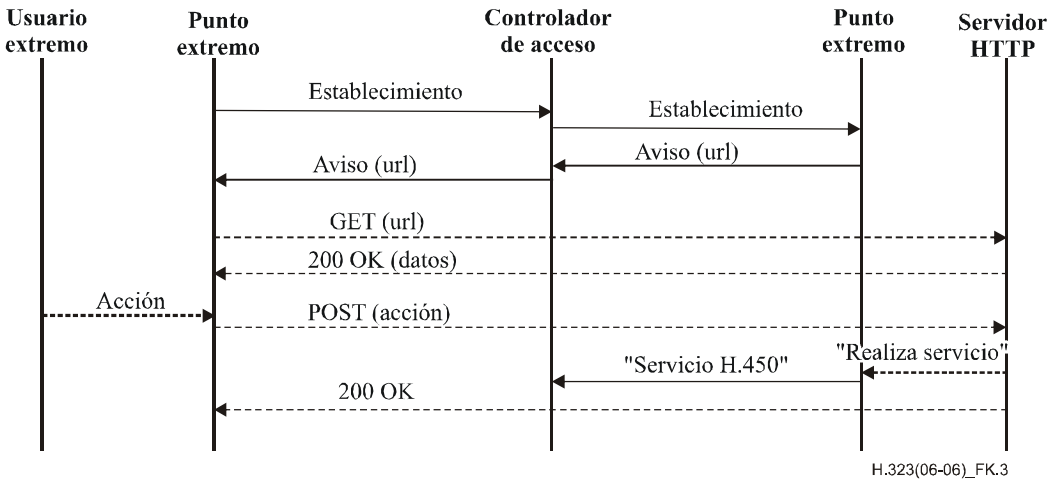


Figura K.3/H.323 – Ejemplo de control de servicio relacionado con la llamada utilizando un URL en los mensajes de señalización de llamada H.225.0

1) El cliente envía un mensaje Establecimiento encaminado a través del controlador de acceso al punto extremo que representa a la parte llamada.

2) La parte llamada se puede encontrar en un estado en el que está programado el procesamiento específico de la llamada que, por ejemplo:

   – Decide rechazar la llamada enviando un mensaje Liberación Completa. Dicho mensaje puede contener un URL que puede ser visualizada por un agente-usuario HTTP en la parte llamante. el URL podría, por ejemplo, ser una referencia a la página originaria de la parte llamada.

   – Decide devolver una lista de opciones relativas al establecimiento de la comunicación. En este caso devuelve un mensaje aviso con un URL que define las opciones dadas a la parte llamante, por ejemplo, desvío de llamada a operador, a secretaria, a buzón de voz, a correo electrónico o intrusión de sesión de llamada en curso.

3) El punto extremo H.323 parte llamante solicita a un usuario-agente HTTP que abra el URL, siendo representados los datos en la interfaz web de la parte llamante. El usuario extremo puede minimizar la ventana de visualización o interaccionar con ella seleccionando un enlace o una acción.

4) Las actuaciones definidas y realizadas en función del contenido de este URL pueden ejecutarse localmente (por ejemplo, mediante enlaces "enviar correo electrónico a") o a distancia en un servidor HTTP con el que se disponga de un enlace, por ejemplo, siendo implementado o estando relacionado con el punto extremo o el controlador de acceso. El punto extremo distante o el controlador de acceso deben analizar la actuación elegida y ejecutarla mediante servicios H.323/H.450 normalizados. El resultado puede ser, por ejemplo, el desvío de la llamada a un servidor de buzones de voz.

K.4 Ejemplos de escenarios

Los ejemplos siguientes sirven para ilustrar la utilización del control de la apertura de servicio:

– un ejemplo sencillo de la utilización de control de servicio no relacionado con la llamada;

– un ejemplo de control de servicio relacionado con la llamada para llamadas encaminadas a través del controlador de acceso;

– ejemplo de control de servicio relacionado con la llamada para llamadas no encaminadas a través del controlador de acceso;

– ejemplo de control de servicio no relacionado con la llamada para la carga de guiones.

En todos los ejemplos sólo se utiliza simultáneamente un canal de control de servicio. Por simplicidad, los mensajes que contienen una estructura **ServiceControlSession** se identifican exclusivamente con la "url".

Ejemplo 1: Control de servicio no relacionado con la llamada

Este ejemplo ilustra las señales de control cuando un usuario se registra ante un controlador de acceso, recibe entonces como respuesta un URL que hace referencia una agenda de números telefónicos, actualiza dicha agenda con los contactos de amigos (alias) y utiliza la agenda actualizada para realizar una llamada (no necesariamente a los mismos amigos) seleccionando una entrada con un URL H.323. Véase la figura K.4.

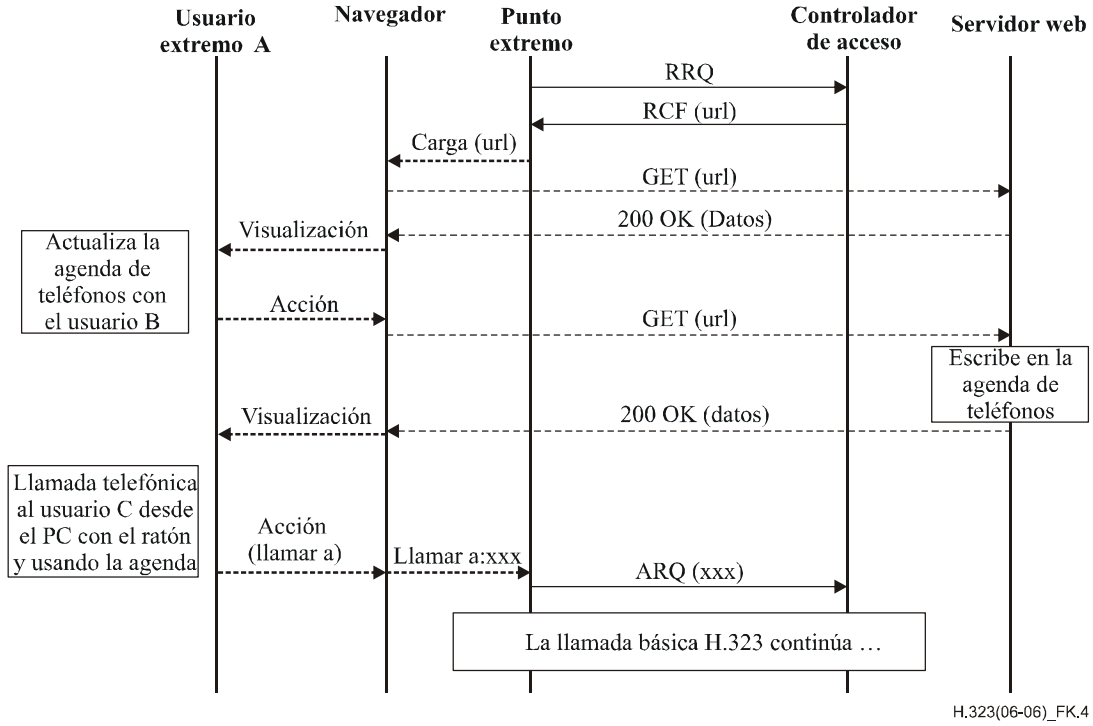


Figura K.4/H.323 – Control de servicio no relacionado con la llamada

Ejemplo 2: Control de servicio relacionado con la llamada, llamada encaminada por el controlador de acceso

Este ejemplo ilustra una variación del "servicio de llamada en espera", con algunas opciones para la parte llamante. El controlador de acceso detecta que la parte llamada está ocupada y proporciona un URL a la parte llamante con un mensaje Aviso (para evitar una temporización en el punto extremo llamante). El URL hace referencia a una página web que contiene un conjunto de opciones para el procesamiento subsiguiente de la llamada.

El usuario escucha un aviso de audio y se le presenta una página web con opciones. Las opciones pueden ser desvío a correo vocal, a correo electrónico u operador. El usuario selecciona el correo vocal y señaliza esta elección al servidor HTTP, que informa de ello al controlador de acceso.

El controlador de acceso realiza la petición de desvío como un reenvío de llamada en ausencia de respuesta (puesto que se ha enviado un aviso) e informa al servidor HTTP del éxito del desvío. El servidor HTTP responde entonces al navegador con una nueva página que, por ejemplo, informa que el desvío se ha realizado con éxito y en la que se le presenta nuevas opciones. Véase la figura K.5.

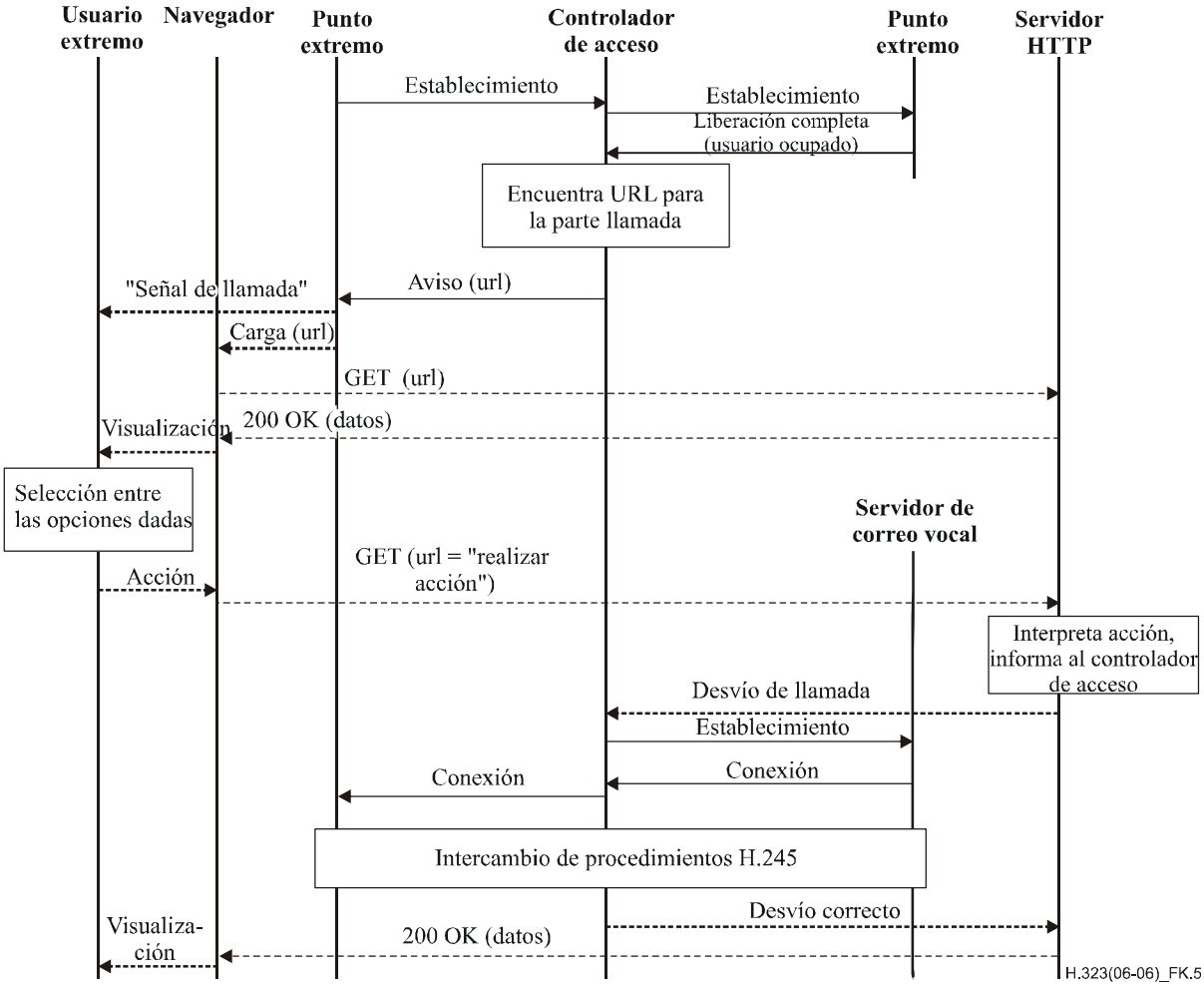


Figura K.5/H.323 – Control de servicio relacionado con la llamada, llamada encaminada por el controlador de acceso

Ejemplo 3: Control de servicio relacionado con la llamada, llamada no encaminada por el controlador de acceso

Este ejemplo ilustra el mismo servicio que el ejemplo 2, pero ejecutado en el punto extremo. El punto extremo llamado está ocupado en una llamada y devuelve un URL a la parte llamante con un mensaje Aviso (para evitar una temporización en el punto extremo llamante). El URL hace referencia a una página web que contiene un conjunto de opciones para el procesamiento subsiguiente de la llamada.

El usuario escucha el aviso de audio y se le presenta una página web con opciones. Las opciones pueden ser desvío a correo vocal, a correo electrónico u operador. El usuario selecciona el correo vocal y señaliza esta elección al servidor HTTP, que informa de ello al punto extremo.

El punto extremo realiza la petición de desvío como un reenvío de llamada en ausencia de respuesta (puesto que se ha enviado un aviso) e informa al servidor HTTP del éxito del desvío. El servidor HTTP responde entonces al navegador con una nueva página que, por ejemplo, informa que el desvío se ha realizado con éxito y en la que le presenta nuevas opciones. Véase la figura K.6.

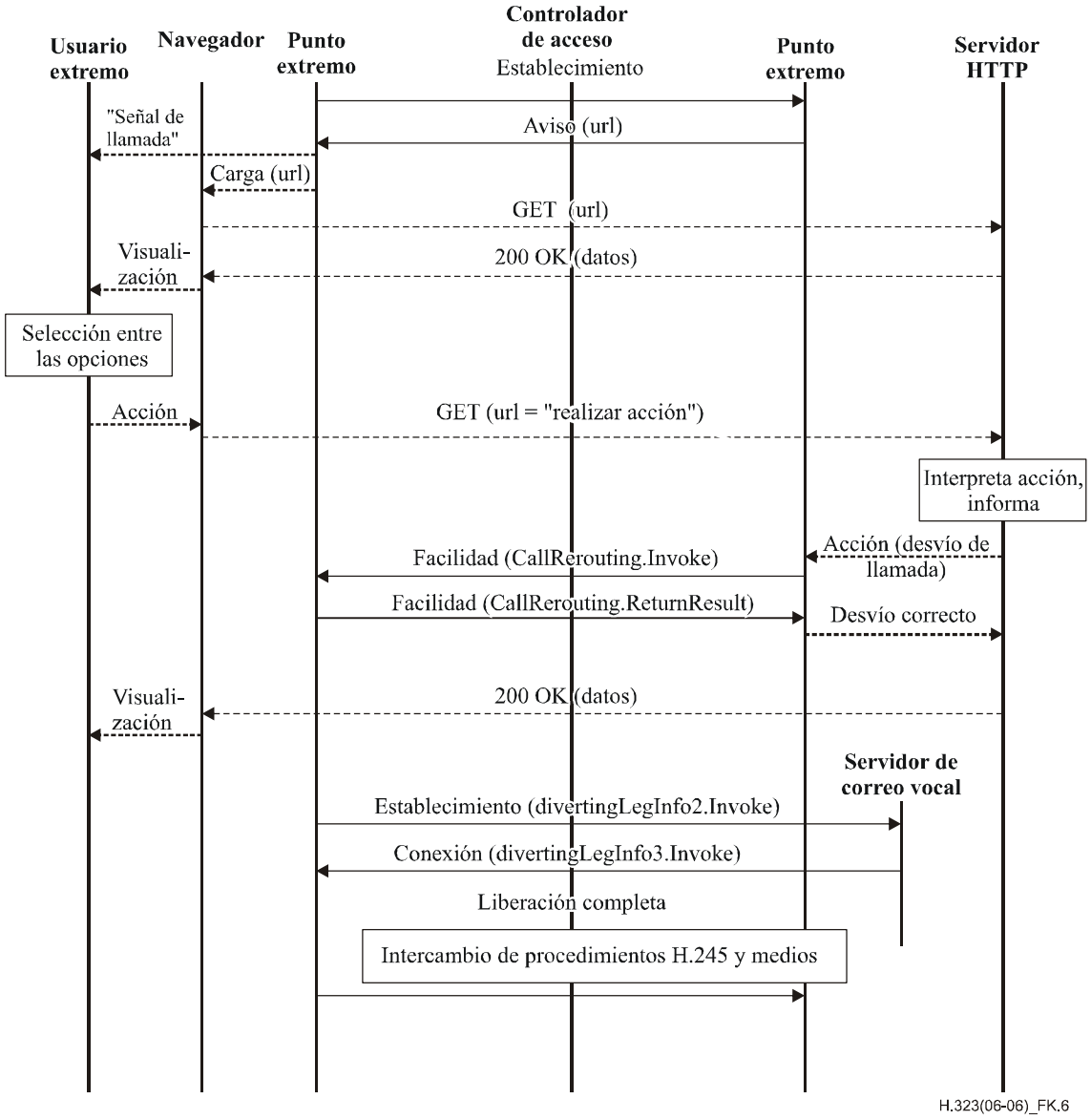


Figura K.6/H.323 – Control de servicio relacionado con la llamada, llamada no encaminada por el controlador de acceso

Ejemplo 4: Control de servicio no relacionado con la llamada, carga de guión

Los guiones de procesamiento de llamada son también una forma de control de servicio. En el ejemplo se muestra un terminal que carga un guión después del registro. El usuario prepara el guión mediante un dispositivo de construcción de gráficos en el punto extremo o por otros medios y decide cargarlo en el servidor.

En este caso, el punto extremo conoce, en el momento en que el usuario decide cargar el guión, que debe utilizar el esquema POST. La información detallada del guión y su impacto en la señalización de llamada subsiguiente depende del guión. Véase la figura K.7.

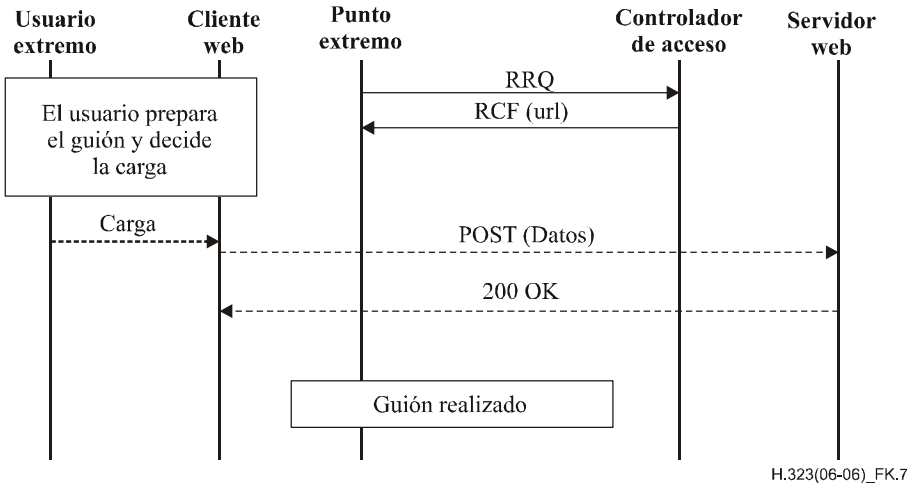


Figura K.7/H.323 – Control de servicio no relacionado con la llamada, carga de guión

K.5 Referencias

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

K.5.1 Referencias normativas

[H2250] Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicaciones multimedia por paquetes*.

[URL] BERNERS-LEE (T.) *et al.*: Uniform Resource Locators (URL), *RFC 1738, Internet Engineering Task Force*, diciembre de 1994.

[HTTP] FIELDING (R.) *et al.*: Hypertext Transfer Protocol – HTTP/1.1, *RFC 2068, Internet Engineering Task Force*, enero de 1997.

K.5.2 Referencias informativas

[S-HTTP] RESCORLA (E.) *et al.*: The Secure HyperText Transfer Protocol, *RFC 2660, Internet Engineering Task Force*, agosto de 1999.

[HTML] BERNERS-LEE (T.): Hypertext Markup Language – 2.0, *RFC 1866, Internet Engineering Task Force*, noviembre de 1995.

[MIME] FREED (N.), BORENSTEIN (N.): Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, *RFC 2045, Innosoft, First Virtual*, noviembre de 1996.

Anexo L

Protocolo de control de estímulo

L.1 Alcance

En este anexo se describen los procedimientos de señalización de estímulos entre terminales H.323 y una entidad funcional servidor de características. Este método de estímulo permite al proveedor del servicio de red implementar nuevos servicios suplementarios para los terminales sin efectuar cambios en el soporte lógico del terminal, lo cual hace el mantenimiento más sencillo. Un ejemplo de estos terminales es un teléfono de características conectado a la LAN. Un servidor de características puede estar colocalizado con el controlador de acceso.

El protocolo estímulo H.323 permite la prestación de servicios por uno o más servidores de características. Para la interoperabilidad, se utiliza la señalización H.225.0 estándar para el control de llamada básica, y todas las manipulaciones de los trenes de medios se efectúan utilizando procedimientos estándar H.245 o de conexión rápida. Se utilizan mecanismos basados en la Rec. UIT-T H.248.1 para manipular las terminaciones físicas tales como el altavoz o el microteléfono.

El protocolo descrito en este anexo puede dar soporte al modelo de señalización directo y al modelo de señalización a través del controlador de acceso.

Las configuraciones típicas ilustradas en las figuras L.1 y L.2 muestran las entidades de señalización funcionales que pueden intervenir en una llamada desde un terminal estímulo H.323 hasta otro punto extremo en una zona H.323 distinta. La figura L.1 muestra el servidor de características actuando como un mandatario de señalización para el terminal del anexo L. La figura L.2 muestra el servidor de características colocalizado con el controlador de acceso del terminal del anexo L. En ambos casos, el servidor de características tiene acceso a la señalización H.323, la cual le proporciona información de estado de la llamada que puede ser útil para determinados servicios, así como para habilitar el servidor de características para afectar a los trenes de medios utilizando la señalización H.245 o de conexión rápida.

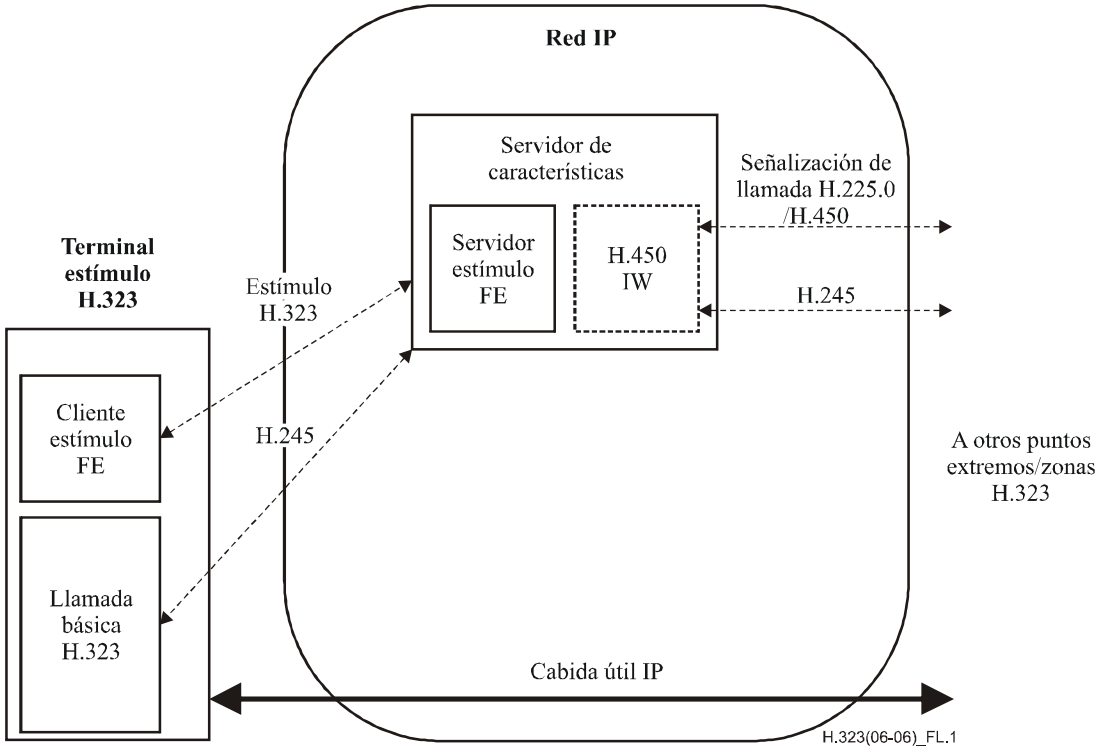


Figura L.1/H.323 – Ejemplo de anexo L junto con el modelo de señalización directa

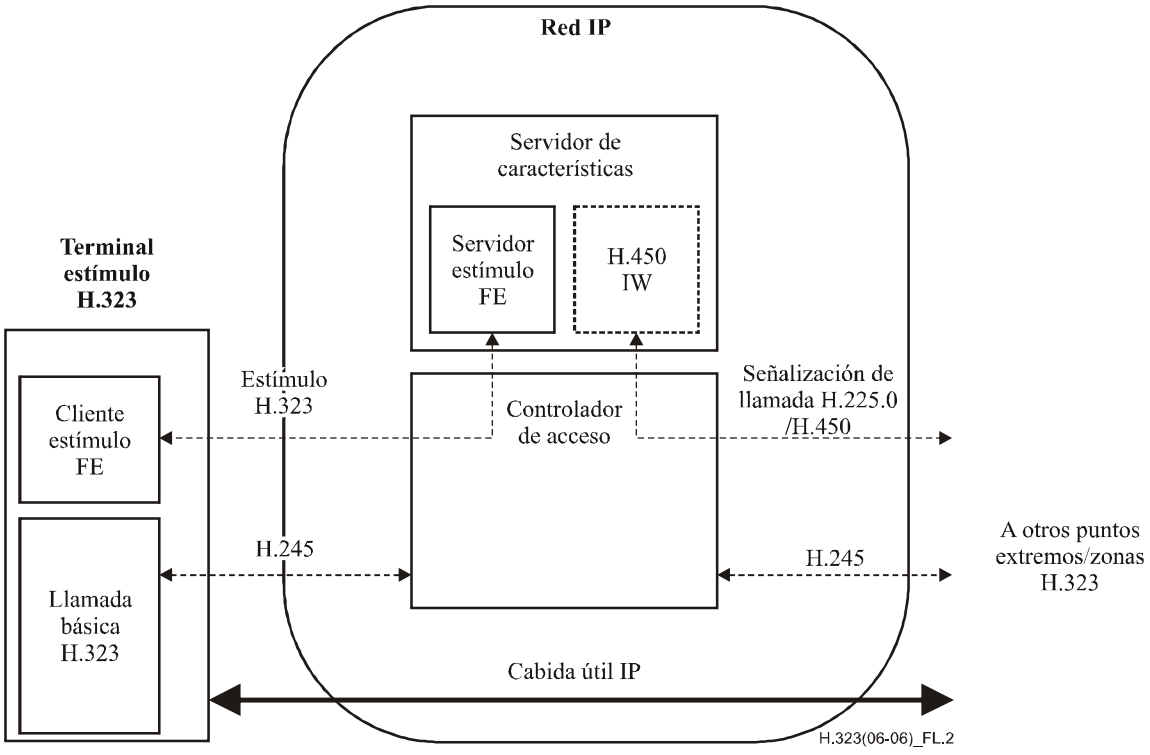


Figura L.2/H.323 – Ejemplo de anexo L junto con el modelo de señalización a través del controlador de acceso

L.1.1 Terminología

L.1.1.1 servidor de características: Entidad funcional que utiliza el método descrito en este anexo para proporcionar características a un punto extremo del anexo L. Un servidor de características puede residir en cualquier parte de la red: puede estar colocalizado con un controlador de acceso, o residir en una pasarela u otra entidad llamable H.323. Un servidor de características puede proporcionar interfuncionamiento entre el protocolo estímulo y los servicios H.450.

L.1.1.2 punto extremo del anexo L: Entidad llamable H.323 que puede ser controlada mediante el método descrito en este anexo.

L.1.1.3 característica: Transacción que puede afectar la interfaz de usuario y alterar la transmisión continua de medios.

L.1.2 Relación del estímulo H.323 con H.248

Dado que H.248 se elaboró para el control de las pasarelas de medios, supone una estrecha relación entre el controlador y la pasarela de medios. Pueden ser incluidos puntos extremos por ejemplo, teléfonos y pasarelas residenciales, como dispositivos controlados y tratarlos como pasarelas de medios de una sola línea. No obstante, están vinculadas a un solo controlador, que proporciona todos los controles de conexión, las características y los servicios a los puntos extremos H.248. Un usuario puede abonarse a las características de un controlador a la vez.

El presente anexo adopta el modelo controlador/punto extremo de H.248 para el control de los servicios suplementarios estímulos, de manera que estos procedimientos necesitan ser definidos una sola vez. Este anexo excluye explícitamente todas las partes de H.248 que están relacionadas con el control de las conexiones de medios, lo que se lleva a cabo utilizando procedimientos estándar H.245 o de conexión rápida.

L.1.3 Relación del estímulo H.323 con HTTP

El anexo K permite el control por terceros de una llamada H.323 basada en una conexión hipertexto separada (con HTTP) para la interacción de usuario. No hay un conjunto fijo de capacidades para la interfaz de usuario, dado que se utilizarán dinámicamente diversos tipos de formato de texto, imágenes y sonidos. El proveedor de servicio (servidor HTTP) es el responsable de establecer la correspondencia entre los eventos HTTP y las acciones de control de llamada (H.450 u otros mensajes) para los servicios suplementarios, de tal forma que el punto extremo H.323 desconoce la aplicación HTTP. El proveedor de servicio puede estar asociado con el controlador de acceso local, con el punto extremo distante, o con el controlador de acceso distante en una llamada H.323.

L.1.4 Relación con los servicios suplementarios H.450

Como el terminal estímulo no realiza servicios suplementarios H.450, el servidor de características o el controlador de acceso se encargan de efectuar una función intermediaria para tratar, en nombre del terminal, los procedimientos H.450 a través de la red.

En este caso, el servidor de características pasa a ser un punto extremo para todas las operaciones H.450 e implementa todos los servicios suplementarios y las máquinas de estado que intervienen. La interacción con el usuario se produce a través de la interfaz de usuario telefónica, que el controlador de acceso puede controlar a través de la señalización estímulo H.323.

L.2 Introducción

El requisito esencial de un protocolo estímulo H.323 es proporcionar un conjunto de capacidades para que un conjunto potencialmente ilimitado de servicios suplementarios pueda tener acceso a puntos extremos. Un protocolo semejante tiene muchas ventajas, por ejemplo, los puntos extremos pueden mantener un peso relativamente ligero y ofrecer un cierto grado de aislamiento con respecto a los efectos ocasionados por la introducción de una nueva característica. En general, estos servicios están controlados por un controlador de acceso, un intermediario u otra entidad de la red. En este

anexo se utiliza el término "servidor de características" para designar genéricamente cualquier entidad de la red que proporciona la configuración o el control estímulo de puntos extremos, según el protocolo descrito.

El protocolo descrito en este anexo tiene las siguientes finalidades:

- dar soporte a servicios suplementarios arbitrarios (estándar y no estándar);
- interfuncionamiento de estos servicios entre el servidor de características y el punto extremo;
- compatibilidad hacia atrás con puntos extremos utilizando H.323 (segunda versión o versiones posteriores).

Este protocolo alcanza dichas finalidades mediante la incorporación de porciones considerables del protocolo descrito en la Rec. UIT-T H.248.1. En dicha Recomendación se describe un modelo estímulo puro de control de punto extremo, mientras que este anexo debe ser necesariamente un híbrido de modelo estímulo y de modelos funcionales H.323. Las entidades del anexo L utilizan las PDU H.248 además de mensajes H.323 estándar para dar soporte a este modelo híbrido.

En este anexo se describe un marco que facilita la prestación de servicios en los sistemas básicos H.323 y H.248 permitiendo un alto grado de uniformidad entre un servidor de características de este anexo y los componentes de un controlador de pasarelas de medios (MGC, *media gateway controller*) H.248 no relacionado con el control de medios. Este marco permite la reutilización de lotes H.248 en sistemas H.323, a menudo con poca o ninguna modificación. Por ejemplo, los lotes diseñados convenientemente pueden permitir que un servidor de características controle diversos elementos de interfaz de usuario de un terminal apto, como por ejemplo:

- escribir en pantalla;
- proporcionar indicaciones independientes del equipo al punto extremo, a partir de las cuales el punto extremo puede controlar sus propios indicadores, como las indicaciones de llamada o de mensaje en espera;
- recibir entradas de usuario, como cifras, textos, teclas especiales (por ejemplo, teclas de función y conmutación);
- asignar funciones a las teclas programables y en los directorios situados en el punto extremo;
- solicitar aplicación de tonos específicos;
- especificar tonos dinámicamente.

Los terminales de este anexo L y los terminales H.248 poseen en común las capacidades de control enumeradas supra; la única diferencia de ambos tipos de capacidades es la forma de tratar los trenes de medios y su asociación con una o más llamadas o "contextos".

Se sugiere la utilización del protocolo descrito en este anexo para los tipos de puntos extremos simples del anexo F, aunque no se limite a los mismos.

L.3 Marco estímulo

L.3.1 Panorama general

Los terminales de este anexo L utilizan los mecanismos H.323 estándar para el registro y el establecimiento del canal de señalización. La señalización de llamada H.225.0 normal se utiliza para el establecimiento y terminación de llamada. El control de medios puede utilizar los procedimientos de conexión rápida H.323 (comprendido el elemento fastStart repetido) u, opcionalmente, los procedimientos con señalización H.245 descritos en las Recs. UIT-T H.245, H.323 y sus anexos. El resultado del uso de estos mecanismos podría ser la

creación de elementos análogos a las terminaciones efímeras H.248 (que no son directamente controlables utilizando este anexo).

Las capacidades de señalización estímulo de los puntos extremos de este anexo L se especificarán en lotes, como en H.248. Por ejemplo, la descripción de un terminal del anexo L podría efectuarse mediante un lote de conjuntos básico (para cambios del dispositivo conmutador, etc.), un lote teclado, un lote alerta, un lote tecla y un lote visualización. Podrán incluirse nuevos lotes a fin de poder modificar parámetros operacionales y/o recopilar estadísticas sobre calidad de funcionamiento.

Como los terminales del anexo L son principalmente puntos extremos H.323, siempre se aplicarán los procedimientos H.323, que no podrán ser incapacitados por ninguna señalización H.248. Por ejemplo, si una instrucción H.248 produce la terminación de una llamada, se sigue necesitando señalización estándar H.245 y H.225.0 para la terminación de la llamada.

L.3.2 Señalización del protocolo

La única forma de señalización a la que deben dar soporte todas las entidades H.323 es la señalización de llamada H.225.0. Se trata del transporte más adecuado para el protocolo estímulo ya que permite que un servidor de características esté colocalizado con un controlador de acceso o cualquier otro tipo extremo H.323.

Las entidades del anexo L deben soportar la encapsulación de los mensajes H.248 en el campo **StimulusControl**, que está disponible en todos los mensajes de señalización de llamada H.225.0. En cada llamada en la que participen estos mensajes, un punto extremo del anexo L que soporte encapsulación H.248 incluirá un campo **StimulusControl** en el primer mensaje de señalización de llamada H.225.0 que envíe hacia cualquier otra entidad H.323 (el campo **StimulusControl** puede estar vacío).

Cuando se registra un punto extremo con un controlador de acceso, éste puede indicar un alias para el servidor de características en el campo **featureServerAlias** de la RCF. Cuando este alias está presente, debe ser utilizado por un punto extremo del anexo L como el destino servidor para señalización H.248 sin tunelización, que está constreñido a la funcionalidad definida en este anexo. Gracias a esta dirección de alias el controlador de acceso puede asociar o encaminar la llamada al servidor de características. Al recibirse un campo **featureServerAlias** válido en una RCF, un punto extremo soporte debe enviar inmediatamente una instrucción **ServiceChange** H.248 que contenga el TerminationId raíz para la dirección indicada del servidor de características.

Esto permite dos modelos de interacción entre un servidor de características y un punto extremo del anexo L:

- el servidor de características está presente en el trayecto de señalización de llamada para todos los mensajes de señalización de llamada H.225.0 de todas las llamadas que se originan y terminan en un punto extremo del anexo L;
- se establece una conexión de señalización de llamada separada entre el punto extremo del anexo L y el servidor de características únicamente cuando se invoca una característica.

L.3.3 Utilización de H.248

Los puntos extremo del anexo L soportarán los procedimientos del nivel de transacción descritos en 7.2/H.248.1. La señalización del anexo L puede incluir cualquiera de los comandos definidos en la cláusula 7/H.248.1.

Debido a que las terminales del anexo L no utilizan H.248 para el control de medios, el uso de los siguientes descriptores H.248 no se aplica a las entidades del anexo L: ModemDescriptor, MuxDescriptor, StreamDescriptor, LocalControl Descriptor, Local Descriptor, Remote Descriptor y TopologyDescriptor. Estos descriptores no serán utilizados para la señalización del anexo L y serán ignorados si se reciben. Obsérvese que este anexo no puede ser utilizado para direccionar

explícitamente distintos trenes de medios; si un terminal del anexo L soporta múltiples trenes de medios (por ejemplo, audio y vídeo), se asume implícitamente la asignación de una terminación al contexto de la llamada (0xFFFFFFFD, véase L.3.4 más adelante) para referirse al tren que transporta el medio apropiado.

Los lotes soportados por el punto extremo deben indicarse en el campo **supportedH248Packages** del RRQ cuando el punto extremo se registra en un controlador de acceso. Si está presente este campo, pero vacío, un servidor de características puede utilizar una interrogación AuditCapabilities para determinar los lotes soportados.

L.3.4 Encapsulación H.225.0

Toda la señalización H.225.0 encapsulada relativa a este anexo L utiliza una estructura **StimulusControl**. En esta cláusula se describe la utilización de sus campos. La utilización del anexo L por un punto extremo se deduce a partir de la presencia de esta estructura en el primer mensaje de señalización de llamada enviado por el punto extremo al servidor de características. Si no se encapsula ningún mensaje H.248 en esta estructura, pueden omitirse todos sus campos opcionales contenidos en dicho mensaje.

El control estímulo encapsulado del anexo L se señalizará utilizando el campo **stimulusControl** en el elemento H.323-UU-PDU empleado para la señalización de llamada en H.323.

El mensaje H.248 a enviar será encapsulado en el campo **h248Message** en la secuencia **stimulusControl**. El mensaje encapsulado es del tipo datos MegacoMessage definido en la Rec. UIT-T H.248.1.

Cuando el servidor de características del anexo L se activa en el contexto de una llamada existente, puede necesitar la determinación del estado de esa llamada, y/o del punto extremo. Esto puede ser llevado a cabo con la utilización de la instrucción AuditValue H.248.

La asignación de TerminationId para las terminaciones físicas en el punto extremo puede ser aprovisionada en el servidor de características y en el punto extremo, predefinida en un lote, u obtenida a través de AuditCapabilities.

La señalización H.248 puede ser binaria (sintaxis del anexo A/H.248.1, aunque utilizando PER para la codificación) o textual (anexo B/H.248.1). La codificación por defecto es la codificación binaria. La presencia del campo **isText** indicará que se ha utilizado la codificación del anexo B/H.248.1 para los descriptores H.248 en la estructura **StimulusControl**. Los puntos extremos del anexo L pueden dar soporte únicamente a una forma de codificación, y utilizarán la misma forma de codificación para la señalización a un servidor de características en todo el anexo L. Los servidores de características del anexo L darán soporte a ambas formas de codificación; la comunicación de un servidor de características a un punto extremo utilizará únicamente la forma cuyo soporte ha indicado el punto extremo.

Para la señalización encapsulada H.225.0 relativa a todo el anexo L, se utilizará el valor especial "ANNEX-L", definido como 0xFFFFFFFD, como ContextId para todas las transacciones relacionadas con las llamadas. Todas las instrucciones se aplicarán a la llamada en curso H.323 (representada por el **callIdentifier** del mensaje de señalización de llamada H.225.0 que encapsula la instrucción H.248). Las instrucciones no relacionadas con la llamada representadas por el mensaje de encapsulación H.225.0 se asociarán con el valor ContextId NULL, como se define en la Rec. UIT-T H.248.1.

Las transacciones encapsuladas del anexo L no utilizarán valores ContextId diferentes de NULL (como se define en la Rec. UIT-T H.248.1) o ANNEX-L (como se definió antes).

Ciertas actividades H.248 no pueden ser asociadas con llamadas activas H.323. En este caso, puede utilizarse cualquier canal de señalización de llamada existente entre el punto extremo y el servidor de características, y se utilizarán los procedimientos de H.248 para asociar la actividad con los objetos H.248 correctos. Para esas actividades, pueden utilizarse procedimientos de señalización independientes H.323 de la llamada. Para la señalización independiente de la llamada, se utilizará el procedimiento de 7.2/H.450.1.

Para actividades H.248 que puedan estar asociadas con una llamada activa con el servidor deseado de características en el trayecto de señalización de llamada, puede utilizarse cualquier mensaje apropiado de señalización de llamada H.225.0 para la comunicación entre el servidor de características y el punto extremo.

L.4 Referencias

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

– Recomendación UIT-T H.248.1 (2005), *Protocolo de control de las pasarelas: Versión 3*.

– Recomendación UIT-T H.248.3 (2000), *Protocolo de control de las pasarelas: Elementos de interfaz de usuario y lotes de acciones*.

– Recomendación UIT-T H.450.1 (1998), *Protocolo funcional genérico para el soporte de servicios suplementarios en la Recomendación H.323*.

Anexo M1

Tunelización de protocolos de señalización (QSIG) en H.323

M1.1 Alcance

La finalidad de este anexo es dar orientación sobre cómo el mecanismo de tunelización genérico descrito en 10.4 puede utilizarse para tunelizar QSIG por redes H.323. Otros grupos tales como ISO/CEI son responsables finalmente de los propios procedimientos QSIG. En las referencias [M1-1] y [M1-2] indicadas a continuación puede verse información sobre los QSIG (también conocidos como PSS1).

M1.2 Referencias normativas

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

[M1-1] ISO/CEI 11572:2000, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Circuit mode bearer services – Inter-exchange signalling procedures and protocol.*

[M1-2] ISO/CEI 11582:2002, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Generic functional protocol for the support of supplementary services – Inter-exchange signalling procedures and protocol*.

[M1-3] Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes*.

M1.3 Procedimientos de punto extremo

Los puntos extremos que soportan la tunelización de información QSIG utilizarán los procedimientos de 10.4, con el siguiente IDENTIFICADOR DE OBJETO utilizado como TunnelledProtocol:

- **{iso (1) identified-organization (3) icd-ecma (0012) private-isdn-signalling-domain (9)}**

Los mensajes H.225.0 tunelizan el mensaje QSIG completo, sin modificación, empezando por el campo discriminador de protocolo y terminando por los otros elementos de información. El contenido binario de los mensajes QSIG se codifica como una CADENA DE OCTETOS en el **H323-UU-PDU.tunnelledSignallingMessage.messageContent**. Como la codificación binaria de los mensajes QSIG es lo que se tuneliza, se preserva completamente la integridad de los mensajes QSIG, incluida cualquier codificación BER de ASN.1 en los elementos de información indicador de facilidad o de notificación.

Los mensajes QSIG pueden, aunque no es necesario, ser tunelizados en los correspondientes mensajes H.225.0. Por ejemplo, el mensaje ESTABLECIMIENTO de QSIG puede ser tunelizado en un mensaje ESTABLECIMIENTO H.225.0, y el mensaje LIBERACIÓN COMPLETA de QSIG puede ser tunelizado en un mensaje LIBERACIÓN COMPLETA H.225.0. Para otros mensajes, es posible que no exista ningún mensaje de señalización de llamada H.225.0 correspondiente (por ejemplo, en el caso de un mensaje DESCONEXIÓN DE QSIG) o que el mensaje correspondiente no esté disponible porque ya haya sido enviado. En estos casos, el mensaje QSIG puede ser tunelizado en un mensaje FACILIDAD H.225.0. Un mensaje LLAMADA EN CURSO de QSIG deberá ser tunelizado en un mensaje FACILIDAD H.225.0 ya que el mensaje LLAMADA EN CURSO H.225.0 no tiene relevancia de extremo a extremo. Además, siendo como son facultativos los mensajes NOTIFICACIÓN y PROGRESO, no podrían ser entregados de extremo a extremo y deberán ser tunelizados en un mensaje FACILIDAD salvo que los tonos o anuncios sean suministrados por el lado llamado y no se haya enviado ningún indicador de progreso al lado llamante hasta el momento. En tal caso debe utilizarse un mensaje PROGRESO (con el descriptor de progreso #1 o #8) para tunelizar el mensaje PROGRESO DE QSIG. Los procedimientos de liberación de llamada QSIG pueden ser soportados tunelizando los mensajes DESCONEXIÓN y LIBERACIÓN de QSIG en el mensaje FACILIDAD H.225.0. En el caso especial de que un mensaje LIBERACIÓN de QSIG tunelizado se interprete como un mensaje LIBERACIÓN COMPLETA de QSIG tunelizado (lo que ocurre al recibir un mensaje LIBERACIÓN de QSIG cuando se esperaba LIBERACIÓN COMPLETA), la llamada H.323 puede ser liberada por el lado que recibe el mensaje LIBERACIÓN de QSIG enviando un mensaje LIBERACIÓN COMPLETA H.225.0 sin ningún mensaje QSIG tunelizado.

Una llamada QSIG puede tunelizarse en una llamada H.323. La relación entre las referencias de llamada QSIG y las referencias de llamada H.225.0 caen fuera del alcance de esta Recomendación.

El cuadro M1.1 es sólo indicativo e ilustra un ejemplo de la correspondencia entre mensajes QSIG y mensajes H.225.0.

Cuadro M1.1/H.323 – Correspondencia entre mensajes QSIG y mensajes H.225.0

Mensaje QSIG	Mensaje H.225.0
ESTABLECIMIENTO	ESTABLECIMIENTO
AVISO	AVISO
CONEXIÓN	CONEXIÓN
LIBERACIÓN COMPLETA	LIBERACIÓN COMPLETA
LLAMADA EN CURSO	FACILIDAD
FACILIDAD	
PROGRESO (nota)	
NOTIFICACIÓN	
DESCONEXIÓN	
LIBERACIÓN	
Demás mensajes …	
NOTA – Si los tonos o anuncios son suministrados por el lado llamado, este mensaje debe tunelizarse en un mensaje PROGRESO en vez de en uno FACILIDAD.	

M1.4 Tunelización de la señalización independiente de la llamada orientada a la conexión QSIG

Para conexiones de señalización independientes de la llamada QSIG, no se requiere ningún canal de control H.245 ni canales de medios.

Los procedimientos de señalización de llamada de H.225.0 pueden utilizarse para establecer una conexión de señalización independiente de la llamada entre dos puntos extremos pares, como se describe en 10.4.

M1.5 Procedimientos de controlador de acceso

Un controlador de acceso que participa en una llamada en la que se utiliza tunelización QSIG entre dos puntos extremos debe pasar mensajes QSIG tunelizados a menos que pretenda terminar el túnel. Puede ser éste el caso cuando un controlador de acceso está ofreciendo servicios QSIG emulados.

Anexo M2

Tunelización de los protocolos de señalización (PU-RDSI) en H.323

M2.1 Alcance

El objetivo de este anexo es proporcionar directrices sobre cómo pueden utilizarse los mecanismos de tunelización genéricos descritos en 10.4 para la tunelización de la parte de usuario de la RDSI (PU-RDSI) sobre redes H.323. El UIT-T es, en última instancia, responsable de los procedimientos de la RDSI. En las referencias [M2-1] y [M2-2] identificadas más abajo puede encontrarse información sobre la PU-RDSI.

M2.2 Referencias normativas

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

[M2-1] Recomendación UIT-T Q.763 (1999), *Sistema de señalización N.º 7 – Formatos y códigos de la parte de usuario de la RDSI*.

[M2-2] Recomendación UIT-T Q.764 (1999), *Sistema de señalización N.º 7 – Procedimientos de señalización de la parte de usuario de la RDSI*.

[M2-3] Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes*.

M2.3 Procedimientos del punto extremo

Los puntos extremos que soportan la tunelización de la información de la PU-RDSI utilizarán los procedimientos descritos en 10.4. El punto extremo identificará la variante de PU-RDSI utilizando el **tunnelledProtocolObjectID** (**identificador de objeto de protocolo tunelizado**) o la estructura **TunnelledProtocolAlternateIdentifier (identificador alternativo de protocolo tunelizado**). Se puede utilizar el **subIdentifier** (**subidentificador**) para identificar la revisión de la variante de PU-RDSI, por ejemplo, "1988". Véase el cuadro M2.1.

Cuadro M2.1/H.323 – Ejemplos de protocolos tunelizados identificados mediante el tunnelledProtocolObjectID

Norma	tunnelledProtocolObjectID	subIdentifier
Rec. UIT-T Q.763 (1988)	{itu-t (0) recommendation (0) q (17) 763}	"1988"
Rec. UIT-T Q.763 (1992)	{itu-t (0) recommendation (0) q (17) 763}	"1992"

Cuando se utilice la estructura **TunnelledProtocolAlternateIdentifier**, se fijará el **protocolType** (**tipo de protocolo**) a "isup". La **protocolVariant** (**variante de protocolo**) será una cadena que identifique la especificación de la PU-RDSI utilizada, por ejemplo, un número de documento. Véase el cuadro M2.2.

Cuadro M2.2/H.323 – Ejemplos de protocolos tunelizados identificados mediante el TunnelledProtocolAlternateIdentifier

Especificación de PU-RDSI (Nota)	protocolType	protocolVariant	subIdentifier
ANSI T1.113-1988	"isup"	"ANSI T1.113-1988"	"1988"
ETS 300 121	"isup"	"ETS 300 121"	"121"
ETS 300 356	"isup"	"ETS 300 356"	"356"
BELLCORE GR-317	"isup"	"BELLCORE GR-317"	"317"
JT-Q761-4 (1987-1992)	"isup"	"JT-Q761-4 (1987-1992)"	"87"
JT-Q761-4 (1993)	"isup"	"JT-Q761-4 (1993)"	"93"
NOTA – La especificación de la PU-RDSI puede ser una norma, una Recomendación o cualquier otro documento que especifique el protocolo PU-RDSI, por ejemplo, una especificación de interconexión de PU-RDSI para un país determinado.			

- **{ itu-t (0) recommendation (0) q (17) 763 }**

Los mensajes H.225.0 tunelizan el mensaje PU-RDSI completo, inalterado. Comenzando con el parámetro código de tipo de mensaje y terminando con los restantes parámetros. El contenido binario de los mensajes PU-RDSI se codifica como una CADENA DE OCTETOS en la **H323-UU-PDU**.**tunnelledSignallingMessage**.**messageContent**. Puesto que lo que se tuneliza en la codificación binaria de los mensajes PU-RDSI, se preserva íntegramente la integridad de los mensajes PU-RDSI.

Por ejemplo, el mensaje inicial de dirección (IAM, *initial address message*) de la PU-RDSI puede tunelizarse en un mensaje H.225.0 ESTABLECIMIENTO y el mensaje ANM de la PU-RDSI puede tunelizarse en un mensaje H.225.0 CONEXIÓN. Es posible que para otros mensajes no exista el correspondiente mensaje H.225.0 (por ejemplo, en el caso e un mensaje IDR de la PU-RDSI) o que el mensaje correspondiente no esté disponible por haber sido ya enviado. En tales casos, el mensaje PU-RDSI puede tunelizarse en un mensaje H.225.0 FACILIDAD.

Una llamada PU-RDSI puede tunelizarse en una llamada H.323.

Es posible que sea necesario que la red H.323 modifique algunos elementos de información del mensaje H.225.0 y que la pasarela que recibe el mensaje PU-RDSI tunelizado necesite invalidar los correspondientes parámetros PU-RDSI.

La bandera **tunnellingRequired** (**tunelización requerida**) se incluirá en el mensaje Establecimiento cuando el parámetro indicación de requerimiento de PU-RDSI del mensaje IAM indique "PU-RDSI requerida".

El cuadro M2.3 sólo tiene carácter indicativo e ilustra un ejemplo de la correspondencia establecida entre los mensajes PU-RDSI y los mensajes H.225.0.

Cuadro M2.3/H.323 – Correspondencia entre mensaje PU-RDSI y mensajes H.225.0

Mensaje PU-RDSI	Mensaje H.225.0
IAM	ESTABLECIMIENTO
SAM	INFORMACIÓN
CPG	LLAMADA EN CURSO, AVISO, PROGRESO, NOTIFICACIÓN o FACILIDAD
ACM	LLAMADA EN CURSO, AVISO, PROGRESO, NOTIFICACIÓN o FACILIDAD
ANM, CON	CONEXIÓN
REL	LIBERACIÓN COMPLETA
Todos los demás mensajes	FACILIDAD

M2.4 Procedimientos del controlador de acceso

Un controlador de acceso que participe en una llamada en la que se utiliza la tunelización PU-RDSI entre los puntos extremos debe dejar pasar los mensajes PU-RDSI tunelizados sin modificación salvo que pretenda terminar el túnel PU-RDSI. Este puede ser el caso cuando un controlador de acceso ofrece servicios PU-RDSI.

Un controlador de acceso no seleccionará un punto extremo que no soporte la PU-RDSI cuando en el mensaje Establecimiento se incluya la bandera **tunnellingRequired**.

Anexo M3

Tunelización de señalización digital de abonado N.º 1 a través de H.323

M3.1 Alcance

El objetivo de este anexo es proporcionar directrices sobre cómo se puede utilizar el mecanismo de tunelización genérico descrito en 10.4 para tunelizar DSS1 (Q.931) sobre redes H.323. Otros grupos pueden adaptar este procedimiento para acomodar las variantes nacionales de DSS1.

M3.2 Referencias normativas

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

[M3-1] Recomendación UIT-T Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de la llamada básica*.

[M3-2] Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes*.

[M3-3] Recomendación UIT-T H.450.1 (1998), *Protocolo funcional genérico para el soporte de servicios suplementarios en la Recomendación H.323*.

M3.3 Procedimientos de los puntos extremos

Los puntos extremos que soportan la tunelización de información DSS1, utilizarán los procedimientos descritos en 10.4, con el IDENTIFICADOR DE OBJETO siguiente utilizado como **TunnelledProtocol.id.tunnelledProtocolObjectID** en un mensaje H.225.0 de señalización de llamada o en el mensaje H.225.0 RAS:

- **{itu-t (0) recommendation (0) q (17) 931}**

  Los puntos extremos que soporten la tunelización de información DSS1 y que actúen como una entidad de usuario DSS1, utilizarán los procedimientos de 10.4, con el valor siguiente de **TunnelledProtocol.subIdentifier**:

- **"User"**

  Los puntos extremos que soporten la tunelización de información DSS1 y que actúen como una entidad de red DSS1, utilizarán los procedimientos de 10.4 con el valor siguiente de **TunnelledProtocol.subIdentifier**:

- **"Network"**

  Cuando se envíe un mensaje H.225.0 RAS solicitando un protocolo tunelizado específico (véase 10.4.2) el punto extremo debe incluir en el campo **desiredTunnelledProtocol** el IDENTIFICADOR DE OBJETO y el subidentificador del protocolo que espera recibir del otro lado para asegurar la adecuada funcionalidad del controlador de acceso.

  DSS1 es un protocolo asimétrico y sólo puede utilizarse entre un usuario y una entidad de red. Utilizando distintos IDENTIFICADORES DE OBJETO para usuarios y para entidades de red, los puntos extremos H.323 pueden asegurar que no se realiza ninguna tunelización DSS1 entre dos usuarios o entre dos entidades de red.

  Los mensajes H.225.0 tunelizan el mensaje completo, sin modificar, comenzando por el campo discriminador de protocolo y terminando por los otros elementos de información. El contenido binario de los mensajes DSS1 se codifica como una CADENA DE OCTETOS en:

- **H323-UU-PDU.tunnelledSignallingMessage.messageContent**

  Dado que se tuneliza la codificación binaria de los mensajes DSS1, se preserva completamente la integridad de los mensajes DSS1, incluyendo cualquier codificación BER de ASN.1 en los elementos de información del indicador de facilidad o de notificación.

  Los mensajes DSS1 pueden tunelizarse en el correspondiente mensaje H.225.0 o en mensajes H.225.0 FACILIDAD. Por ejemplo, el mensaje DSS1 ESTABLECIMIENTO puede tunelizarse en un mensaje H.225.0 ESTABLECIMIENTO, y el mensaje DSS1 LIBERACIÓN COMPLETA puede tunelizarse en un mensaje H.225.0 LIBERACIÓN COMPLETA. Para los demás mensajes, es posible que no se soporte el correspondiente mensaje H.225.0 (por ejemplo, un mensaje DSS1 ACUSE DE RECIBO CONEXIÓN), que puede no estar disponible por haber sido ya enviado o transportado de forma no transparente extremo a extremo. En estos casos, el mensaje DSS1 deberá ser tunelizado en un mensaje H.225.0 FACILIDAD. En particular, los mensajes H.225.0 ACUSE DE RECIBO DE ESTABLECIMIENTO o LLAMADA EN CURSO no se utilizarán para la tunelización de un mensaje DSS1, debido a la posibilidad de no alcanzar el punto extremo H.225.0 de origen si un controlador de acceso intermedio ya ha enviado dicho mensaje. En su lugar, para la tunelización de un mensaje DSS1 ACUSE DE RECIBO DE ESTABLECIMIENTO o LLAMADA EN CURSO, se enviará en primer lugar un mensaje H.225.0 ACUSE DE RECIBO DE ESTABLECIMIENTO o LLAMADA EN CURSO sin un mensaje DSS1 tunelizado, seguido de un mensaje H.225.0 FACILIDAD que tuneliza el

mensaje DSS1 ACUSE DE RECIBO DE ESTABLECIMIENTO o LLAMADA EN CURSO. Asimismo, los mensajes DSS1 ESTADO e INDAGACIÓN DE ESTADO se tunelizarán en un mensaje H.225.0 FACILIDAD para garantizar que los mensajes DSS1 alcanzan el punto extremo H.225.0.

Los procedimientos de liberación de llamada DSS1 pueden soportarse mediante la tunelización de los mensajes DSS1 DESCONEXIÓN y LIBERACIÓN en el mensaje H.225.0 FACILIDAD.

Una llamada única DSS1 se tuneliza en una única llamada H.323. El punto extremo de entrada selecciona la referencia de llamada DSS1, que será la misma en todos los mensajes DSS1 tunelizados para una llamada H.323. Sin embargo, el valor de referencia de llamada DSS1 en una red TDM es único para cada entidad DSS1 par. En un sistema H.323, no existe la referencia de la entidad DSS1 par pues cualquier llamada H.323 puede terminar en cualquier punto extremo. Para garantizar el carácter unívoco, el valor de referencia de la llamada H.323 sólo debería utilizarse para identificar la llamada H.323.

Los procedimientos de tunelización DSS1 no se utilizarán junto con los procedimientos H.450.1 en la misma llamada.

En el cuadro M3.1 se ilustra la relación existente entre los mensajes DSS1 tunelizados y los mensajes H.225.0 que contienen a los mismos.

Cuadro M3.1/H.323 – Relación entre los mensajes DSS1 tunelizados y los mensajes H.225.0 envolventes

Mensaje Q.931/Q.932	Mensaje H.225.0	Observaciones
Mensajes de establecimiento de la comunicación		
AVISO	AVISO	
LLAMADA EN CURSO	FACILIDAD	
CONEXIÓN	CONEXIÓN	
ACUSE DE CONEXIÓN	FACILIDAD	
INFORMACIÓN	FACILIDAD	Es facultativo el soporte del mensaje H.225.0 INFORMACIÓN
PROGRESO	FACILIDAD	Es facultativo el soporte del mensaje H.225.0 PROGRESO
ESTABLECIMIENTO	ESTABLECIMIENTO	
ACUSE DE ESTABLECIMIENTO	FACILIDAD	
Mensajes de liberación de llamada		
DESCONEXIÓN	FACILIDAD	
LIBERACIÓN	FACILIDAD	
LIBERACIÓN COMPLETA	LIBERACIÓN COMPLETA	

Cuadro M3.1/H.323 – Relación entre los mensajes DSS1 tunelizados y los mensajes H.225.0 envolventes

Mensaje Q.931/Q.932	Mensaje H.225.0	Observaciones
Mensajes de información de llamada		
REANUDACIÓN	En estudio	
ACUSE DE REANUDACIÓN	En estudio	
RECHAZO REANUDACIÓN	En estudio	
SUSPENSIÓN	En estudio	
ACUSE DE SUSPENSIÓN	En estudio	
RECHAZO DE SUSPENSIÓN	En estudio	
INFORMACIÓN DE USUARIO	FACILIDAD	
Mensajes diversos		
CONTROL DE CONGESTIÓN	FACILIDAD	
NOTIFICACIÓN	FACILIDAD	Es facultativo el soporte del mensaje H.225.0 NOTIFICACIÓN
ESTADO	FACILIDAD	
INDAGACIÓN DE ESTADO	FACILIDAD	
FACILIDAD	FACILIDAD	
RETENCIÓN	FACILIDAD	
ACUSE DE RETENCIÓN	FACILIDAD	
RECHAZO DE RETENCIÓN	FACILIDAD	
RECUPERACIÓN	FACILIDAD	
ACUSE DE RECUPERACIÓN	FACILIDAD	
RECHAZO DE RECUPERACIÓN	FACILIDAD	
NOTA – Los mensajes DSS1 con referencia de llamada global, por ejemplo, REINICIO, ACUSE DE REINICIO y ESTADO pueden ser tratados por los puntos extremos y, por tanto, puede no ser necesario tunelizarlos.		

M3.4 Tunelización de la señalización DSS1 independiente del portador

Para la tunelización de los mecanismos de transporte independientes del portador de DSS1 que se describen en 6.3.2/Q.932, no son necesarios ni el canal de control ni los canales de medios H.245.

Los procedimientos de señalización de llamada de H.225.0 pueden utilizarse para establecer una conexión de señalización independiente de la llamada entre los puntos extremos pares, tal como se describe en 10.4. En 6.2/H.450.1 puede encontrarse más información sobre esta conexión de señalización independiente de la llamada.

M3.4.1 Transporte sin conexión DSS1

El mecanismo de transporte sin conexión DSS1 que se describe en 6.3.2.2/Q.932, se basa en los mensajes FACILIDAD que utilizan el valor de referencia de llamada ficticio.

Cada uno de dichos mensajes DSS1 FACILIDAD deberán ser transportados en una conexión H.225.0 separada, que deberá ser liberada inmediatamente después de alcanzarse el lado de terminación.

En particular, un mensaje DSS1 FACILIDAD deberá transportarse en un mensaje H.225.0 ESTABLECIMIENTO, tal como se describe en 10.4 y en 6.2/H.450.1. El lado de terminación (pero no el controlador de acceso intermedio) deberá liberar esta conexión inmediatamente mediante un mensaje H.225.0 LIBERACIÓN COMPLETA. Además, la entidad que envía el mensaje H.225.0 ESTABLECIMIENTO deberá liberar la llamada después de recibir la indicación de expiración de un temporizador adecuadamente elegido y que arrancó después del envío del mensaje H.225.0 ESTABLECIMIENTO.

M3.4.2 Transporte con conexión independiente del portador DSS1

El mecanismo de transporte con conexión independiente del portador DSS1 que se describe en 6.3.2.1/Q.932, se basa en conexiones que se han iniciado con mensajes REGISTRO.

En este caso, se deberá aplicar la concordancia de mensajes que se indica a continuación.

Mensaje Q.931/Q.932	Mensaje H.225.0	Observaciones
REGISTRO	ESTABLECIMIENTO	El mensaje H.225.0 ESTABLECIMIENTO deberá utilizarse para establecer una conexión de señalización independiente de la llamada, tal como se describe en 6.2/H.450.1. Se deberá acusar recibo del mensaje H.225.0 ESTABLECIMIENTO mediante un mensaje H.225.0 CONEXIÓN al objeto de evitar la liberación de la llamada después de la expiración de T303.
FACILIDAD	FACILIDAD	
LIBERACIÓN COMPLETA	LIBERACIÓN COMPLETA	

M3.5 Procedimientos del controlador de acceso

Un controlador de acceso que participe en una llamada en la que se utiliza la tunelización DSS1 entre los puntos extremos, debería dejar pasar los mensajes DSS1 tunelizados sin modificarlos salvo que intente participar en los procedimientos DSS1 y terminar el protocolo DSS1. Éste puede ser el caso cuando un controlador de acceso ofrezca servicios DSS1.

Anexo M4

Tunelización de la sintaxis de señalización de banda estrecha a través de H.323

M4.1 Alcance

El presente anexo tiene por objeto servir de guía para la utilización del mecanismo de tunelización genérico descrito en 10.4 para tunelizar NSS a través de redes H.323. Otras Comisiones del UIT-T son responsables, en última instancia, de los procedimientos de la NSS. En la Rec. UIT-T Q.1980.1 figura información sobre NSS.

M4.2 Referencias

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

– Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes*.

– Recomendación UIT-T Q.1980.1 (2004), *Sintaxis de señalización de banda estrecha – Definición de sintaxis.*

M4.3 H.225.0 – Procedimientos de punto extremo

Los puntos extremos que soportan la tunelización de información NSS utilizarán los procedimientos de 10.4. Los puntos extremos identificarán la NSS empleando la estructura **tunnelledProtocolObjectID**. Se puede utilizar el **subIdentifier** para identificar la revisión de la variante de NSS, por ejemplo, "2004". Véase el cuadro M4.1.

Cuadro M4.1/H.323 – NSS identificada mediante tunnelledProtocolObjectID

Norma	tunnelledProtocolObjectID	subIdentifier
Rec. UIT-T Q.1980.1 (2004)	{itu-t (0) recommendation (0) q (17) 1980 1}	"2004"

Los mensajes H.225.0 tunelizan el mensaje NSS completo, sin cambios, iniciando con el parámetro de versión (VER) y finalizando con una secuencia de dos pares de octetos retroceso del carro-cambio de renglón (0xD0xA). El contenido de texto de los mensajes NSS se codifica como una CADENA DE OCTETOS en el **H323-UU-PDU.tunnelledSignallingMessage.messageContent**. Como lo que se tuneliza es la codificación de texto de los mensajes NSS, se preserva completamente la integridad de los mensajes NSS.

Por ejemplo, el mensaje IAM de NSS se puede tunelizar en un mensaje SETUP H.225.0 y el mensaje ANM de NSS se puede tunelizar en un mensaje CONNECT H.225.0. Para otros mensajes, es posible que no exista ningún mensaje H.225.0 correspondiente (por ejemplo, en el caso de un mensaje IDR de NSS) o que el mensaje correspondiente no esté disponible porque ya haya sido enviado. En esos casos, se puede tunelizar el mensaje NSS en un mensaje FACILIDAD H.225.0.

Un solo mensaje de llamada de NSS se debe tunelizar en una llamada H.323 única.

La red H.323 podría haber modificado algunos de los elementos de información del mensaje H.225.0, y la pasarela que recibe el mensaje NSS tunelizado podría tener que invalidar los parámetros de NSS correspondientes.

En el cuadro M4.2, que se presenta a modo de ejemplo, se ilustra la correspondencia entre mensajes NSS y mensajes H.225.0.

Cuadro M4.2/H.323 – Correspondencia entre mensajes NSS y mensajes H.225.0

Mensaje NSS	Mensaje H.225.0
IAM	ESTABLECIMIENTO
SAM	INFORMACIÓN
CPG	LLAMADA EN CURSO, AVISO, PROGRESO, NOTIFICACIÓN o FACILIDAD
ACM	LLAMADA EN CURSO, AVISO, PROGRESO, NOTIFICACIÓN o FACILIDAD
ANM, CON	CONEXIÓN
REL	LIBERACIÓN COMPLETA
Todos los demás mensajes	FACILIDAD

M4.4 Procedimientos de controlador de acceso

Un controlador de acceso que participa en una llamada en la que se utiliza tunelización NSS entre puntos extremos, debe pasar sin modificar mensajes NSS tunelizados, a menos que pretenda terminar el túnel. Esto puede ocurrir cuando un controlador de acceso está ofreciendo servicios NSS.

M4.5 Procedimientos de RAS para llamadas encaminadas directamente

En el caso de llamadas encaminadas directamente, el punto extremo H.323 podría desear intercambiar mensajes NSS con el controlador de acceso. El punto de extremo H.323 podría enviar uno cualquiera o todos los mensajes NSS hacia el controlador de acceso tunelizados en mensajes RAS.

El mensaje RAS tunelizará el mensaje NSS completo, sin cambios, iniciando con el parámetro de versión (VER) y finalizando con una secuencia de dos pares de octetos retroceso del carro-cambio de renglón (0xD0xA).

Por ejemplo, el mensaje IAM de NSS puede tunelizarse en mensajes ARQ y ACF de RAS, y el mensaje REL de NSS puede tunelizarse en mensajes DRQ y DCF de RAS. Se pueden tunelizar otros mensajes de NSS en mensajes SCI y SCR de RAS. En el cuadro M4.3 se da un ejemplo de la correspondencia entre mensajes NSS y mensajes RAS.

Cuadro M4.3/H.323 – Correspondencia entre mensajes NSS y mensajes RAS

Mensaje NSS	Mensaje RAS
IAM	ARQ, ACF
REL	DRQ, DCF
Todos los demás mensajes	SCI, SCR

M4.5.1 Característica de túnel de protocolo RAS

Los mensajes NSS se han de encapsular en un parámetro de túnel de protocolo en los mensajes RAS. El parámetro de túnel de protocolo se ha de codificar en el parámetro genericData en el parámetro de solicitud de RasMessage H.225.0.

El parámetro GenericData indica la característica de túnel de protocolo y contiene un parámetro de túnel de protocolo.

En el cuadro M4.4 se define la característica de túnel de protocolo RAS.

Cuadro M4.4/H.323 – Característica de túnel de protocolo RAS

Nombre de la característica:	Túnel de protocolo RAS
Descripción de la característica:	Esta característica permite que se tunelicen mensajes NSS en mensajes RAS
Tipo de identificador de la característica:	Estándar
Valor del identificador de la característica:	1000

M4.5.2 Parámetro del túnel de protocolo RAS

En el cuadro M4.5 se define el parámetro del túnel de protocolo RAS.

Cuadro M4.5/H.323 – Parámetro del túnel de protocolo RAS

Nombre de parámetro:	Túnel de protocolo
Descripción del parámetro:	El parámetro encapsula el mensaje NSS enviado en un mensaje RAS. El contenido es un campo sin procesar compuesto por RasTunnelledSignallingMessage con codificación PER de ASN.1, tal y como se especifica en la ASN.1 más adelante
Tipo de identificador del parámetro:	Estándar
Valor del identificador del parámetro:	1
Tipo de parámetro:	Raw
Cardinalidad del parámetro:	Una y sólo una vez

M4.5.3 Definición ASN.1 de túnel de protocolo

A continuación se muestra la definición de túnel de protocolo empleada en GenericData.

```
RAS-PROTOCOL-TUNNEL DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
     TunnelledProtocol,
     NonStandardParameter
     FROM H323-MESSAGES;

RasTunnelledSignallingMessage ::=         SEQUENCE
{
```

```
    tunnelledProtocolID  TunnelledProtocol,        -- tunnelled signalling protocol ID
    messageContent       SEQUENCE OF OCTET STRING, -- sequence of entire message(s)
    tunnellingRequired   NULL OPTIONAL,
    nonStandardData      NonStandardParameter OPTIONAL,
    ...
}


END
```

M4.5.4 Descripción de campos y tipos de ASN.1

tunnelledProtocolID – contiene el identificador de protocolo de señalización tunelizado.

tunnellingRequired – si este campo se encuentra presente, la llamada continuará únicamente si se soporta la tunelización.

messageContent – éste es el contenido del mensaje de señalización tunelizado.

Anexo O

Uso de los URL y las DNS

O.1 Alcance

La presente Recomendación define un medio de construcción de servicios de comunicación multimedia, entre ellos Internet, sobre una red de paquetes arbitraria. Es conveniente aprovechar servicios tales como el sistema de nombres de dominio (DNS) [O-1] y ENUM [O-9] para facilitar la realización de las llamadas multimedia, especialmente cuando se utiliza H.323 sobre Internet. La presente Recomendación define los procedimientos de utilización del DNS para localizar controladores de acceso y puntos extremos, y para resolver los alias de los URL H.323. Esta Recomendación define asimismo los parámetros que se han de utilizar con los URL H.323.

O.2 Referencias normativas

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

[O-1] IETF RFC 1034 (1987), *Domain names – concepts and facilities*.

[O-2] IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax.*

[O-3] IETF RFC 2782 (2000), *A DNS RR for specifying the location of services (DNS SRV).*

O.3 Referencias informativas

Obsérvese que estos documentos son de carácter informativo no siendo necesaria su implementación en este anexo.

[O-4] Recomendación UIT-T E.164 (2005), *Plan internacional de numeración de telecomunicaciones públicas*.

[O-5] IETF RFC 768 (1980), *User datagram protocol*.

[O-6] IETF RFC 793 (1981), *Transmission control protocol*.

[O-7] IETF RFC 1006 (1987), *ISO transport services on top of the TCP: Version 3*.

[O-8] IETF RFC 2806 (2000), *URLs for Telephone Calls*.

[O-9] IETF RFC 2916 (2000), *E.164 number and DNS*.

[O-10] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

O.4 El URL H.323

El localizador uniforme de recursos (URL, *uniform resource locator*) H.323 define la ubicación de una entidad o servicio H.323 a la que se puede llegar por procedimientos normalizados H.323. El URL H.323 puede incluir parámetros opcionales para especificar servicios y protocolos de transporte que faciliten las comunicaciones H.323. Los URL son de gran utilidad en las páginas web, como entradas facilitadas por el usuario, como salidas de los procedimientos ENUM, etc.

El URL H.323 suele ser de la forma *user@hostport* donde alguna de las partes (o sea o bien sólo *user* o bien sólo *@host*) o ambas (o sea tanto *user* como *@host)* están presentes. La parte *user* corresponde a un usuario o nombre de servicio H.323. La parte *host* es una dirección IP numérica legal o un nombre de dominio perfectamente determinado que, por consiguiente, permite resolver las direcciones utilizando la infraestructura DNS.

En 7.1.4 puede consultarse la sintaxis específica del URL H.323.

Este anexo define los URL H.323 y los procedimientos para la utilización de los URL H.323.

O.5 Codificación de los URL H.323 en los mensajes H.323

En términos generales, los procedimientos definidos en este anexo son aplicables a los URL H.323 codificados con su nombre de esquema. El procesamiento de URL/URI sin nombre de esquema codificado queda pendiente de estudio salvo indicación explícita en sentido contrario en esta Recomendación.

Los puntos extremos codificarán los URL H.323 con su nombre de esquema en el campo **url-ID** de **AliasAddress**.

Durante el procedimiento de resolución de la dirección, el controlador de acceso intentará recuperar un URL H.323 del campo **url-ID** de **AliasAddress**. Si no puede conseguirlo, el controlador de acceso deberá intentar recuperar el URL H.323 del **h323-ID** de **AliasAddress**. La misión de este último es soportar el direccionamiento de los URL incluso cuando no haya una interfaz URL expuesta a un usuario de anteriores implementaciones de puntos extremos. Esto permite que el usuario sea capaz de transportar el URL de destino insertándolo manualmente con su nombre de esquema como si se tratase de un **url-ID** de formato libre.

O.6 URL y URI no H.323 en el contexto H.323

Los esquemas de URL y URI de norma distinta a H323 (tales como *mailto*, *tel* y *sip*) pueden integrarse en los mensajes H.323.

Los URI que no sean H.323 deberán insertarse en los mensajes H.323 con su formato completo (incluido el nombre del esquema) en un campo **url-ID** del tipo **AliasAddress**.

Una entidad H.323 (tal como un controlador de acceso) deberá procesar los URI (integrados en los mensajes H.323) de acuerdo con su sintaxis y semántica determinados por el nombre de su esquema.

O.7 Parámetros de URL H.323

El cuadro siguiente resume los *url-parameters* normalizados de los URL H.323. Las combinaciones de parámetros válidas se deducen del texto principal de esta Recomendación.

Parámetro	Descripción abreviada
user (usuario)	Indica que la parte *user* del URL H.323 contiene un número de teléfono.
service (servicio)	Especifica el tipo de servicio recomendado (o sea uno de los protocolos H.323) que ha de invocarse para llegar a la entidad en cuestión.
transport (transporte)	Indica el protocolo de transporte que hay que utilizar para el servicio citado.

O.7.1 Sintaxis ABNF

Este anexo especifica los siguientes valores normalizados para el **url-parameter** definido en 7.1.4:

```
user-parameter      =   "user=phone"
service-parameter   =   "service="("ls" | "rs" | "cs" | "be")
transport-parameter =   "transport="("udp" | "tcp" | "h323mux" | "sctp")
```

NOTA – Es posible que estos parámetros adquieran valores adicionales en las futuras revisiones de la presente Recomendación.

O.7.2 Parámetro User (usuario)

Actualmente sólo hay definido un único valor normalizado para el parámetro *user*, a saber: *phone* (teléfono).

user=phone expresa explícitamente que la parte de usuario del URL H.323 transporta un número de teléfono.

Cuando se codifica el esquema *tel* URL [O-8] en el URL H.323, se omitirá el nombre de su esquema (es decir "tel:") y todos los atributos utilizados (los que comienzan con ";") se colocarán en la parte *user* del URL H.323. Obsérvese que se aplicará una secuencia de escape a todos los caracteres que existan en *tel* URL pero que no se admitan en la parte de usuario del URL H.323.

O.7.3 Parámetro Service (servicio)

El *service-parameter* puede adoptar uno de los cuatro valores siguiente: *ls*, *rs*, *cs* o *be* que representarán, respectivamente, RAS LRQ, RAS RRQ, los mensajes de señalización de llamada H.225.0, o el protocolo inter/intradominio definido en el anexo G/H.225.0.

El valor de *service-parameter* es el del servicio preferido. En el proceso de establecimiento de la conexión, el lado origen puede intentar utilizar otros servicios distintos al especificado en el *service-parameter*.

Si falta el *service-parameter*, la entidad H.323 puede intentar probar con cada uno de los servicios en el orden definido por el usuario. Sírvase consultar en la cláusula O.9 directrices específicas al respecto.

O.7.4 Parámetro Transport (transporte)

Los protocolos de señalización definidos en esta Recomendación pueden utilizar distintos transportes. Los valores *udp*, *tcp*, *h323mux,* y *sctp* especifican UDP [O-5], TCP [O-6], anexo E/H.225.0 y SCTP [O-10], respectivamente. Para cada protocolo H.323 hay valores por defecto tanto para el protocolo de transporte como para el puerto de escucha (es decir, el identificador TSAP conocido) especificado en las Recs. UIT-T H.323, H.225.0 y sus correspondientes anexos. Los valores por defecto pueden especificarse mediante *transport-parameter* y/o *port* del URL H.323. Los valores que sean distintos de los valores por

defecto, deberán especificarse mediante los parámetros *transport-parameter* y/o *port* del URL H.323.

Obsérvese que la inclusión del parámetro *port* (incluido su valor por defecto) tiene un significado especial. Se trata de una indicación a la entidad resolutiva, de que el *host* apunta a una entidad H.323 específica en vez de a un dominio DNS distante conteniendo SRV RR H.323. Pueden consultarse más detalles al respecto en la cláusula O.9.

El valor de *transport-parameter* es el del transporte preferido. En el proceso del establecimiento de la conexión, el lado origen puede intentar utilizar otros protocolos de transporte distintos al especificado en *transport-parameter*.

O.8 Uso del URL H.323

En la actualidad hay dos motivos principales que justifican la utilización de URL H.323: la posibilidad de localizar una entidad H.323 llamable y la de localizar un controlador de acceso en el que registrar un punto extremo.

Adicionalmente, ENUM [O-9] define un sistema de almacenamiento y acceso a las correspondencias entre los números E.164 [O-4] y los servicios asociados a éstos. El sistema ENUM se implementa mediante el sistema de nombres (DNS), en el que los servicios disponibles se representan mediante URI [O-2] normalizados.

Los demás usos del URL H.323 quedan pendientes de estudio.

O.8.1 Localización de los destinos H.323

Cuando un URL H.323 está integrado en una página web o en otro hiperenlace, se puede llegar a un usuario o servicio específicos por medio del protocolo H.323.

Las entidades H.323 pueden resolver los URL H.323 mediante la utilización del DNS, incluidos los puntos extremos, controladores de acceso y elementos frontera como parte del procedimiento de establecimiento de comunicación definido en 8.1.

Cuando un punto extremo de origen opta por resolver el URL de destino, debe codificar tanto el URL como la dirección IP de destino resuelta (de conformidad con la cláusula O.9) en el **destinationInfo** del mensaje ARQ RAS o en el **destinationAddress** de establecimiento y continuar el establecimiento normal de llamada H.323. De lo contrario, es decir si el punto extremo de origen prefiere no resolver el URL destino o falla la búsqueda de DNS, el punto extremo deberá codificar el URL H.323 correspondiente a la cláusula O.5 en el **destinationInfo** del mensaje ARQ RAS o en el **destinationAddress** del mensaje Establecimiento y continuar con el establecimiento normal de la llamada H.323.

Si el URL de destino contiene únicamente la parte *user*, la entidad H.323 resolutiva deberá comportarse lógicamente como si el *hostport* contuviese su propio nombre de dominio.

Sólo una entidad resolutiva que pertenezca al dominio URL (especificado por el *hostport*) interpretará y procesará la parte *user* del URL H.323 con arreglo a su política local. Esta política local puede establecerse en base a los procedimientos definidos por H.225.0 RAS, anexo G/H.225.0, LDAP o la configuración local, entre otros.

Si el *hostport* del URL H.323 es distinto del dominio DNS de la entidad resolutiva deberá ejecutar en primer lugar el procedimiento DNS especificado en la cláusula O.9. Sólo cuando falla el procedimiento DNS, podrá la entidad resolutiva recurrir a un procedimiento de resolución de direcciones distinto basado en su política local.

O.8.2 Localización del control de acceso

Esta Recomendación define un medio de descubrir el control de acceso por medio del mensaje GRQ RAS. Normalmente, esto supone que el envío de los mensajes GRQ se realiza sin que sea necesaria ninguna configuración previa.

No obstante, suele ser habitual dotar estáticamente una ubicación de control de acceso en un punto extremo, lo que además permite mejorar la gestión de la red e implementar esquemas de seguridad flexibles en la misma.

El suministro de una posición de controlador de acceso en términos de URL H.323 y los procedimientos DNS de soporte para el descubrimiento del controlador de acceso por parte de los puntos extremos proporcionan beneficios adicionales. Si se implementan registros de recurso SRV, se puede instalar transparentemente controladores de acceso duplicados y mecanismos de equilibrado de cargas en los puntos extremos.

Si se suministra a un punto extremo la posición de su controlador de acceso mediante un URL H.323 de la forma "h323:*@hostport*" sin parámetros debe utilizarse el valor *hostport* para el descubrimiento de su controlador de acceso. Si se suministra a un punto extremo la posición de su controlador de acceso simplemente con un nombre de dominio DNS válido se supone que este nombre de dominio DNS es el valor del *hostport* del antedicho URL H.323.

Si no se suministra al punto extremo el URL H.323 correspondiente a la posición del controlador de acceso pero se le facilita su propio URL H.323, puede utilizarse el valor *hostport* del URL del punto extremo para el descubrimiento del controlador de acceso.

Para descubrir el controlador de acceso, el punto extremo debe utilizar el valor *hostport* proporcionado con el **service** implícito igual a h323*rs* y con **proto** igual a *udp* como entradas al procedimiento de resolución de direcciones definido en la cláusula O.9.

De fracasar este procedimiento, el punto extremo deberá utilizar los procedimientos normales de descubrimiento del controlador de acceso resumidos en el texto principal de esta Recomendación.

O.9 Resolución de un URL H.323 en dirección IP por medio de DNS

La parte *host* del URL H.323 puede especificar uno de los siguientes elementos:

– La dirección IP numérica de una entidad H.323.

– El nombre DNS de un anfitrión que sea entidad H.323.

– El dominio DNS distante conteniendo RR SRV H.323.

En esta cláusula se define el procedimiento de resolución de direcciones para estos tres casos.

Cuando el *host* contiene una dirección numérica IP, no hay nada que resolver mediante DNS. Los mensajes H.323 se enviarán directamente a la dirección IP especificada.

Cuando la parte *hostport* del URL está presente y contiene un número de puerto, significa que el *host* apunta a una entidad H.323 específica (en vez de especificar un dominio DNS conteniendo RR SRV H.323). Se supondrá que este valor de *port* es el puerto al que han de dirigirse los mensajes H.323. Obsérvese que cuando haya de utilizarse el puerto por defecto, deberá insertarse el número de puerto por defecto para poder representar este caso. La entidad resolutiva deberá intentar recuperar los registros de recursos de direcciones (RR "A" o RR "AAAA") correspondientes al nombre de dominio especificado por el *host*. De recuperarse más de un registro, la entidad resolutiva deberá seleccionar un solo registro en base a su política local (véase asimismo O.10.1). Los mensajes H.323 se enviarán a la dirección IP recuperada (y posiblemente seleccionada) y al puerto especificado por el URL.

Cuando la parte *hostport* del URL esté presente pero no contenga un número de puerto, el *host* indicará casi con toda seguridad, un dominio DNS conteniendo RR SRV H.323. La entidad resolutiva debe intentar localizar esta entidad mediante una recuperación secuencial de registros SRV de un subconjunto de los servicios H.323 posibles (o sea, *h323ls*, *h323rs*, *h323be* y *h323cs*) y sus correspondientes protocolos de transporte posibles (o sea, *udp*, *tcp* y *h323mux*) con arreglo al procedimiento especificado en O.10.4. Este subconjunto deberá ser congruente con las capacidades de la entidad resolutiva y con el objeto del procedimiento (o sea la localización de un controlador de acceso, la de un elemento frontera o la de un destino). Si el *service-parameter* del URL H.323 está presente o si se especifica el *service* SRV (por ejemplo *h323rs*), la búsqueda ordenada de SRV debe realizarse en base a su valor. Cuando no se especifique el *service-parameter*, la entidad resolutiva podrá buscar cualquier otro tipo de registro SRV, o todos ellos, en cualquier orden.

Tras cada recuperación con éxito, es necesario efectuar una consulta adicional al DNS para recuperar los registros de recursos de direcciones. Si la consulta se resuelve con éxito, se enviarán los mensajes a la dirección IP recuperada y seleccionada y a un número de puerto por defecto (correspondiente al protocolo de transporte).

Si no se implementa el protocolo de recuperación del RR SRV, o si falla, la entidad resolutiva puede intentar recuperar los registros de recursos de direcciones correspondientes al nombre de dominio especificado por el *hostport* incluso cuando no se haya especificado el *port.* De recuperarse más de un registro, la entidad resolutiva deberá seleccionar un único registro en base a su política local (véase O.10.1). Si el procedimiento de recuperación tiene éxito, los mensajes H.323 se enviarán a la dirección IP recuperada (y posiblemente seleccionada) y al correspondiente número de puerto por defecto.

O.10 Utilización de los registros de recursos DNS SRV

O.10.1 Aplicabilidad

La utilización de RR DNS SRV (RFC 2782 [O-3]) permite publicar una dirección (es decir, un URI) correspondiente a un servicio específico (*Service*) accesible mediante un protocolo específico (*Proto*). "El RR SRV permite a los administradores utilizar varios servidores para un único dominio [DNS], la transferencia de servicios entre anfitriones con pocas complicaciones y la designación de determinados anfitriones como servidores principales de un servicio y de otros como servidores de seguridad".

En las cláusulas siguientes se definen los nombres simbólicos de los servicios H.323 y de los protocolos de transporte H.323 que han de registrarse en la IANA y son necesarios para la utilización de RR DNS SRV. Este anexo define asimismo los procedimientos normativos que rigen la utilización de RR SRV en los sistemas H.323.

O.10.2 Registro en la IANA

Esta especificación define los siguientes nombres simbólicos para su utilización en el campo *Service* del registro SRV con arreglo a RFC 2782 [O-3].

Servicio	Nombre	Significado
h323ls	Servicio de localización	Entidad H.323 que soporta el procedimiento LRQ H.225.0
h323rs	Servicio de registro	Entidad H.323 que soporta el procedimiento RRQ H.225.0 (es decir controlador de acceso que acepta el registro de puntos extremos)
h323cs	Señalización de llamada	Entidad H.323 que ejecuta la señalización de llamada H.225.0
h323be	Elemento frontera	H.323 que soporta la comunicación definida en el anexo G/H.225.0

Esta especificación define los siguientes nombres simbólicos para su utilización en el campo *Proto* del registro SRV con arreglo a RFC 2782 [O-3].

Nombre simbólico	Significado
udp	UDP definida en RFC 768 "Protocolo de datagrama de usuario" [O-5]
tcp	TPKT [O-7] sobre TCP [6] con arreglo al apéndice IV/H.225.0
sctp	SCTP definido en RFC 2960 [O-10]
h323mux	Definido en el anexo E "Marco y protocolo de redes alámbricas para el transporte de la señalización de llamadas multiplexadas"

O.10.3 Relleno de RR SRV

De acuerdo con la definición de RFC 2782 [O-3], el código de tipo de DNS para RR SRV es 33 y su formato el siguiente:

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

Todos los campos deberán rellenarse con arreglo a RFC 2782.

Service y *Proto* deberán tener uno de los nombres simbólicos definidos anteriormente. *Port* deberá tener un valor de puerto de escucha en el anfitrión H.323, definido mediante un *Target*.

Si en un dominio DNS hay diversas formas de acceso H.323 (es decir, combinaciones de *Service* y *Proto*) deberán publicarse todas ellas utilizando registros SRV separados.

Los campos *Priority* (*prioridad*) y *Weight* (*peso*) deberán utilizarse para expresar la política de preferencias locales de los servicios.

O.10.4 Recuperación y procesamiento de RR SRV

Este procedimiento no define la prioridad de procesamiento de los *Service*s H.323 ni de los *Proto*s H.323.

Este procedimiento tiene como entrada un valor específico de *Service* H.323 y un valor específico de *Proto*, exclusivamente. No se permiten las búsquedas de la forma _service.*.

Si no se recupera ningún registro SRV falla el procedimiento.

El procesamiento local de los registros SRV recuperados deberá ajustarse al algoritmo de selección basado en *Priority* descrito en RFC 2782. Se utilizará el algoritmo de selección basado en *Weight* descrito en RFC 2782. No cabe comparar los valores Priority y Weight entre *Services* H.323 o *Protos* H.323 distintos.

El resultado de este proceso es una lista ordenada de RR SRV (con o sin RR de direcciones correspondientes posiblemente suministrados en la cláusula de datos adicionales de RR SRV).

O.10.5 Ejemplo 1

En este ejemplo se muestra un fragmento de una zona DNS o fichero de dominio DNS correspondiente a **example.com**. Todos los servidores H.323 se encuentran a la escucha en TSAP conocidos. Hay dos controladores de acceso instalados en el dominio. El **local-gatekeeper** proporciona los servicios de registro y puede ser "descubierto" por sus puntos extremos locales. Desde el exterior, los servicios H.323 son accesibles a través del **external-gatekeeper** mediante la consulta de los servicios de señalización de llamada del dominio. Además, el **external-gatekeeper** resolverá sus direcciones de punto extremo respondiendo a las peticiones LRQ procedentes del exterior de su dominio.

La separación funcional entre ambos controladores de acceso puede ser únicamente lógica y resulta útil en los entornos protegidos por NAT en los que ambos controladores de acceso utilizan direccionamiento IP local y externo.

```
$ORIGIN example.com.
_h323rs._udp            SRV 0 1 2517 local-gatekeeper.example.com.
_h323ls._udp            SRV 0 1 2517 external-gatekeeper.example.com.
_h323cs._tcp            SRV 0 1 1720 external-gatekeeper.example.com.
local-gatekeeper        A   172.30.79.11
external-gatekeeper     A   172.30.79.12
; NO se soporta el acceso H.323 sobre H.323 anexo E
*._h323mux              SRV  0 0 0 .
; NO se soportan otros servicios (ni siquiera el elemento frontera H.323)
*._tcp                  SRV  0 0 0 .
*._udp                  SRV  0 0 0 .
```

O.10.6 Ejemplo 2

En este ejemplo se representa un fragmento de una zona DNS o fichero de dominio DNS correspondiente a **example.com**. Todos los servidores H.323 se encuentran a la escucha en TSAP conocidos. El servicio H.323 se suministra a través de un elemento frontera y de controladores de acceso. No se define, ni cabe suponer, prioridad alguna entre el elemento frontera y los controladores de acceso, siendo ésta una cuestión que depende de la aplicación. Por ejemplo, el servicio exclusivo de voz de alta calidad se presta a través del elemento frontera mientras que la videoconferencia H.323 se presta a través de los controladores de acceso.

Un teléfono de voz H.323 que resida en un dominio debe tener el siguiente URL: **h323:my-alias@example.com;service=be**. En este caso se efectuará en primer lugar una búsqueda de **_h323be._udp** que tendrá éxito. Obsérvese que también se permite buscar **_h323cs._tcp**.

Un servicio de videoconferencia prestado por una MCU H.323 situada en una zona de **main-gatekeeper** o de **secondary-gatekeeper** se publicaría como **h323:conference-alias@example.com;service=cs**. Esto se debe al hecho de que los registros SRV que concuerdan con **_h323cs._tcp** se recuperarán en base al *service-parameter*. Además, gracias al campo **Weight** el acceso real a **main-gatekeeper** es tres cuartos del correspondiente a **secondary-gatekeeper** siempre que alguno de los controladores de acceso se encuentre en funcionamiento.

```
$ORIGIN example.com.
_h323be._udp            SRV 0 1 2099 border-element.example.com.
_h323cs._tcp            SRV 0 1 1720 secondary-gatekeeper.example.com.
_h323cs._tcp            SRV 0 3 1720 main-gatekeeper.example.com.
border-element          A   172.30.79.10
main-gatekeeper         A   172.30.79.11
secondary-gatekeeper    A   172.30.79.12
; NO se soporta el acceso H.323 sobre H.323 anexo E
*._h323mux              SRV  0 0 0 .
; NO se soportan otros servicios (ni siquiera el elemento frontera H.323)
*._tcp                  SRV  0 0 0 .
*._udp                  SRV  0 0 0 .
```

Anexo P

Transferencia de señales módem por sistemas H.323

P.1 Alcance

El objetivo de este anexo es describir los procedimientos para transferir señales módem por redes H.323. Los procedimientos de señalización describen la utilización de eventos de señalización de estado (SSE, *state signalling events*) H.245 (incluidas las capacidades de conexión rápida y conexión rápida ampliada, para indicar las capacidades del punto extremo, abrir y cerrar canales lógicos, y señalar los cambios de estado. Las entidades H.323 que soportan el transporte de señales módem por redes IP proporcionarán esa funcionalidad de conformidad con este anexo.

P.2 Referencias

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

[P-1] Recomendación UIT-T V.150.1 (2003), *Módem sobre redes de protocolo Internet: Procedimientos para la conexión de extremo a extremo de los equipos de terminación de circuitos de datos de la serie V*.

[P-2] Recomendación UIT-T H.460.6 (2002), *Característica de conexión rápida ampliada*.

[P-3] IETF RFC 2198 (1997), *RTP Payload for Redundant Audio Data*.

P.3 Definiciones

En este anexo se definen los términos siguientes.

P.3.1 módem sobre IP: Transporte de señales módem por una red IP, según se describe en la Rec. UIT-T V.150.1.

P.3.2 retrasmisión módem: Transporte de datos de módem sobre una red de paquetes, mediante terminaciones módem en los puntos de acceso a la red.

P.3.3 evento de señalización de estado: Mensajes de eventos codificados en protocolo en tiempo real (RTP, *real time protocol*) que coordinan la conmutación entre diferentes estados de medios, según se describe en el anexo C/V.150.1.

P.3.4 datos en banda vocal: El transporte de señales módem por un canal audio de una red de paquetes con la codificación adecuada para las señales módem.

P.4 Abreviaturas

En este anexo se utilizan las siguientes siglas.

FEC Corrección de errores en recepción (*forward error correction*)

MoIP Módem sobre el protocolo Internet (*modem over IP*)

MPS Tren de cabida útil múltiple (*multiple payload stream*)

OLC Apertura de canal lógico (*open logical channel*)

RTP Protocolo en tiempo real (*real time protocol*)

SPRT Transporte simple para la retransmisión de paquetes (*simple packet relay transport*)

SSE Evento de señalización de estado (*state signalling event*)

VBD Datos en banda vocal (*voice band data*)

P.5 Introducción

Los sistemas H.323 se están utilizando mucho en todo el mundo para transportar tráfico de audio, de vídeo y de datos sobre redes de paquetes, en particular redes IP. Una de sus aplicaciones ha sido el tránsito de llamadas audios entre dos redes con conmutación de circuitos separadas o dos puntos en la misma red de conmutación de circuitos. En este tipo de aplicaciones, la llamada se origina en la red de conmutación de circuitos y se entrega a una pasarela H.323. Seguidamente esta pasarela establece la comunicación con una pasarela distante que, a su vez, entrega la llamada a una red con conmutación de circuitos.

En estas aplicaciones también convendría transmitir datos entre pasarelas, y no únicamente audio o vídeo. El anexo D presenta los procedimientos de señalización necesarios para facilitar el transporte de datos facsímil sobre redes IP entre pasarelas y otros dispositivos. El propósito de este anexo es especificar los procedimientos para el transporte de datos módem sobre redes IP entre dos pasarelas.

En la figura P.1 se han representado dos pasarelas H.323 que transportan señales de módem entre dos terminales de módem sobre una red IP.

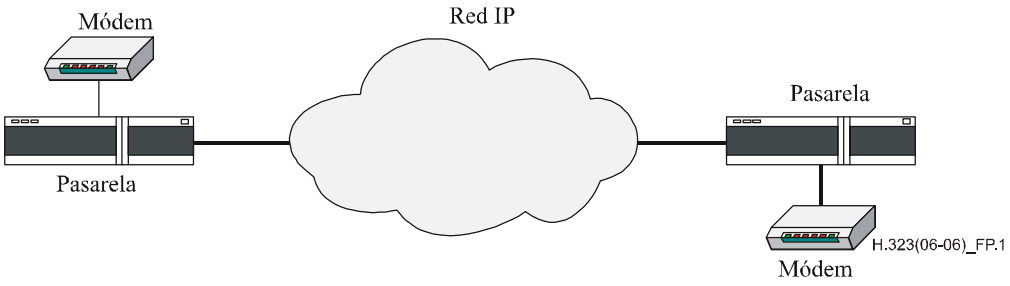


Figura P.1/H.323 – Aplicación característica del módem sobre IP

En la Rec. UIT-T V.150.1 se definen procedimientos generales para el transporte de señales módem sobre redes IP entre dos pasarelas. Esa Recomendación y este anexo son complementarios. La Rec. UIT-T V.150.1 define el transporte de señales módem en general, no para un determinado protocolo de control de llamada, pero en este anexo se definen los procedimientos necesarios y específicos para esta Recomendación.

A no ser que se estipule explícitamente lo contrario, cuando se hable de puntos extremos H.323 en el resto de este anexo se trata de puntos extremos capaces de transportar señales módem sobre redes IP.

P.6 Anuncio de capacidades

Como de costumbre, los puntos extremos anuncian sus capacidades utilizando el mensaje **terminalCapabilitySet** definido en H.245. Las capacidades especialmente importantes y necesarias para las aplicaciones de módem sobre IP son las capacidades de aplicaciones de datos MoIP y SSE (definidas en el anexo F/V.150.1), los eventos de telefonía audio RTP (véase B.2.2.13/H.245) y la capacidad audio **vbd**. Para mejorar la fiabilidad del canal datos en banda vocal (VBD, *voice band data*), los sistemas pueden soportar las capacidades **fecCapability** y/o **redundancyEncodingCapability**.

Los puntos extremos también anunciarán en el conjunto de capacidades que transmiten a los demás puntos extremos que soportan **multiplePayloadStream** (MPS).

Las capacidades MoIP y SSE se definen en el anexo F/V.150.1.

De conformidad con la Rec. UIT-T V.150.1, la lista de códecs soportados como códec VBD incluirá ley μ y ley A G.711. Además, los puntos extremos H.323 soportarán G.711 para VBD a 64 kbit/s y, opcionalmente, a 56 kbit/s.

P.7 Establecimiento de comunicación

Vistas las rigurosas condiciones de tiempo de transmisión de la señalización módem, el punto extremo llamante debería utilizar el procedimiento conexión rápida a fin de ofrecer uno o más canales adecuados para el funcionamiento MoIP. Además debería incluir las capacidades de su terminal en el campo **parallelH245Control** para facilitar la rápida negociación de canales para MoIP.

Asimismo, el punto extremo llamado debería contestar a la conexión rápida lo más rápidamente posible. La respuesta será la aceptación o el rechazo de los canales ofrecidos. Además, si en el mensaje Establecimiento figura el campo **parallelH245Control**, el punto extremo llamado debería confirmar la recepción de esa información, según se especifica en 8.2.4.

Si por alguna razón no se pudieran negociar los medios mediante la conexión rápida, los puntos extremos iniciarán, lo más rápidamente posible, la señalización de canal lógico vía el canal de control H.245. Una vez más, se advierte a los implementadores que las condiciones de tiempo de transmisión del MoIP son muy estrictas y se recomienda que se inicie esta señalización mucho antes de la transmisión del mensaje Conexión.

P.8 Señalización del canal lógico

Hay cinco tipos de trenes que son especialmente importantes para los puntos extremos que soportan MoIP. Estos trenes son: tren de audio, tren VBD, eventos de telefonía audio RTP, eventos de señalización de estado (SSE), y tren SPRT. Los puntos extremos agruparán lógicamente los trenes necesarios para MoIP a través de un canal MPS. La excepción a este requisito es la posibilidad de señalar el tren SPRT en un canal aparte, y relacionarlo con el canal audio/VBD mediante el campo **associatedSessionID**.

En el contexto de una sesión MoIP, se debería considerar que el canal MPS que contiene los trenes de audio y/o VBD, y otros trenes para MoIP, es la sesión audio primaria. Así, el valor de **sessionID** H.245 debería ser uno. Ahora bien, los puntos extremo tienen la libertad de atribuir identificadores de sesión de forma dinámica, según se estipula en la Rec. UIT-T H.245.

Aunque no hay un límite estricto del número de trenes que puede contener un canal MPS, el canal MPS que se utilice para MoIP tendrá cero o más trenes audio, uno o más trenes VBD, un tren SSE, y un tren SPRT. Si este último se abre como un canal separado, el canal MPS no incluirá un tren SPRT. Además, habrá diferentes tipos de cabida útil para audio, para trenes VBD, SSE y SPRT en el MPS. Es posible que se utilicen más de cuatro tipos de cabida útil para los trenes de audio, VBD, SSE y SPRT. Por ejemplo, si el tren VBD está protegido mediante la corrección de errores de recepción (FEC, *forward error correction*) y esos paquetes FEC están incluidos en un paquete de codificación con redundancia, es posible que en lugar de uno haya tres tipos de cabida útil para el tren VBD: uno en el encabezamiento RTP para indicar que el paquete contiene una cabida útil codificada con redundancia, uno para la cabida útil primaria (datos VBD) y otro para los datos FEC que se transportan como codificación secundaria.

Si además se desea proteger un tren VBD, el punto extremo puede utilizar la corrección de errores en recepción y/o la codificación redundante. Es necesario señalar los trenes que utilizan la corrección de errores en recepción, en el campo **fec** de la estructura **DataType** incluida en la estructura **MultiplePayloadStreamElement**. Para señalar los trenes que utilizan la codificación redundante se utilizará el campo **redundancyEncoding** de la estructura **DataType** contenida en la estructura **MultiplePayloadStreamElement**.

Como ejemplo de utilización de la MPS para MoIP, considérese una instrucción apertura de canal lógico (OLC, *open logical channel*) que tiene un tren audio G.729, un tren VBD G.711 ley A protegido con codificación redundante, un tren SSE y un tren SPRT. Básicamente, la composición de esta instrucción **OpenLogicalChannel** sería la que se muestra en este ejemplo abreviado:

```
{
     forwardLogicalChannelNumber 1,
     forwardLogicalChannelParameters {
          dataType : multiplePayloadStream {
               element {
                    dataType : audioData : g729 2
               },
               element {
                    dataType : redundancyEncoding {
                         primary {
                              dataType : audioData : vbd : g711Alaw64k 160
                         },
                         secondary {
                              dataType : audioData : vbd : g711Alaw64k 160
                              payloadType 97 -- The PT for the redundant encoding
                         }
                    },
                    payloadType 101 -- The PT for the RFC 2198 packet
               },
               element {
                    dataType : data {
                         application : genericDataCapability {
                              -- SSE capability
                              capabilityIdentifier : standard {
                                   itu-t(0) recommendation(0) v(22) 150 sse(1)
                              },
                              nonCollapsing {
                                   {
                                        parameterIdentifier : standard 0,
                                        parameterValue : octetString "3,5"
                                             -- A comma-separated string
                                             -- of supported events (this string
                                             -- illustration of syntax and is not
                                             -- necessarily an appropriate list)
                                   },
                                   {
                                        parameterIdentifier : standard 1,
                                        parameterValue : logical
                                   }
                              }
                         }
                    },
                    payloadType 102     -- The PT for the SSE packets
               },
               element {
                    dataType : data {
                         application : genericDataCapability {
                              -- MoIP capability
                              capabilityIdentifier : standard {
                                   itu-t(0) recommendation(0) v(22) 150 moip(0)
```

```
                                   major-version-one(1) minor-version-one(1)
                              },
                              nonCollapsingRaw '0000'H
                                   -- This value shown is only presented
                                   -- for illustration and is not
                                   -- a valid value
                         }
                    },
                    payloadType 103     -- The PT for the MoIP packets
               }
          }
     },
     multiplexParameters : h2250LogicalChannelParameters {
          sessionID 1
     }
}
```

P.8.1 Conexión rápida ampliada

La conexión rápida ampliada [P-2] se debería utilizar para reconfigurar los canales lógicos, ya que es mucho más rápido que intercambiar una serie de mensajes H.245. Cuando un punto extremo necesita pasar de funcionamiento audio a funcionamiento MoIP y en ese momento no tiene un canal abierto adecuado para MoIP, en primer lugar debería tratar de reconfigurar los canales utilizando la conexión rápida ampliada.

La conexión rápida ampliada también debería ser la primera opción en la señalización por canales lógicos, aun cuando haya canales que soporten MoIP. Por ejemplo, si el punto extremo desea reemplazar el códec audio G.729 de un MPS por el códec audio G.723.1, debería tratar de reconfigurar los canales lógicos mediante la conexión rápida ampliada, en lugar de utilizar la señalización H.245.

P.8.2 Señalización H.245

Se puede emplear la señalización de canales lógicos H.245, mediante el canal de control H.245, para configurar o reconfigurar trenes de medios cuando sea necesario. Los puntos extremo con capacidades MoIP soportarán la tunelización H.245 cuando sea necesario utilizar un canal de control H.245. Ahora bien, se precisa que el hecho de soportar la tunelización H.245 no garantiza que se vaya a utilizar, y que puede ser necesaria una conexión aparte, aunque no se recomienda.

Si bien la señalización para abrir nuevos canales no supone normalmente un problema para los puntos extremos H.323, existe la posibilidad de que dos puntos extremos traten de abrir canales cada uno por su lado, lo que daría lugar a una configuración incompatible. Para resolver este tipo de problemas, el maestro rechazará las propuestas OLC del dispositivo esclavo con el motivo **masterSlaveConflict**. Seguidamente el maestro debería enviar un mensaje **RequestMode** al dispositivo esclavo a fin de proponer un modo de funcionamiento compatible.

Si el punto extremo determina que es necesario pasar a otro modo de funcionamiento para, por ejemplo, pasar del modo sólo audio a un modo que soporte MoIP, el punto extremo enviará un mensaje **RequestMode** al otro punto extremo. Por ejemplo, supóngase que dos puntos extremos abren un canal audio G.729 en cada sentido y que uno de ellos determina que es necesario cambiar del modo de funcionamiento audio al MoIP. El punto extremo enviará un mensaje **RequestMode** por el canal de control H.245 en el que indicará el modo de funcionamiento deseado. El punto extremo receptor responderá con un mensaje de confirmación o de rechazo, según corresponda, aunque debería hacer todo lo posible para aceptar el modo de funcionamiento solicitado. Los puntos extremos intercambiarían estos mensajes más o menos como se indica en la figura P.2. En la medida de lo posible, los mensajes se deberían intercambiar en paralelo para reducir los retardos debidos a la transición de modo.

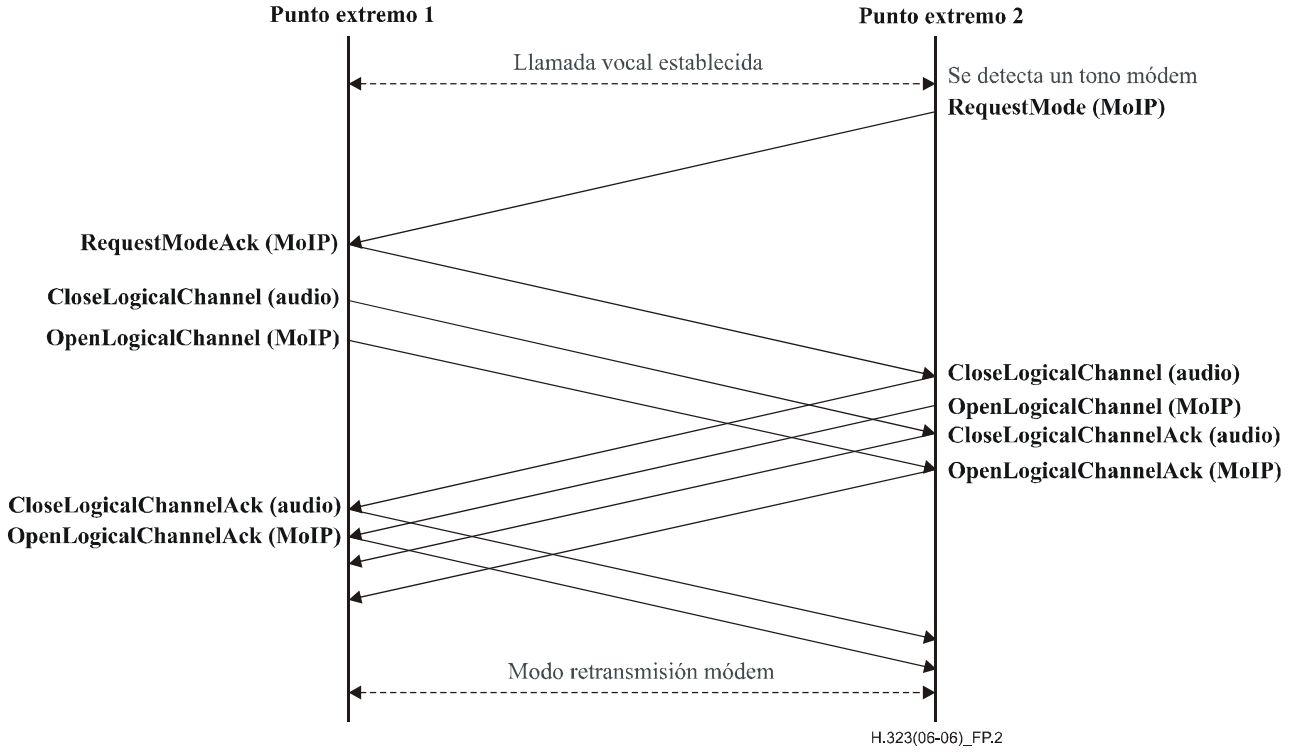


Figura P.2/H.323 – Paso del modo audio al modo MoIP realizado satisfactoriamente

Anexo Q

Control de cámara en el extremo lejano y Recomendaciones H.281 y H.224

Q.1 Alcance

Este anexo tiene como finalidad proporcionar un protocolo de control de cámara en el extremo lejano de conformidad con H.281 y H.224. También permite a un punto extremo H.323 ejecutar cualquier aplicación H.224 mediante el protocolo IP/UDP/RTP/H.224 que se define en el presente anexo.

Q.2 Referencias normativas

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

[Q-1] Recomendación UIT-T H.224 (2005), *Protocolo de control en tiempo real para aplicaciones símplex que utilizan los canales de datos a baja velocidad, datos a alta velocidad y protocolo multicapa de la Rec. UIT-T H.221*.

[Q-2] Recomendación UIT-T H.281 (1994), *Protocolo de control de cámara en el extremo lejano para videoconferencias conforme a la Recomendación H.224*.

[Q-3] Recomendación UIT-T T.140 (1998), *Protocolo de conversación mediante texto para aplicaciones multimedia*.

Q.3 Introducción

El protocolo descrito en este anexo se puede utilizar para soportar el control de cámara en el extremo lejano (FECC, *far-end camera control*) en esta Recomendación utilizando la pila IP/UDP/RTP/H.224/H.281. Este protocolo soporta aplicaciones punto a punto y multipunto.

Este método se puede utilizar como plan de FECC "simple" cuando no se necesita recurrir a las características complejas de las Recomendaciones UIT-T H.282 y H.283.

El método se utilizará para el FECC mediante pasarelas H.320-H.323 y H.324-H.323 cuando los puntos extremos H.320 o H.324 no soporten lo indicado en la Rec. UIT-T H.282.

Los requisitos que figuran *infra* sólo se aplican en el caso en que se haya seleccionado el protocolo descrito en este anexo, conforme a los procedimientos normales de la Rec. UIT-T H.245.

Se autoriza la ejecución de cualquier aplicación H.224 mediante el protocolo IP/UDP/RTP/H.224 definido en el presente anexo. La otra única aplicación H.224 actualmente normalizada es la que figura en la Rec. UIT-T T.140.

Q.4 Protocolo de control de cámara en el extremo lejano

Q.4.1 Generalidades

Este protocolo se basa en la Rec. UIT-T H.281, que utiliza a su vez la Rec. UIT-T H.224 en un canal RTP/UDP.

En las redes de transporte IP, la estructura de los octetos del protocolo H.224 será la indicada en la figura 2/H.224, excepto que, en el primer caso, se omitirán el relleno del bit HDLC, las banderas HDLC y la secuencia de verificación de trama HDLC. La totalidad del contenido restante de cada trama se colocará en un único paquete RTP.

Las referencias que figuran en la Rec. UIT-T H.224 con respecto al canal LSD de la Rec. UIT-T H.221, se deben interpretar en relación con el canal lógico H.224, descrito en el presente anexo. Con ese canal lógico, cuyo funcionamiento se considera que se efectúa a 4800 bit/s, independientemente de la velocidad binaria real del canal, se cumplirán los requisitos de tiempo de transmisión máximo conforme a la Rec. UIT-T H.224.

Este protocolo utilizará el RTP en un canal lógico H.245 unidireccional no fiable. El valor de parte útil del RTP será dinámico. El campo descriptor de cabida útil del **RTPPayloadType** H.245 utilizará el identificador de objeto H.224.

A fin de soportar la capa de enlace de datos en aplicaciones multipunto, se utilizará la numeración terminal conforme a los procedimientos de la Rec. UIT-T H.243. El par de dirección MCU/Terminal <M><T> se utilizará solamente para identificar cada terminal en una conferencia. La dirección de destino especial de <0><0> será utilizada como dirección de radiodifusión. La dirección de origen especial <0><0> indicará que el emisor no conoce su dirección. Una dirección con el número terminal puesto a 0 indica que se trata del MC. Por ejemplo, <n><0> indica que el número del MC es n.

Cuando en una llamada punto a punto sólo intervienen dos terminales, éstos no tienen una dirección <M><T>. En ese caso, las direcciones de origen y destino <M><T> serán siempre <0><0>.

Para una conferencia centralizada se abrirá un canal H.224 entre cada terminal y el MC. Cuando un terminal envíe un paquete H.224, el MC lo seguirá hasta el terminal de destino retransmitiendo cada paquete a todos los demás terminales conectados o bien retransmitiendo selectivamente cada paquete sólo hacia el terminal de destino. La decisión de qué método utilizar corresponde al fabricante de la MCU.

En una conferencia descentralizada con multidifusión, cada terminal debe difundir el paquete FECC a todos los demás terminales. El MC no interviene en la difusión de los paquetes. A fin de identificar los terminales de origen y destino, se deberán utilizar los números de terminales conforme a la Rec. UIT-T H.243.

En conferencias descentralizadas con multiunidifusión, cada terminal utilizará un canal lógico separado para cada terminal de extremo lejano al que se desea enviar paquetes H.224.

Q.4.2 Pasarelas H.320 a H.323

Las pasarelas H.320 a H.323 introducirán y retirarán banderas HDLC, rellenos de bit HDLC y secuencias de verificación de trama HDLC, según corresponda, en cada dirección, de manera que el tren de bits H.320 se ajuste a la Rec. UIT-T H.224, y el tren de bits H.323 se ajuste a los párrafos indicados *supra*.

Q.4.3 Pasarelas H.324 a H.323

Las pasarelas H.324 a H.323 introducirán y retirarán banderas HDLC, rellenos de octetos HDLC y secuencias de verificación de trama HDLC, según corresponda, en cada dirección, de manera que el tren de bits H.324 se ajuste al uso de la Rec. UIT-T H.224 según se describe en la Rec. UIT-T H.324, y el tren de bits H.323 se ajuste a las cláusulas indicadas *supra*.

Q.4.4 Señalización H.245

El uso de este protocolo se señalará con la parte **GenericCapability** de la secuencia **DataApplicationCapability** indicada en H.245. Se utilizará para H.224 la capacidad genérica descrita en la Rec. UIT-T H.224, que se colocará en la parte **receiveAndTransmitDataApplicationCapability** de la elección **Capability**.

Este protocolo no se señalará en las partes **receiveDataApplicationCapability** o **transmitDataApplicationCapability** de la elección **Capability**.

Q.5 Información de encabezamiento del RTP

En el encabezamiento del RTP se rellenarán los siguientes campos:

V:	2
M:	0 NA
PT:	El mismo número enviado en el campo OLC dynamicRTPPayloadType
Número de secuencia:	Rellenado, aumentado en una unidad por cada paquete RTP enviado
Indicación de tiempo:	Rellenada con velocidad de reloj a 8 kHz
SSRC:	Rellenado con el origen de la sincronización

Anexo R

Métodos de robustez para entidades H.323

R.1 Introducción y alcance

Este anexo especifica los métodos que pueden ser utilizados por entidades H.323 para implementar robustez o tolerancia a un conjunto específico de fallos, y especifica métodos de recuperación de canales de señalización de llamada (Rec. UIT-T H.225.0) y de señalización de control de llamada (Rec. UIT-T H.245). El RAS (Rec. UIT-T H.225.0), que no requiere conexión ni recuperación, mas sí registro en un controlador de acceso alternativo, se trata en otro lugar, por lo que no se describe en este anexo. La recuperación de las relaciones de servicio del anexo G queda en estudio.

Las llamadas H.323 requieren la cooperación de dos o más entidades H.323. La información de estado de llamada es distribuida entre las diversas entidades que intervienen en la llamada. La señalización de llamada puede depender de que haya conexiones persistentes entre algunas de las entidades que intervienen. Si una entidad falla y no posee un par de seguridad, podría resultar imposible establecer nuevas comunicaciones. Si una entidad que interviene en una llamada activa falla y no posee un par de seguridad, o ese par no tiene un método de recuperar suficiente información de estado de llamada, podría resultar imposible continuar la llamada. Esta Recomendación proporciona cierto soporte para la construcción de sistemas robustos, pero los mecanismos se hallan repartidos en todo este anexo y se indican pocos procedimientos, o ninguno, para utilizarlos.

Este anexo describe dos métodos alternativos compuestos de mecanismos, así como procedimientos para utilizarlos en la construcción de sistemas que puedan recuperarse de un conjunto importante de fallos específicos. Un método es más apropiado para sistemas de pequeña escala, utiliza entidades más simples y no recupera tanta información de estado de llamada. El otro método es adecuado para sistemas de gran escala, y puede recuperar tanta información como se desee, pero requiere entidades más complejas. Ambos métodos comparten varios mecanismos y pueden utilizarse simultáneamente en diferentes partes de un sistema.

R.2 Referencias normativas

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

[R-1] Recomendación UIT-T H.225.0 (2006), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes*.

[R-2] Recomendación UIT-T Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de la llamada básica*.

[R-3] Recomendación UIT-T X.680 (2002), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.

R.3 Definiciones

Además de los términos definidos en el cuerpo principal de esta Recomendación, se definen los términos siguientes.

R.3.1 entidad de seguridad o par de seguridad: Par de una entidad que puede asumir las funciones de la entidad si ésta falla.

R.3.2 entidades pares: Dos entidades del mismo tipo en un sistema H.323, por ejemplo, dos controladores de acceso. Las dos entidades pueden cooperar en una llamada (por ejemplo, los controladores de acceso de origen y de terminación en una señalización de llamada encaminada por controlador de acceso) o una de las dos puede proporcionar seguridad a la otra.

R.3.3 métodos de robustez: Procedimientos y mecanismos que permiten la recuperación después del fallo de una o más entidades H.323. La amplitud de la recuperación varía de un método a otro y puede incluir mantenimiento de llamadas activas en estado estable o solamente la posibilidad de efectuar nuevas llamadas. Los métodos descritos en el presente anexo suelen poder mantener las llamadas activas.

R.3.4 vecino de señalización: Otras entidades con las que una entidad determinada tiene conexiones directas de señalización de llamada o de control de llamada en una llamada determinada. Por ejemplo, un controlador de acceso que utiliza el modelo de encaminamiento por controlador de acceso puede tener una conexión directa de señalización de llamada en una llamada determinada a una pasarela y otro controlador de acceso. Estas otras dos entidades serían vecinos de señalización del controlador de acceso en esa llamada.

R.3.5 llamadas estables: Una llamada se considera estable o en un estado estable después de que se ha enviado o recibido Conexión y se han establecido canales de medios en ambos sentidos (mediante procedimientos H.245 o de conexión rápida). Una llamada es inestable cuando se ha enviado o recibido Liberación Completa. Ciertas instrucciones de Facilidad utilizadas para cambiar conexiones de señalización de llamada pueden también hacer que una llamada se considere inestable. Esta versión de esta Recomendación ofrece métodos para mantener únicamente llamadas estables durante la recuperación.

R.3.6 entidades en tándem: Dos (o más) entidades pares, todas las cuales menos una actúan como entidades de seguridad para una entidad activa.

R.3.7 entidad virtual: Dos (o más) entidades par estrechamente acopladas que aparecen colectivamente como una sola entidad al resto de un sistema H.323 mientras se produce la recuperación tras un fallo.

R.4 Abreviaturas

En este anexo se utilizan las siguientes siglas.

CRV Valor de referencia de llamada (*call reference value*)

GK Controlador de acceso (*gatekeeper*)

GW Pasarela (*gateway*)

RAS Registro, admisión y situación (*registration, admission and status*)

SCTP Protocolo de transmisión de control de trenes (*stream control transmission protocol*) (IETF RFC 2960) (para información solamente)

SDL Lenguaje de especificación y descripción (*specification and description language*)

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

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

R.5 Sinopsis de los dos métodos

En esta versión del anexo se ofrecen dos métodos de robustez.

El problema que se pretende resolver es la recuperación de un fallo de entidad H.323 que falla. El objetivo es mantener tantas llamadas activas como sea posible. Como mínimo se desea mantener todas las llamadas en un estado "estable". Las llamadas aún no completamente conectadas o que se encuentran en proceso de desconexión pueden perderse. También se persigue el objetivo de conservar la información de facturación más pertinente, como la hora de comienzo y de fin de la llamada, etc., incluso si esta información es mantenida en la entidad que falla (por ejemplo, el controlador de acceso de encaminamiento).

Se supone que la entidad que falla tiene una o varias entidades de seguridad designadas, aunque la solución a pequeña escala puede permitir la recuperación cuando la entidad que falla vuelve rápidamente al servicio. Deben resolverse dos problemas básicos para recuperar señalización de llamadas activas:

1) Redireccionamiento y restablecimiento de señalización a la entidad de seguridad.
2) La entidad de seguridad debe recuperar suficiente información de estado de llamada de la que residía en la entidad que falla.

Los dos métodos se distinguen sobre todo por el método de recuperar información de estado acerca de las llamadas activas y por la cantidad de información recuperada.

R.5.1 Método A: Recuperación de estado a través de los vecinos

En el método A, cada entidad conoce las direcciones de transporte de señalización de las entidades de seguridad de cada vecino de señalización ascendente y descendente. Cuando las entidades se enteran del fallo de su vecino de señalización ascendente o descendente, intentan conectarse a una de las entidades de seguridad. La entidad de seguridad recupera el estado mínimo de llamada por su vecino de señalización utilizando los mensajes Estado e Indagación de estado (ampliados con campos adicionales). Téngase en cuenta que en algunos casos puede ser necesario que el vecino pregunte a su vecino el estado de llamada si no ha mantenido localmente toda la información necesaria (por ejemplo, un controlador de acceso de encaminamiento puede tener información de canal lógico abierto caché).

El estado de llamada recuperado es suficiente para continuar la llamada (envío de señalización de llamada y de señalización de control de llamada y conocimiento de canales lógicos abierto) pero no para permitir a la entidad recuperada participar en la facturación y en algunos otros servicios.

R.5.1.1 Método parcial A

Se puede presentar asimismo un caso en el que una entidad H.323 no disponga de una entidad de respaldo aunque siga implementando el procedimiento de robustez para contribuir a la protección de las llamadas en la eventualidad de que falle su vecino de señalización cuando éste no disponga de una entidad de respaldo.

Cuando una entidad H.323 que participa en la recuperación de llamadas estables de la entidad de respaldo de su vecino de señalización, no tiene su propio respaldo, se dice que implementa el método parcial A.

R.5.2 Método B: Recuperación de estado a través de un depositario compartido

La segunda arquitectura se basa en una seudoentidad tolerante a los fallos. Puede implementarse:

1) Utilizando una plataforma o sistema operativo tolerantes a los fallos.
2) Un fondo común de entidades no tolerantes a los fallos y que compartan información de estado de llamada mediante memoria compartida, discos compartidos, o a través de mensajes. El mecanismo de compartición no se especifica en esta Recomendación.

Las entidades reales en esta seudoentidad tolerante a los fallos deben compartir suficiente información de estado con sus entidades pares para permitir la recuperación del estado de llamada deseado sin ayuda alguna de sus vecinos de señalización. Esta Recomendación definirá las entidades de información mínimas que deben ser compartidas. Toda información adicional que se desea que sea recuperable puede ser compartida. Hay que señalar que este método exigirá que todas las entidades del fondo común que constituyen la seudoentidad provengan del mismo vendedor, ya que el mecanismo de compartición no está normalizado. La comisión sugeriría una o dos posibles soluciones y consideraría recomendar un mecanismo de compartición normalizado en las versiones de la H.323 superiores a 4.

Más adelante se darán más detalles de esta arquitectura.

R.5.3 Comparación

Cada una de estas dos arquitecturas presenta ventajas, lo cual hace que la elección diste de ser evidente. Algunos de los aspectos a tener en cuenta son:

El método de recuperación a través de los vecinos:

1) permite entidades más simples;
2) añade menos tara antes de un fallo (aunque necesita mensajes Mantener vivo en algunos casos);

pero:

1) requiere más cambios en los mensajes H.323;
2) hace la recuperación algo más lenta (debido a los mensajes Estado e Indagación de estado);
3) no es escalable; sólo es adecuado para sistemas de pequeña escala.

El método del depositario compartido:

1) oculta la mayor parte del proceso de recuperación de la entidad H.323, por lo cual requiere menos cambios en los mensajes existentes;
2) hace la recuperación más rápida;
3) permite el uso futuro de protocolos de mantenimiento de estado que pueden implementarse por debajo de la capa de aplicación H.323 (véase la Nota Informativa 2 en la cláusula R.13);
4) puede soportar recuperación de información de facturación y otra información de estado deseada;

pero:

1) añade considerable tara a toda la señalización (antes del fallo);
2) requiere entidades o seudoentidades más complejas.

R.6 Mecanismos comunes

Los dos métodos comparten varios mecanismos comunes.

R.6.1 Detección de conexión basada en TCP perdida

En caso de fallo de red, el primer intento "automático" se haría a nivel de protocolos de encaminamiento IP. Si no tiene éxito, se informará del fallo TCP a ambos extremos (la entidad y su vecino de señalización, por ejemplo, controlador de acceso y punto extremo). Tanto un fallo de red como un fallo del vecino de señalización aparecerá como un fallo TCP.

Cuando se estableció la comunicación, se determinó si el vecino de la entidad soportaba procedimientos de robustez.

En caso de que uno de los extremos no soporte el procedimiento de robustez definido, se sugiere liberar la llamada debido a estado de fallo de conexión TCP.

En el lado punto extremo, en caso de que ambos lados soporten el procedimiento de robustez, se sugiere mantener un tiempo muerto para que el procedimiento de robustez pueda ser iniciado por el otro lado. Este tiempo es necesario para tratar un posible problema de conectividad de red. Una vez expirado este plazo, deben liberarse los recursos internos (consumidos por la llamada).

R.6.2 Tratamiento de fallo de protocolo

Para las entidades que utilizan este anexo, si se produce un fallo de protocolo en un canal de control y ambos vecinos de señalización soportan la robustez, el canal y todos los canales lógicos asociados **no** se cierran (al contrario de 8.6). En su lugar, se intentan los procedimientos de recuperación de este anexo.

R.6.3 Detección de fallos – keepAlive (mantener vivo)

Sin un mecanismo keepAlive, un fallo de entidad o de conexión de señalización se conocerá solamente cuando se utilice la conexión. El anexo E proporciona un mecanismo keepAlive para detectar el fallo aun con poco tráfico. El mecanismo keepAlive del TCP tiene un tiempo muerto demasiado largo para ser de utilidad y, por tanto, con un fallo TCP podría no ser detectado durante largo tiempo en condiciones de bajo tráfico enviado a la entidad que falla. Nuestra solución de pequeña escala depende de que el fallo sea detectado por ambos vecinos de señalización (las conexiones se establecen siempre desde el vecino hacia la entidad recuperada), por lo que necesitamos mensajes keepAlive a nivel H.323 que puedan utilizarse con conexiones TCP. Hay mensajes keepAlive que pueden opcionalmente utilizarse en H.245. Especificaríamos que se utilicen periódicamente mensajes Estado/Indagación de estado en las conexiones TCP para proporcionar este mecanismo keepAlive. Aunque éste es un aspecto común, veremos que es solamente un problema importante en el método A, de recuperación de estado a través de los vecinos.

La entidad más próxima a la parte llamada (lado destino de la conexión o lado que utiliza la bandera de referencia de llamada = 1 en el CRV utilizado en la conexión – véase en la Rec. UIT-T Q.931 la definición de la bandera de referencia de llamada) enviará periódicamente Indagación de estado (éste es el sentido de menor tráfico durante las comunicaciones establecidas). El periodo debe variar aleatoriamente desde un valor máximo configurable hasta la mitad de ese valor a fin de evitar la congestión. Dos segundos es el máximo por defecto recomendado a fin de permitir la detección del fallo antes del vencimiento del plazo de otros mensajes. El valor máximo se incluirá en la Indagación de estado como el tiempo hasta en directo (timeToLive), para que el recibiente pueda también supervisar el fallo sin necesidad de un intercambio adicional de Indagación de estado/Estado en sentido opuesto. El sistema recibiente necesitará solamente mantener un temporizador que utilice el valor máximo indicado como tiempo muerto.

Cuando se utilizan canales multiplexados, no es necesario enviar Indagación de estado/Estado para cada llamada señalizada en el canal. Se aplica a todas las llamadas que utilizan el canal un mensaje de Indagación de estado o Estado con un CRV IE igual a 0 (cero) y con el campo de identificador de la llamada igual a 0 (cero).

Los mensajes keepAlive, especialmente al nivel H.323, pueden añadir considerable tara de señalización. Pero hay que tener en cuenta que sólo el método A utiliza estos mensajes con conexiones TCP y que el método A es para el caso de pequeña escala en el que el número de conexiones por entidad es bajo. Para minimizar la tara debe evitarse la utilización del TCP. StatusInquiry/Status keepAlives **no** se necesitan en nuestra solución de gran escala.

Para reducir al mínimo la repercusión del intercambio de keepAlives, si hay varias llamadas entre estas dos mismas entidades, puede ser necesario enviar mensajes StatusInquiry/Status por cualquiera de las conexiones entre dichas entidades. Para asociar cada llamada activa al conjunto de entidades adecuado, la entidad de origen deberá incluir un GUID de punto extremo en el mensaje Establecimiento y la entidad de destino deberá incluir otro en el mensaje Conexión. Estos GUID deberán ser exclusivos de cada entidad y, cuando una entidad tenga más de una interfaz de señalización, deberán generarse para cada interfaz. Cuando en la entidad haya varios ejemplares H.323, cada uno de ellos generará un GUID único. Deberán mantenerse temporizadores KeepAlive en cada par de GUID único. Una vez expirado el temporizador keepAlive, cualquier entidad podrá enviar un mensaje StatusInquiry con el IE CRV igual a 0 (cero) y con el campo callIdentifier igual a 0 (cero), por cualquier conexión disponible. El vecino de señalización responderá con un mensaje keepAlive Status.

La detección de fallos de las conexiones del anexo E se efectuará utilizando la mensajería Estoy Vivo (I-Am-Alive) existente. El procedimiento descrito anteriormente define los mensajes keepAlive entre entidades de señalización con temporizador. El temporizador utiliza un valor definido por el temporizador T-IMA1, que por defecto se pone a 6 segundos. No obstante, cuando las dos entidades implementan el anexo R, este temporizador deberá ser configurable de conformidad con los valores recomendados citados. La mensajería Estoy Vivo utiliza también el contador definido por el N-IMA1, que define el número de reintentos consecutivos de los mensajes Estoy Vivo antes de que se declare el fallo del vecino de señalización. En las entidades que tienen anexo R, se recomienda que el valor máximo de este contador sea dos (2).

R.6.4 Dirección de transporte y conexiones restablecidas

Estas dos soluciones (con la posible excepción de alguna de plataforma tolerante a los fallos) deben ocuparse de la recuperación del canal de señalización utilizando una dirección de transporte de seguridad. Éstas deben ser intercambiadas cuando se establece la señalización de llamada, utilizando los campos backupCallSignalAddresses en los mensajes Establecimiento y Conexión. Una entidad envía la dirección de señalización de llamada de su par de seguridad en Establecimiento y en Conexión. Una entidad recibe la dirección de señalización de llamada de la entidad de seguridad de su vecino del lado origen cuando recibe Establecimiento, y de su vecino del lado terminación cuando recibe Conexión.

Las entidades que implementen el método parcial A deberán enviar una **backupCallSignalAddresses** vacía para indicar que participa en el procedimiento de robustez aunque no cuentan con un respaldo propio.

Todas las entidades deberán añadir su propia dirección de señal de llamada como primera entrada de la lista **backupCallSignalAddresses** incluido el número de puerto por el que están a la escucha. Esto es imprescindible para que el vecino de señalización (o su respaldo) reanude la conexión con la entidad.

R.6.4.1 Establecimiento de una nueva conexión TCP

Una entidad que detecte pérdida de un canal de señalización de llamada con un vecino de señalización, tratará de restablecer este canal utilizando la dirección de transporte de seguridad. Alternativamente, la entidad que detecta fallo puede intentar sondear a su vecino de señalización original utilizando otros métodos que están fuera del alcance de esta Recomendación (por ejemplo, ping) y, si cree que el vecino de señalización original puede ser utilizable, puede tratar de restablecer el canal hacia aquél antes de ensayar con la dirección de transporte de seguridad. Los implementadores que escojan esta opción deben saber que intentar establecer una conexión TCP con una entidad que no responde puede causar retardos importantes.

El canal de señalización de llamada restablecido asumirá el estado del anterior – no se comporta como un nuevo canal (**no** comenzará con Establecimiento). Véanse más adelante detalles a continuación para asegurar la sincronización de estado entre vecinos de señalización.

PARA INFORMACIÓN – Una alternativa es utilizar el SCTP para el transporte en lugar del TCP. Los canales SCTP se asocian con una lista de direcciones de transporte alternativas que pueden ser utilizadas si es necesario para mantener el canal sin intervención de la capa de aplicación. La Nota Informativa 2 de la cláusula R.13 contiene más información acerca de la utilización del SCTP.

R.6.4.2 Asociación entre la llamada y la nueva conexión TCP

La asociación entre la llamada y la nueva conexión TCP (en el lado punto extremo) se hará mediante la recuperación del valor del identificador de llamada (callIdentifier) a partir del mensaje recibido en la nueva conexión TCP.

R.6.4.3 Cierre de una antigua conexión TCP

Una vez abierta la nueva conexión, podría haber dos conexiones TCP abiertas pertenecientes a la misma llamada en el lado que no falló. Hay dos opciones en este caso:

1) La conexión TCP se perdió después de enviarse (y recibirse) el mensaje ESTABLECIMIENTO. En este caso el lado que no falló identificará la situación y cerrará la conexión. Esto debe realizarse detectando un identificador de llamada idéntico para ambas conexiones.
2) La conexión TCP se perdió antes de transferirse el primer mensaje.

En ese caso, el lado que no falló no tiene ningún modo de distinguir entre la primera conexión TCP (antigua) y la segunda (nueva). Esto puede resolverse por un procedimiento que permita al lado receptor cerrar una conexión si ha estado abierta durante un tiempo sin que se haya recibido por ella ningún mensaje en un plazo previamente definido. (Este procedimiento no se describe en este anexo.)

R.6.5 Soporte de la situación extendida

Para mejorar la interoperabilidad entre los dos métodos, todas las entidades que soportan la robustez soportarán el mensaje Estado ampliado que incluye el campo comienzo rápido (fastStart). Esto permitirá a una entidad con un depositario compartido cooperar con un vecino que requiera Estado para la recuperación de estado.

R.7 Método A: Recuperación de estado a través de los vecinos

R.7.1 Introducción

Actualmente las Recs. UIT-T H.323 y H.225.0 no definen explícitamente los procedimientos para la detección y la consiguiente recuperación de un fallo de conexión. El objetivo de este método es introducir un procedimiento para:

- la detección de fallo de conexión basada en TCP;
- la sincronización entre los dos lados de la conexión en términos de estado de llamada;
- la definición del comportamiento recomendado en cada lado a fin de renovar la conexión de señalización de llamada y proceder con la llamada como sea normal en cada estado de la llamada.

La principal motivación para mantener una llamada (cuando se ha perdido una conexión) se presenta en situaciones en donde un controlador de acceso, que trata un número considerable de llamadas, falla debido a un problema de soporte físico o de soporte lógico. En este caso, puede transferirse un control a un controlador de acceso de reserva (que puede conservar toda la información acerca de las llamadas mediante alguna base de datos común). El procedimiento

definido y presentado en este anexo se refiere al caso de fallo del controlador de acceso y hace posible que las llamadas gestionadas continúen sin interrupción alguna.

Este procedimiento no trata todos los aspectos de fallo y recuperación de conexión basada en TCP en otros casos y topologías posibles. No obstante, en el futuro podrán tratarse casos adicionales de manera similar.

R.7.2 Alcance

Esta propuesta trata solamente las conexiones basadas en TCP (canales de señalización de llamada H.225.0 y de control de llamada H.245). Los canales UDP (RAS) no se tratarán puesto que sus situaciones de fallo ya se han tratado en el mecanismo de reintentos definido para canales UDP.

R.7.3 El procedimiento de robustez

Después de un fallo, la entidad H.323 restablecerá la conexión de señalización de llamada y enviará los mensajes INDAGACIÓN DE ESTADO y ESTADO a la otra entidad H.323. La otra entidad H.323 responderá con mensajes ESTADO, alcanzándose así un estado en el que ambos lados conocen el estado de llamada del otro. Si la entidad receptora no se entera de la llamada, deberá responder con un mensaje ESTADO con el IE CallState igual a NULL. La conexión de señalización de llamada debe establecerse a una de las entradas de **backupCallSignalAddresses** en un orden de preferencia definido por el orden de los elementos en la estructura **backupCallSignalAddresses**.

En el caso de que ambas entidades inicien simultáneamente la conexión de señalización de llamada, la entidad con el menor valor numérico del TransportAddress utilizado a partir de **backupCallSignalAddresses** cerrará la conexión TPC que abrió y utilizará la conexión abierta por el otro punto extremo. Para comparar los valores numéricos de TransportAddress de **backupCallSignalAddresses**, cada octeto de la dirección se comparará individualmente empezando por el primer octeto de la CADENA DE OCTETOS y continuando de izquierda a derecha en la CADENA DE OCTETOS hasta que se encuentren valores diferentes. La comparación se efectuará con el elemento de dirección de capa de red del TransportAddress de **backupCallSignalAddresses**, y si se ve que es igual, con el elemento de dirección (puerto) de transporte. Véase la figura R.1.

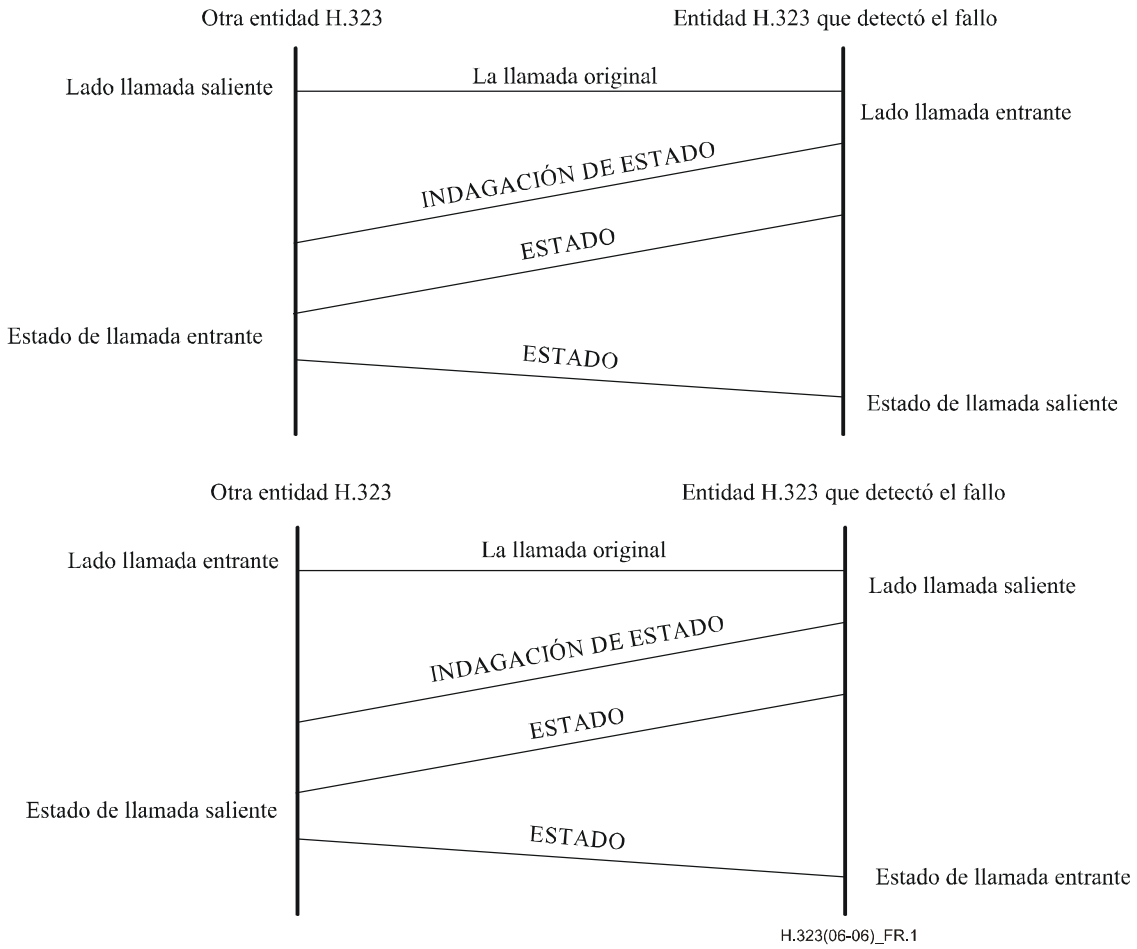


Figura R.1/H.323 – Procedimiento de robustez

Se cerrarán todas las conexiones anteriores que pudieran aún estar abiertas para la llamada, lo cual se aplica a la conexión de señalización de llamada y a la conexión de control de llamada.

Para facilitar la sincronización del estado de canales lógicos, pueden utilizarse los nuevos campos **IncludeFastStart** en los mensajes INDAGACIÓN DE ESTADO y **RobustnessFastStart** en ESTADO. El emisor del mensaje ESTADO debe incluir el campo **RobustnessFastStart** que contiene los canales entonces activos de recepción y transmisión con las direcciones de recepción para trenes de medios y de control de medios. El emisor de un mensaje INDAGACIÓN DE ESTADO puede solicitar la inclusión del campo **RobustnessFastStart** en el mensaje de ESTADO fijando el valor **IncludeFastStart** a TRUE.

Si una entidad intermedia necesita sincronizar el estado de canal lógico, debe enviar el mensaje INDAGACIÓN DE ESTADO a uno de los tramos de llamada, debe esperar el mensaje ESTADO con un campo comienzo rápido, debe emitir los mensajes ESTADO e INDAGACIÓN DE ESTADO al otro tramo de la llamada, debe esperar el mensaje ESTADO que contenga la información de canal lógico del segundo tramo y debe enviar el mensaje ESTADO al primer tramo de la llamada.

Este procedimiento se utiliza para sincronizar los estados de los canales lógicos abiertos que se abrieron mediante el procedimiento de comienzo rápido y de establecimiento de canal lógico H.245.

En las situaciones en que la llamada no haya alcanzado el estado activo antes del fallo, la llamada debe abandonarse.

Tanto la entidad H.323 que se recupera como su vecino de señalización deberán reiniciar implícitamente sus máquinas de estado H.245 para la llamada, debido a que la entidad que se recupera no se entera de las capacidades del terminal distante ni tiene conocimiento del resultado de las negociaciones MSD. Además, las capacidades de la entidad de recuperación pueden diferir de las de la entidad que falló. Antes de enviar mensajes H.245, ambas entidades deberán intercambiar mensajes TCS y efectuar la determinación del principal/subordinado.

R.7.4 Diagrama SDL para la máquina de estados del método A

Véase la figura R.2.

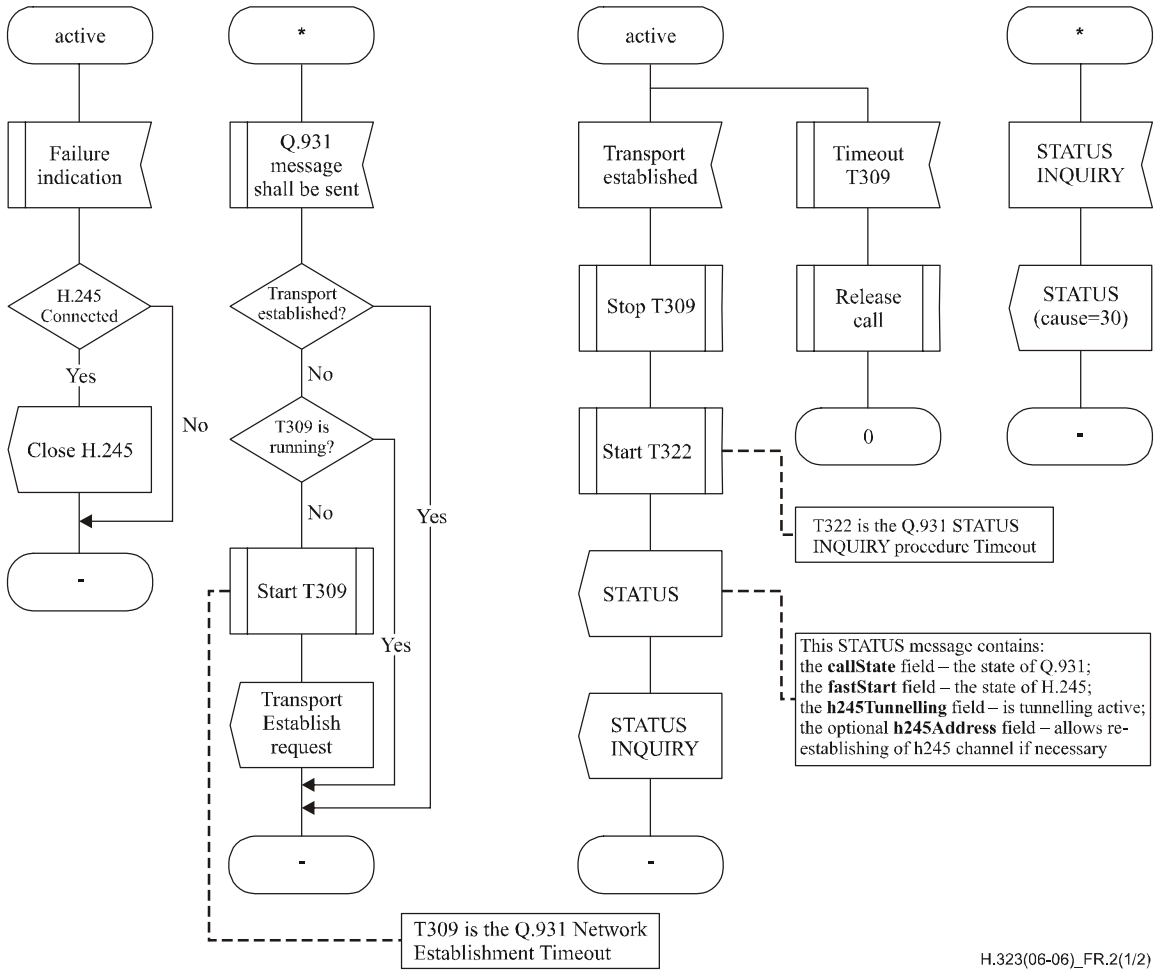


Figura R.2/H.323 – Máquina de estados del método A (*hoja 1 de 2*)

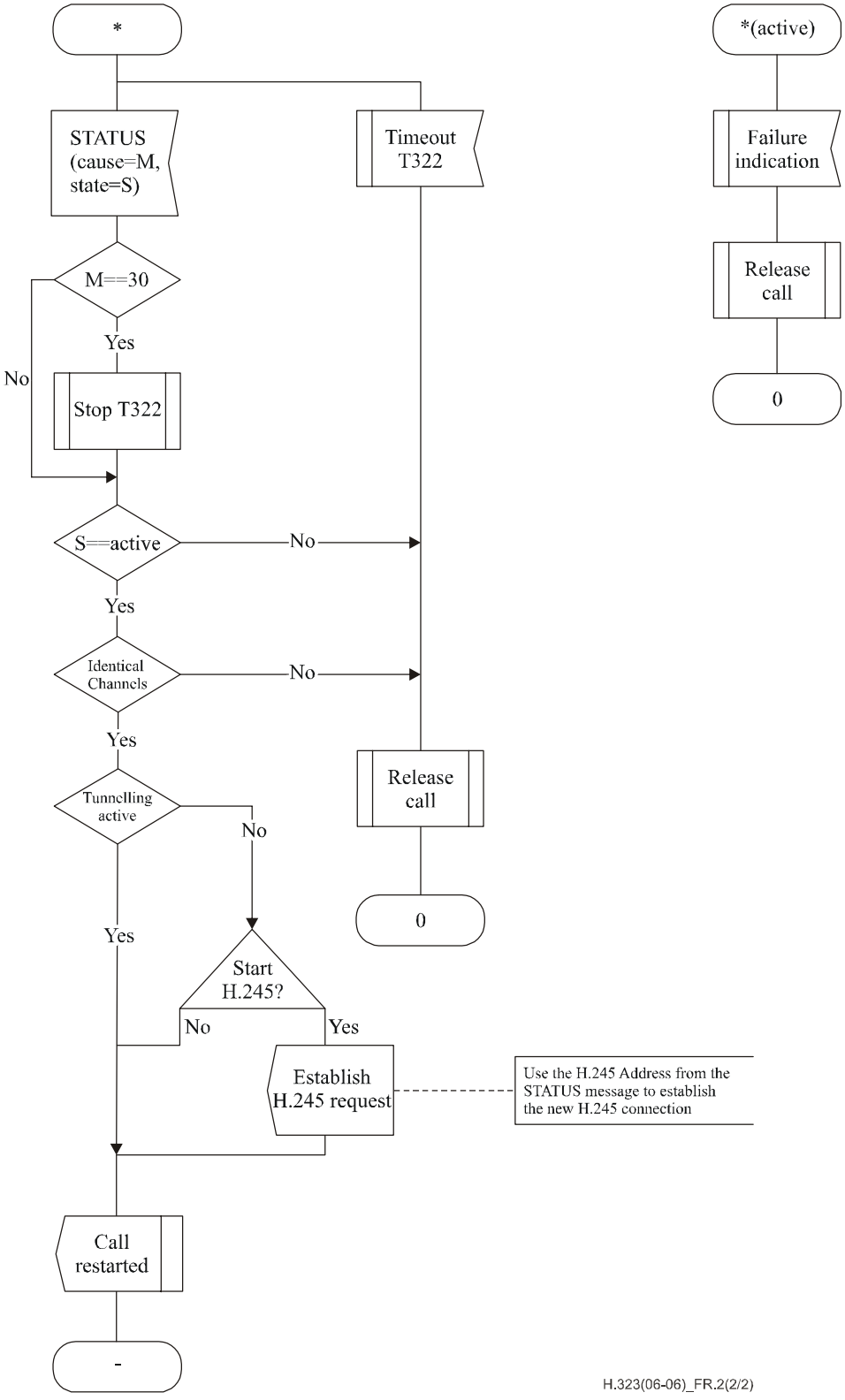


Figura R.2/H.323 – Máquina de estados del método A (*hoja 2 de 2*)

R.8 Método B: Recuperación de estado a través de un depositario compartido

Este método depende de una entidad o seudoentidad tolerante a los fallos y (si la entidad de seguridad requiere una dirección de señalización diferente) de un mecanismo para restablecer la señalización de llamada en la entidad de seguridad. Hay varias maneras de hacerlo. El mecanismo tolerante a los fallos no se normalizará en esta versión de esta Recomendación, pero sugeriremos

algunas soluciones. Podemos recomendar la normalización de la solución en una versión futura de esta Recomendación. Existen algunos protocolos IETF emergentes que pueden ayudar a resolver este problema, pero aún no se encuentran en un estado tal que puedan ser referenciados por H.323v4 (noviembre de 2000).

R.8.1 Plataforma tolerante a los fallos

Una solución es implementar la entidad robusta en una plataforma tolerante a los fallos que utilice soporte físico y soporte OS. Esta solución haría la recuperación de estado completamente transparente a la H.323. Si la plataforma también mantiene una dirección de transporte constante, es entonces una entidad virtual tolerante a los fallos, el canal de señalización no fallará y no se necesitan procedimientos a nivel de aplicación. Si cambia la dirección de transporte, se necesitará el mecanismo de esta cláusula.

R.8.2 Conglomerado tolerante a los fallos

Otra solución es establecer un conglomerado (dos o más) de entidades tándem no tolerantes a los fallos, que se comporten colectivamente como una seudoentidad tolerante a los fallos. Las entidades del conglomerado se arreglarían para compartir suficiente información de estado de llamada especificada para permitir a un par asumir el mando en caso de fallo de la entidad activa. Posibles soluciones podrían ser:

1) activo/reserva ("1+1");
2) reserva única compartida por varias entidades activas (la entidad de reserva comparte información de estado de compartición de reserva con cada entidad activa a la que pudiera sustituir) ("N+1");
3) y otras configuraciones.

Aunque la información de estado es compartida, lo que permite al conglomerado aparecer como una entidad virtual tolerante a los fallos, no será posible mantener una dirección de transporte de señalización de llamada constante, por lo cual, debe utilizarse uno de los mecanismos de R.8.3 para restablecer el canal de señalización de llamada.

Un problema clave del modelo de conglomerado es cómo compartir el estado. La información de estado debe ser sincronizada en momentos clave de la llamada, de modo que el sistema pueda con seguridad recurrir a ellos. Estos momentos se denominarán *puntos de verificación* (*checkpoints*). Esta Recomendación especifica los puntos de verificación y los datos mínimos que deben ser compartidos. En esta versión de esta Recomendación no sugerimos una solución normalizada de la compartición, pero en la Nota Informativa 2 de la cláusula R.13 consideraremos varias soluciones para ilustrar las ventajas prácticas de este modelo.

R.8.3 Restablecimiento de conexión de señalización de llamada

La compartición de direcciones de señalización de seguridad es la misma que en el método A. El restablecimiento de conexiones de señalización de llamada es similar pero presenta diferencias, pues la entidad de seguridad tiene suficiente información para restablecer la conexión en el segundo lado en lugar de esperar a que el otro vecino también detecte el fallo.

Cuando una entidad de seguridad toma el lugar de un par que ha fallado y recibe un mensaje en una nueva conexión, recuperará el estado de llamada (utilizando como clave el identificador de llamada), lo cual permitirá continuar soportando la llamada, incluida la señalización de encaminamiento, mantener la información de facturación, etc. Una entidad que detecte un fallo no restablecerá la conexión hasta que tenga un mensaje que enviar por la conexión. La entidad de seguridad tendrá canales nuevos para cada llamada utilizada por el par que falla, a menos que se hayan utilizado canales multiplexados. La política de restablecer solamente cuando sea necesario repartirá los restablecimientos en el tiempo.

La posibilidad de retrasar el restablecimiento hasta que se necesite el canal para un mensaje, y el hecho de que la entidad de seguridad posea suficiente información para establecer el nuevo canal en el otro lado, significa que no es necesario un mecanismo keepAlive en el método B.

Como tanto la entidad recuperada como su vecino de señalización pueden restablecer la conexión, existe una condición potencial de competición en velocidad, pero evitamos la necesidad de mensajes de mantenimiento en activo con las conexiones TCP. Como el tráfico es mayor en un sentido que en el otro y el restablecimiento se produce solamente cuando existe tráfico de mensaje, la condición de competición en velocidad será rara. Podemos resolver la condición de competición por los mismos métodos utilizados en el establecimiento de canal H.245. La entidad que tenga el menor valor numérico de la dirección h245 cerrará la conexión TCP que abrió y utilizará la conexión abierta por el otro punto extremo.

Para los canales de señalización multiplexados, la detección de un fallo en cualquier llamada implicará fallo del canal. Cuando se establece un nuevo canal, se utilizará para el mismo conjunto de llamadas que el canal que falla. Téngase en cuenta que esto implica que la lista de llamadas que comparten un canal debe formar parte de los datos compartidos entre una entidad y su entidad o entidades de seguridad, o entre entidades a través del depositario compartido. Después de un fallo, se restablece el canal multiplexado cuando hay un mensaje que enviar para cualesquiera de las llamadas que comparten el canal. Existe una condición de competición de velocidad similar a esa en los canales no multiplexados. Si se ve que dos canales de señalización tratan el mismo conjunto de llamadas o llamadas del mismo conjunto, se abandonará una conexión.

Si una entidad recibe una nueva conexión de señalización que incluye un identificador de llamada que concuerda con el de una conexión existente, verificará si la conexión proviene de la misma entidad que la conexión anterior o tiene la misma dirección de señalización de llamada de seguridad de esa misma entidad. Si se cumple una de esas condiciones, la entidad que recibe la nueva conexión considerará que la conexión anterior ha fallado y la cerrará.

R.8.4 Restablecimiento de conexión H.245

Una vez que se ha restablecido el canal de señalización de llamada y que el procedimiento de robustez ha alcanzado un estado estable, si se utilizaba tunelización H.245, las entidades pueden continuar tunelizando mensajes utilizando el nuevo canal de señalización de llamada.

Si se estaba utilizando una conexión H.245 separada, puede que haya fallado sola o junto con el canal de señalización de llamada. Si la entidad ha detectado fallo en un canal H.245, abandonará su conexión sin cerrarla (sin enviar la instrucción EndSessionCommand, que indicaría al otro extremo la finalización de la llamada). Intentará entonces establecer una nueva conexión enviando su dirección h245 en un mensaje Facilidad a su vecino de señalización. Una entidad que recibe Facilidad con una dirección h245 en una llamada para la que ya posee un canal H.245 (que posiblemente, haya fallado sin haber sido detectado) cerrará el canal existente y abrirá uno nuevo. Ninguna de las dos entidades aplicará procedimientos de inicialización H.245 (determinación de principal-subordinado e intercambio de capacidad de terminal) para el nuevo canal.

La entidad de recuperación puede tener un conjunto de capacidades distinto del de la entidad averiada. En este caso, especialmente cuando se hubieran iniciado los procedimientos H.245 entre los vecinos de señalización, las entidades deben reiniciar sus máquinas de estado H.245 y comenzar de nuevo. Esto se realiza mediante la bandera **resetH245** en los datos de robustez ESTADO. Una vez transmitida esta bandera, las entidades deben proceder al intercambio de los mensajes TCS y MSD.

R.8.5 Datos compartidos a través de un depositario compartido

Como mínimo, deben compartirse los datos siguientes a través de un depositario compartido:

1) backupCallSignallingAddresses;
2) hasSharedRepository;
3) identificador de llamada (callIdentifier);
4) estructuras OpenLogicalChannel, de H.245 o Comienzo rápido (fastStart).

Pueden compartirse datos adicionales para soportar la recuperación de llamadas inestables o permitir la recuperación de datos adicionales que cambian durante llamadas estables (por ejemplo, registros de detalles de llamada, datos de temporización de llamada, datos de facturación, testigos de autorización).

R.8.6 Puntos de verificación

En esta versión de esta Recomendación mantenemos solamente las llamadas que están en el estado estable. Por tanto, sólo se necesita un punto de verificación cuando se entra en el estado estable. Así ocurre cuando se ha enviado o recibido Conexión y se han establecido canales de medios en ambos sentidos (mediante procedimientos H.245 o de conexión rápida).

Las entidades pueden utilizar puntos de verificación adicionales para soportar la recuperación de llamadas inestables o permitir la recuperación de datos adicionales que puedan cambiar durante llamadas estables.

R.9 Interfuncionamiento entre métodos de robustez

Los vecinos de señalización deben acordar un método de robustez que será utilizado entre ellos. **No** es necesario que se utilice el mismo método de extremo a extremo.

El soporte de robustez (cualquier método) es indicado por la entidad del lado origen incluyendo el campo RobustnessGenericData en Establecimiento. Además, es indicado por el soporte del método B (depositario compartido) el campo hasSharedRepository de Establecimiento. La entidad de lado terminación indica su soporte de robustez y del método B mediante los mismos campos de Conexión. La selección del método A o del método B se indica en la cláusula R.10, Procedimientos para la recuperación.

Si una entidad que encamina señalización de llamada soporta el método B (tiene un depositario compartido), puede ser necesario utilizar el método B en una conexión y el método A en la otra para la misma llamada. En este caso, sigue las reglas indicadas en la cláusula R.10 independientemente en las dos conexiones. Si una entidad de seguridad con un depositario compartido recibe una Indagación de estado, puede responder con Estado utilizando la información del depositario compartido.

R.10 Procedimientos para la recuperación

1) Si el vecino no soporta el método B (depositario compartido) y se utiliza señalización TCP, se utilizarán entonces los StatusInquiry keepAlives. Si la entidad tiene un depositario compartido (incluso si el vecino no lo tiene) enviará periódicamente Indagación de estado (StatusInquiry). Si la entidad no tiene un depositario compartido, sólo la entidad más próxima a la parte llamada enviará periódicamente StatusInquiry.
2) Si una entidad tiene un mensaje que enviar por un canal de señalización de llamada (incluido un keepAlive StatusInquiry) y detecta fallo, intentará establecer un canal con la primera dirección en backupCallSignalAddresses (entidad de seguridad).
3) Después de que un canal de señalización de llamada está restablecido, si el vecino no tiene depositario compartido, se utilizará el método A y la entidad que establece enviará Estado (con el campo fastStart) antes del mensaje en espera de envío.

4) La entidad que establece la conexión puede también enviar un mensaje Indagación de estado antes del mensaje, si desea auditar la consistencia del estado.

5) Si una entidad con depositario compartido recibe StatusInquiry, enviará una StatusInquiry a su vecino del otro lado para recuperar la información de estado necesaria (incluidos datos fastStart), a menos que mantenga todos esos datos en su depositario.

6) Si una entidad que no tiene depositario compartido recibe una StatusInquiry, esperará hasta que recibe un Status de su vecino del otro lado (enviando StatusInquiry, si es necesario, al otro vecino, si el canal de señalización del otro lado está disponible).

R.10.1 Procedimientos de recuperación con valores CRV en conflicto

Es posible que en el momento del fallo, la entidad activa y su par de respaldo se encuentren llamando simultáneamente al mismo vecino de señalización. En tal caso existe la distante posibilidad de que estas dos llamadas utilicen los mismos valores CRV con el vecino de señalización y que el par de respaldo no sea capaz de continuar la llamada de la entidad averiada con el mismo CRV. En tal caso se requiere la asignación de un nuevo CRV y su comunicación al vecino de señalización.

Si la entidad averiada implementa el método A, el vecino de señalización restablece una conexión de señalización de llamada con la entidad de respaldo de la entidad averiada. A continuación el vecino de señalización enviará mensajes Indagación de Estado y Estado a la entidad de respaldo. No obstante, antes del envío de los mensajes Indagación de Estado y Estado, la entidad deberá comprobar si se trata de la que originó la llamada (o sea del lado llamante) y si se han cursado previamente llamadas a la entidad de respaldo. Si el vecino de señalización se encuentra en el lado llamante y ha cursado previamente llamadas a la entidad recuperada como muestra la figura R.3, el vecino de señalización asignará un nuevo valor CRV único a esta llamada a la entidad recuperada y lo utilizará (en el IE CRV) en la subsiguiente señalización de llamada H.225.0 y en los mensajes RAS. La entidad recuperada asignará un valor CRV único a esta llamada y lo utilizará en su comunicación con el controlador de acceso. Si el vecino de señalización se encuentra en el lado llamado y ha recibido llamadas previas de la entidad recuperada como se representa en la figura R.4, la entidad asignará un nuevo valor CRV único en el mensaje Indagación de Estado con bandera CRV = 1 porque se encuentra en el lado de destino de la llamada. La entidad recuperada adoptará este nuevo CRV para la llamada. Los mensajes subsiguientes de señalización de llamada H.225.0 correspondientes a esta llamada utilizarán este nuevo valor CRV. La entidad recuperada, cuando sea necesario, asignará un único valor CRV a esta llamada a fin de utilizarlo en los mensajes RAS.

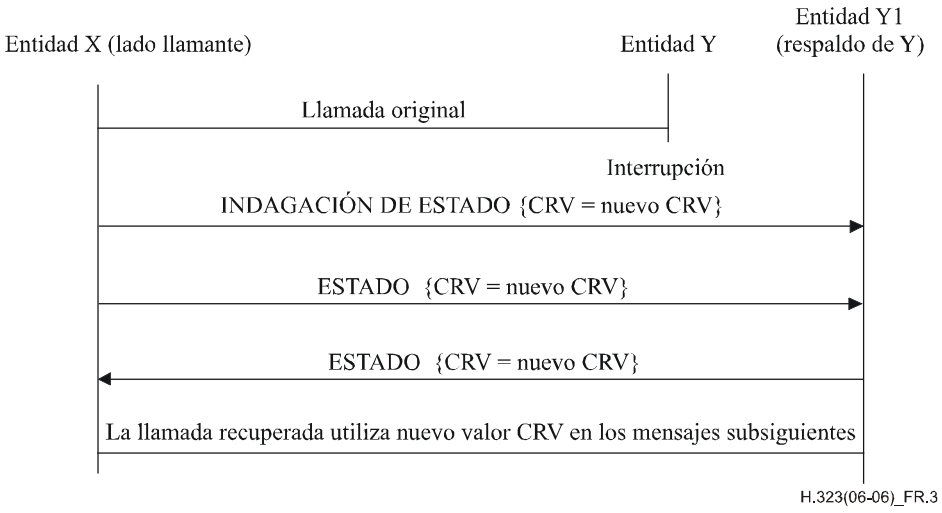


Figura R.3/H.323 – La entidad averiada utiliza el método A y está en el lado llamado

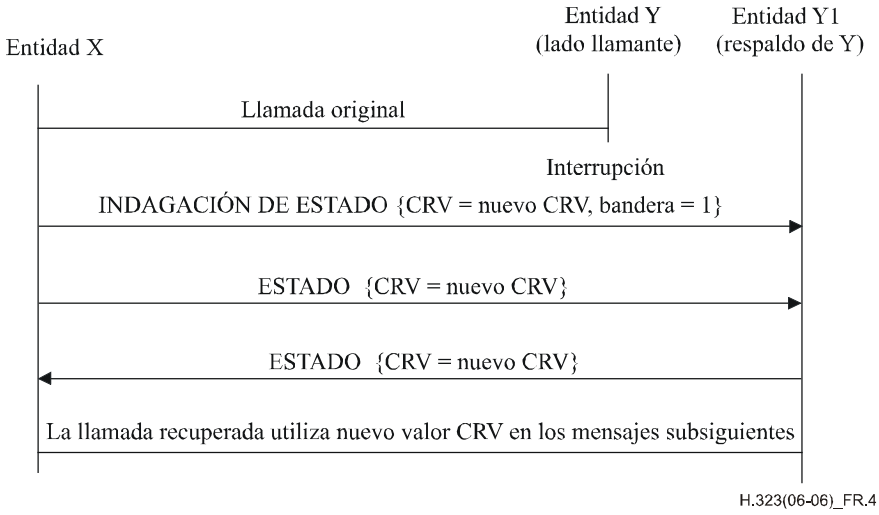


Figura R.4/H.323 – La entidad averiada utiliza el método A y está en el lado llamante

Si la entidad averiada implementa el método B, el vecino de señalización o la entidad de respaldo de la entidad averiada pueden restablecer la conexión de la señalización de llamada. Independientemente de qué entidad restablezca la conexión de señalización de llamada, antes de enviar mensajes de señalización de llamada H.225.0, la entidad deberá comprobar si se trata de la que originó la llamada (es decir la del lado llamante) y si ya ha recibido llamadas anteriores a la entidad recuperada. Si la entidad que restablece la conexión se encuentra en el lado llamante y ha cursado llamadas previas al vecino de señalización como se representa en la figura R.5, la entidad deberá asignar un nuevo valor CRV a esta llamada y utilizarlo en la subsiguiente señalización de llamada H.225.0 y en los mensajes RAS. El vecino de señalización asignará un valor CRV único a esta llamada y lo utilizará en los mensajes RAS y en su comunicación con el controlador de acceso. Si la entidad que restablece la conexión se encuentra en el lado llamado y tiene llamadas previas procedentes de la entidad vecina de señalización como se representa en la figura R.6, la entidad deberá asignar un nuevo valor CRV único y utilizarlo en un mensaje de señalización de llamada H.225.0 con la bandera CRV = 1 porque éste es el lado de destino de la llamada. La entidad vecina de señalización deberá adoptar este nuevo CRV para la llamada. Los mensajes subsiguientes de señalización de llamada H.225.0 correspondientes a esta llamada deberán utilizar este nuevo valor CRV. La entidad vecina de señalización, cuando sea necesario, deberá asignar un único valor CRV a esta llamada a fin de utilizarlo en los mensajes RAS.

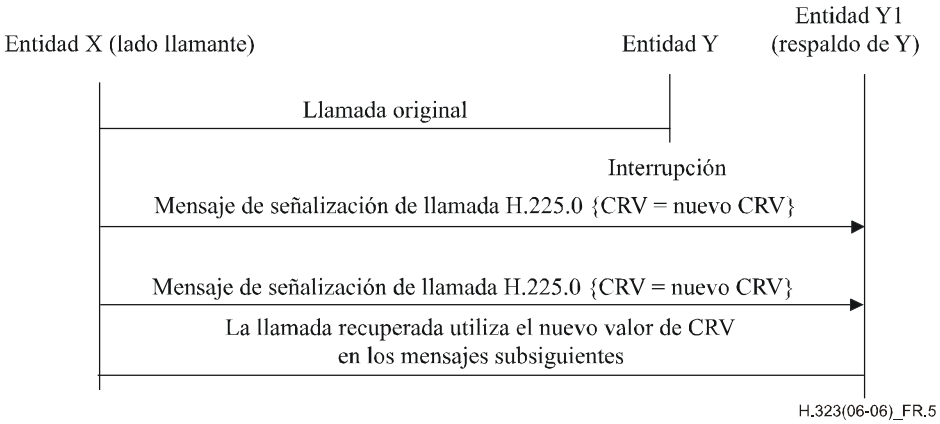


Figura R.5/H.323 – La entidad averiada utiliza el método B y se encuentra en el lado llamado y la entidad que sobrevive inicia el restablecimiento

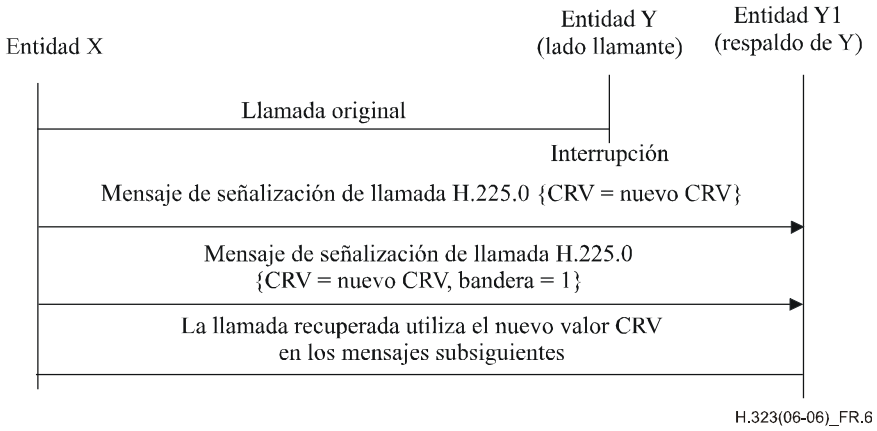


Figura R.6/H.323 – La entidad averiada utiliza el método B y se encuentra en el lado llamante mientras que la entidad que sobrevive inicia el restablecimiento

R.11 Utilización de GenericData (datos genéricos)

Los campos de datos necesarios para implementar las características de este anexo son transportados en los campos de datos genéricos de los diferentes mensajes, como se define a continuación. Los `datos de robustez` (`RobustnessData`) serán codificados y los datos binarios resultantes serán transportados como un ejemplar sin procesar de datos genéricos en los mensajes especificados.

```
RobustnessData ::= SEQUENCE
{
     versionID          INTEGER (1..256),
     robustnessData     CHOICE {
          rrqData            Rrq-RD,
          rcfData            Rcf-RD,
          setupData          Setup-RD,
          connectData        Connect-RD,
          statusData         Status-RD,
          statusInquiryData  StatusInquiry-RD,
          ...
     },
     ...
}

BackupCallSignalAddresses ::= SEQUENCE OF CHOICE {
     tcp                TransportAddress,
     alternateTransport AlternateTransportAddresses,
     ...
}

Rrq-RD ::= SEQUENCE
{
     backupCallSignalAddresses   BackupCallSignalAddresses,
     hasSharedRepository         NULL OPTIONAL,
     ...
}

Rcf-RD ::= SEQUENCE
{
     hasSharedRepository     NULL OPTIONAL,
     ...,
```

```
    irrFrequency            INTEGER (1..65535) OPTIONAL     -- in seconds;
                                                            -- not present
                                                            -- if GK does not
                                                            -- want IRRs for
                                                            -- recovered calls
}

Setup-RD ::= SEQUENCE
{
    backupCallSignalAddresses   BackupCallSignalAddresses,
    hasSharedRepository         NULL OPTIONAL,
    endpointGuid                GloballyUniqueIdentifier OPTIONAL,
    ...
}

Connect-RD ::= SEQUENCE
{
    backupCallSignalAddresses   BackupCallSignalAddresses,
    hasSharedRepository         NULL OPTIONAL,
    endpointGuid                GloballyUniqueIdentifier OPTIONAL,
    ...
}

Status-RD ::= SEQUENCE
{
    h245Address   TransportAddress OPTIONAL,
    fastStart     SEQUENCE OF OCTET STRING OPTIONAL,
    ...,
    resetH245     NULL OPTIONAL
}

StatusInquiry-RD ::= SEQUENCE
{
    h245Address        TransportAddress OPTIONAL,
    timeToLive         TimeToLive OPTIONAL,
    includeFastStart   NULL OPTIONAL,
    ...
}
```

El GenericIdentifier será 1:

```
robustnessId GenericIdentifier ::= standard:1
```

Además, se incluirá un featureDescriptor que transporta el robustnessId en las desiredFeatures de los mensajes especificados a continuación.

R.11.1 Utilización de GenericData en los mensajes H.225.0

RRQ, RCF, ARQ, ACF, Establecimiento, Conexión, Estado e Indagación de Estado deberán incluir datos de robustez en datos genéricos con arreglo a las correspondientes definiciones de datos de los respectivos mensajes.

Todos los mensajes (RRQ, RCF, ARQ, ACF, Establecimiento y Conexión) salvo Estado e Indagación de Estado deberán incluir la FeatureDescr de robustez en desiredFeatures de featureSet. Obsérvese que las desiredFeatures no se encuentran en el featureSet de Establecimiento.

La versión de estos datos (campo versionID de RobustnessData) deberá ponerse a 1.

R.12 Nota Informativa 1: Antecedentes de los métodos de robustez

Esta cláusula describe los tipos de fallo de sistema y tipos de robustez desde un punto de vista general. No todos los fallos de sistema que aquí se describen son tratados mediante métodos de robustez en la actual versión de este anexo. Se ofrece esta visión más general para dar contexto a los

métodos actualmente definidos y ayudar al lector a entender qué tipos de fallo de sistema son tratados aquí. También sirve como lista de fallos que podrían tratarse en versiones futuras del anexo.

R.12.1 Tipos de métodos de robustez

Puede proporcionarse robustez de sistema de varias maneras:

1) métodos de redundancia de soporte físico/sistema operativo (posiblemente incluyendo varias tarjetas NIC);
2) entidades en tándem;
3) entidades virtuales.

R.12.2 Entidades robustas

Las entidades a considerar para la robustez incluyen esencialmente todas las entidades H.323:

1) controladores de acceso;
2) elementos de frontera;
3) controladores multipunto;
4) posibles procesadores multipunto (para el fallo de trenes de medios);
5) pasarelas (incluidas pasarelas IP a IP);
6) mandatarios cortafuegos; y
7) ciertos tipos de puntos extremos.

No todos los modelos de robustez son adecuados para todos los componentes de sistema.

R.12.3 Alcance de un sistema robusto

El alcance de robustez o la parte de un sistema que implementa robustez puede incluir uno o varios de los siguientes aspectos:

1) zonas H.323 (intrazona, con uno o varios controladores de acceso);
2) intradominio H.323 (intradominio, interzona con varios controladores de acceso);
3) interdominio H.323 (interdominio, con varios controladores de acceso y elementos de frontera).

R.12.4 Terminación y fallos de sistema

Debe proveerse una terminación de sistema ordenada (tal como un MC que abandona una conferencia) así como un fallo de sistema. La terminación ordenada permite, en principio, al punto extremo de terminación notificar a sus pares, simplificando así la detección, pero también requiere mecanismos adicionales o ligeramente diferentes. Obsérvese que la notificación puede fallar debido a pérdida de paquetes repetida, de manera que la frontera con los fallos de sistema es casi imperceptible.

En las cláusulas siguientes se trata el tema de los aspectos de fallo de sistema.

R.12.4.1 Tipos de fallos

Los métodos descritos en este anexo tratan solamente con fallos que puedan ser detectados desde el punto de vista de un protocolo "en línea". El fallo de un procesador en un sistema de multiprocesador con memoria compartida no es visible desde el exterior, por lo que no se trata en estos métodos. En cambio, el fallo de una tarjeta NIC requiere la utilización de una dirección de transporte diferente, por lo cual es visible y debe tratarse. Los siguientes tipos de fallos serán visibles a los vecinos de señalización y son objetivos de este trabajo:

1) fallo total de un componente del sistema (fallo de alimentación eléctrica, fallo total del soporte lógico);
2) fallo parcial de un componente del sistema (fallo de una de las varias interfaces de comunicación);
3) fallo total del enlace de red (un componente del sistema ha dejado de ser accesible); y
4) fallo parcial del enlace de red (no todos los componentes del sistema son accesibles entre sí, pero algunos pueden aún comunicarse, incluido, en particular, la conectividad parcial y el fallo de media conexión).

Debe señalarse que algunos de estos fallos pueden no sólo ser difíciles de detectar (simétricamente) sino también no distinguirse entre sí (véase más adelante).

5) Ataques malintencionados al sistema deben considerarse en el contexto de los trabajos de seguridad H.323.

R.12.4.2 Detección de fallo

1) Tiempo para detectar un fallo.
2) Formas de detectar un fallo (vigilancia permanente explícita o detección al invocarse una función).
3) Entidades responsables de/o que intervienen en la detección de un fallo.
4) Aparición de un fallo a un componente de sistema o a un conjunto de componentes de sistema.
5) Posibilidad de determinar el tipo de fallo.
6) Coherencia/temporización de la detección de fallos entre los diferentes componentes de un sistema.
7) La detección de fallo puede no ser transitiva, es decir, de "A puede/no puede hablar con B" y "B puede/no puede hablar con C" no puede deducirse necesariamente que "A puede/no puede hablar con C".
8) ¿Cuánta tara es aceptable?

R.12.4.3 Tratamiento de un fallo

1) Tiempo hasta la reparación.
2) Entidad que inicia el proceso de reparación.
3) Posibilidad de reparar el fallo.
4) Consecuencias si no puede repararse el fallo.
5) Cómo asegurar el tratamiento coherente de un fallo por todas las entidades que intervienen.
6) ¿Cómo tratar las opiniones/detecciones de fallos divergentes por diversos componentes (fallan o no)?
7) ¿Cómo tratar la diferente temporización de la detección de fallos?
8) ¿Cómo tratar con estado incoherente cuando se trata un fallo?
9) ¿Cómo tratar los vacíos de información de estado cuando se trata un fallo?

10) Consecuencias sobre la operación total del sistema (por ejemplo, una llamada saliente).

11) ¿Cuánta tara es aceptable?

12) ¿Cómo tratar con múltiples fallos simultáneos?

R.12.4.4 Escenarios de fallo

Esta cláusula enumera muchos escenarios de fallo identificados para los sistemas H.323. Los métodos de robustez del presente anexo no permiten la recuperación tras todos estos fallos, pero se enumeran para tener una visión completa y para dar contexto a los fallos cubiertos por los métodos de robustez.

1) (Controlador de acceso – punto extremo): sin relación aún, o sin más relación.

2) (Controlador de acceso – punto extremo): descubierto pero no registrado.

3) (Controlador de acceso – punto extremo): descubierto y registrado.

4) En el proceso de establecimiento de la comunicación:
   a) directo;
   b) encaminado por controlador de acceso.

5) Durante una llamada/conferencia: Rec. UIT-T D.160: "estado estable" – discutir lo que esto significa para los diversos protocolos:
   a) directo;
   b) encaminado por controlador de acceso.

6) En el proceso de liberación de llamada:
   a) directo;
   b) encaminado por controlador de acceso.

Considerar las implicaciones resultantes de los diversos nuevos protocolos que se desarrollan actualmente (familia de la serie H.450.x, anexo K, anexo L de esta Recomendación, etc.).

Considerar los trenes de medios así como las relaciones RAS/señalización de llamada/comunicación de control de conferencia.

R.13 Nota Informativa 2: Compartición de estado de llamada entre una entidad y su par de seguridad

Esta nota sugiere modos de implementar la compartición de estado de llamada entre una entidad y otra que le sirve como par de seguridad. La selección de un método no forma parte de esta Recomendación. Como el método no está normalizado, es posible que pares provenientes de diferentes vendedores puedan no ser adecuados como pares de seguridad robustos.

R.13.1 Memoria compartida

Si los miembros de un mismo conglomerado están físicamente localizados en la misma habitación, pueden utilizar un dispositivo de memoria compartido (o reflectivo). Este caso es similar al de muchas plataformas tolerantes a los fallos, pero en donde se puede simplemente escribir en una memoria compartida en cada punto de control en lugar de utilizar un sistema operativo tolerante a los fallos.

R.13.2 Disco compartido

Si los miembros del conglomerado están ubicados físicamente cerca unos de otros, pueden utilizar un disco compartido y escribir la información de estado en cada punto de verificación.

R.13.3 Paso de mensaje

La entidad activa puede enviar un mensaje actualizando el estado compartido a cada uno de los demás miembros del conglomerado en cada punto de verificación. Se implementa así una memoria compartida distribuida, conocida también como *boletín*. Los mensajes pueden enviarse utilizando diferentes mensajes UDP, mensajes multidifusión, enlaces TCP persistentes o protocolos de paso de mensajes tolerantes a los fallos tales como el ASAP (que soporta un mecanismo de multidifusión de envío al grupo que no requiere IP de multidifusión). Este aspecto se discute con más detalle en APC-1772, donde se sugieren algunos puntos de verificación.

R.13.3.1 SCTP/ASAP

Esta cláusula ilustrará, con un ejemplo de llamada H.323, la utilización de ASAP y SCTP con fines de robustez en un sistema H.323. Incluirá en resumen:

1) una sinopsis arquitectural de un sistema H.323 que utiliza ASAP/SCTP;
2) una visión de las pilas de protocolos necesarias en los respectivos nodos H.323; y
3) escenarios de reparación de fallos en un ejemplo de llamada H.323 con dos controladores de acceso y dos puntos extremos.

R.13.3.1.1 Referencias

[R.13-1] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

[R.13-2] STEWART (R.) *et al*.: *Aggregate Server Access Protocol (ASAP)*, <draft-ietf-rserpool-asap-14.txt>, IETF, octubre de 2006.

[R.13-3] XIE (Q.) *et al*.: *Endpoint Name Resolution Protocol (ENRP)*, <draft-ietf-rserpool-enrp-08.txt>, IETF, junio de 2004.

R.13.3.1.2 Pilas de protocolos

En general, una aplicación H.323 que utilice ASAP/SCTP [R.13-1] a [R.13-3] para la tolerancia de fallos tendrá la siguiente pila de protocolos:

H.323(06-06)_FR.13.3.1.2

Esto puede permitir la reparación rápida de fallos, transparente a la aplicación de capa superior, tanto a nivel de conexión como de sesión:

1) nivel de enlace (SCTP) – soporte multibuscador, supervivencia a fallos de red;
2) nivel de sesión (ASAP) – soporte de fondo común servidor (2N, N+K, etc.), supervivencia a fallos de proceso/nodo.

Además, el ASAP proporciona:

- transparencia de ubicación;
- compartición de carga;
- enchufe activo, es decir alta escalabilidad;
- evita un punto de fallo individual.

R.13.3.1.3 Visión arquitectural de un sistema H.323

La figura R.7 presenta un sistema H.323 construido sobre la base del modelo ASAP/SCTP.

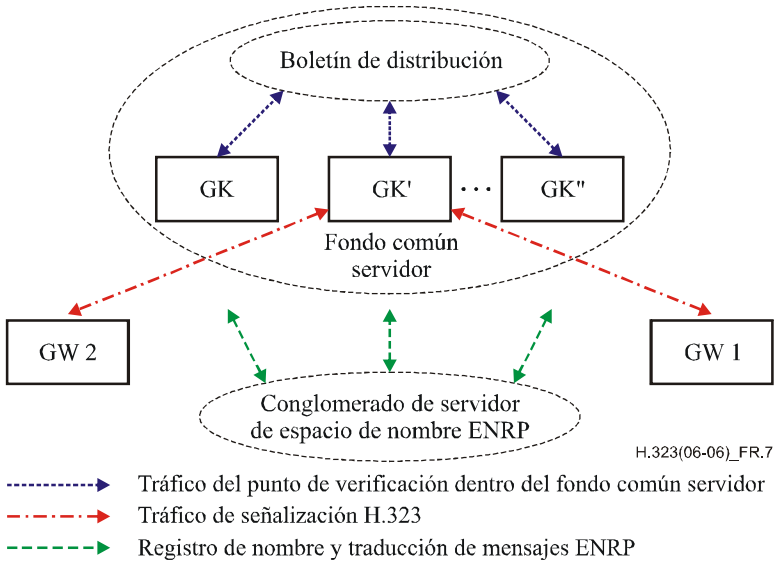


Figura R.7/H.323 – Sistema H.323 construido sobre la base del modelo ASAP/SCTP

En este sistema, todos los componentes H.323, incluidos los GW 1, GW 2 y los GK utilizan las pilas ASAP/SCTP que se muestran en la cláusula anterior. En este ejemplo, suponemos que el controlador de acceso H.323 se implementa como un fondo común servidor (la figura representa las interioridades de este fondo común servidor), mientras que las pasarelas pueden o no implementarse como fondo común servidor.

Como se muestra en la figura, dentro del fondo común servidor del controlador de acceso existen múltiples ejemplares de controladores de acceso H.323 funcionalmente idénticos, GK, GK', ... GK". Los ejemplares GK comparten entre sí información de estado de llamada y otra información crítica de recuperación de llamada mediante un boletín de distribución interna. El mecanismo y la implementación de este boletín es específico del vendedor, por lo que se sale del alcance del ASAP o SCTP (este boletín puede, sin embargo, utilizar ASAP/SCTP para mejorar la tolerancia a los fallos y la escalabilidad).

Todos los nodos ASAP/SCTP, incluidos los GW y los GK, se basan en un único conglomerado servidor de espacio de nombre ENRP o en un grupo de conglomerados ENRP conectados, para el registro de nombre y los servicios de traducción de nombres [R.13-2]. Para formar el fondo común servidor de controlador de acceso, todos los ejemplares GK se registran en el espacio de nombre ENRP bajo el mismo nombre. No obstante, cada ejemplar GK puede registrarse con una capacidad de tratamiento de carga diferente.

El ASAP entregará cada mensaje de llamada H.323 a uno de los ejemplares GK en el fondo común servidor. La selección del ejemplar GK receptor se hace sobre la base de la política de compartición de carga en vigor y la situación en ese momento de cada ejemplar GK en el fondo común. Algunas veces es muy deseable que todos los mensajes de señalización H.323 relacionados con una llamada

sean tratados por el mismo ejemplar GK durante el ciclo de vida completo de la llamada, y sólo dejar que otro ejemplar GK pueda relevarlo solamente en caso de desaparición total de la original. Denominamos esta relación entre la llamada y el ejemplar del servidor "vínculo holgado". El ASAP ha sido diseñado para soportar muy fácilmente este tipo de relaciones de "vínculo holgado" [R.13-2] y [R.13-3].

Además, cuando un ejemplar GK está tratando una llamada, debe publicar en el boletín distribuido (por ejemplo, en el "punto de verificación") toda la información crítica de estado de llamada, cada vez que la llamada alcanza una cierta fase de su ciclo de vida. Esta información ayudará al ejemplar GK alternativo a recuperar la llamada en caso de que el ejemplar original que le trata falle totalmente.

R.13.3.1.4 Ejemplo de llamada H.323

Para los fines de descripción de una llamada se utilizarán los flujos de señalización de la figura R.8.

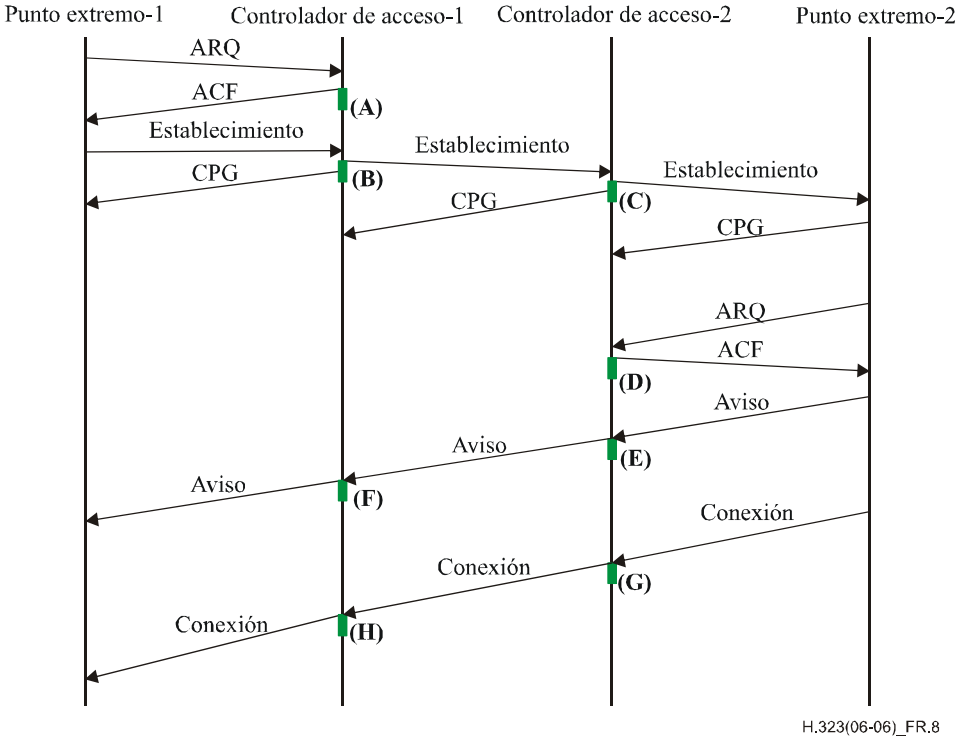


Figura R.8/H.323 – Ejemplo de llamada H.323

Hay que tener en cuenta que las referencias en este flujo de llamadas son bastante antiguas y que se ha extrapolado el segundo controlador de acceso. Pueden existir algunas diferencias con respecto al modo en que la actual especificación H.323 tendría un flujo de llamada, pero lo que importa aquí es resaltar cómo se utilizaría el ASAP/SCTP. Aun si algunos detalles pequeños son incorrectos en la figura anterior, esto no invalida el ejemplo.

R.13.3.1.4.1 Descripción general

La llamada se inicia con una solicitud de anchura de banda por parte del punto extremo-1, que en este caso utiliza el ASAP para solicitar a un controlador de acceso, conocido por un nombre o posiblemente por un puerto y dirección IP. En ambos casos, una demanda de traducción de nombre ENRP (que no se muestra en la figura) propagará al punto extremo el conjunto de todos los controladores de acceso (primarios y redundantes) en el fondo común servidor. Esta información será almacenada en una memoria caché local de la capa ASAP en el punto extremo-1, para su futura referencia en caso de fallo. Este mismo tipo de memoria caché aparecerá en todos los puntos

extremos ASAP en la cadena transparente a la llamada. Hay que tener en cuenta que la memoria caché es una característica opcional. Al tratarse de una opción, los puntos extremos que no la utilicen pueden aún obtener un controlador de acceso alternativo, y se necesitaría una solicitud adicional al servidor ENRP en el momento de detección de fallo.

Llegamos ahora al punto (**A**), paso en el que el controlador de acceso atribuye anchura de banda y verifica este mensaje de información de utilización de anchura de banda en un área del "boletín", área que puede ser cualquiera de las siguientes:

- una parte de memoria distribuida compartida, mantenida por un subsistema separado;
- una parte de memoria reflectiva, específicamente construida con este fin;
- una base de datos comercial distribuida;
- alguna otra invención creativa.

Debe advertirse ahora que lo importante aquí es que, de alguna manera los controladores de acceso redundantes/pares posean un mecanismo de compartición de estado de llamada. Pueden utilizar todos los mecanismos existentes, o que existirán en el futuro, de compartición de llamada.

El controlador de acceso-1 ocupa su estado relacionado ARQ y pone esta información en el "boletín", y responde a la petición con un ACF.

El punto extremo-1 reacciona y envía el mensaje Establecimiento al controlador de acceso-1, que selecciona el siguiente controlador de acceso, controlador de acceso-2, y reenvía su establecimiento, haciendo llegar la información de estado de llamada (al punto (**B**)), posiblemente relacionada de alguna manera con la información anterior (quizás con alguna forma de referencia cruzada, es decir, la llamada X está utilizando la anchura de banda Y representado por la información ARQ). Después de depositar la información en el punto (**B**), el controlador de acceso-1 envía el mensaje de llamada en curso al punto extremo-1.

El controlador de acceso-2 recibe el mensaje de establecimiento de su controlador de acceso par y selecciona el punto extremo de destino, reenviando el establecimiento y depositando la información de estado de la llamada en el punto (**C**). A continuación, envía un mensaje de llamada en curso al controlador de acceso-1.

Cuando el punto extremo-2 recibe el establecimiento, envía un mensaje de llamada en curso y solicita a su controlador de acceso anchura de banda dentro de su propio mensaje ARQ.

Esto hace que el controlador de acceso-2 asigne anchura de banda, deposite información de estado en el punto (**D**) y envíe el mensaje ACF. El punto extremo-2, al recibir este mensaje, envía un mensaje Aviso al controlador de acceso-2.

El controlador de acceso-2 al recibir el mensaje de aviso, depositaría una pequeña actualización en su boletín (punto (**E**)), es decir, informa de que la llamada está en Aviso, y reenvía el mensaje Aviso al controlador de acceso-1.

El controlador de acceso-1 repetirá el procedimiento, actualizando su información de estado en el punto (**F**) y reenviando el mensaje de aviso.

El punto extremo-2 responde a la llamada, enviando un mensaje Conexión al controlador de acceso-2, que depositará otra pequeña actualización del estado en el punto **G**, indicando que la llamada se encuentra ahora en estado de respondida y reenvía el mensaje de conexión al controlador de acceso-1.

El controlador de acceso-1, al recibir el mensaje Conexión, repetirá la operación, registrando su estado en el punto (**H**) y enviando el mensaje de conexión al punto extremo-1.

R.13.3.1.4.2 Escenarios de fallo

Las anteriores descripciones suponen el máximo nivel de redundancia y de mantenimiento de estado/llamada. En este contexto, todo fallo de un controlador de acceso es transparente a ambos puntos extremos. Si se produce un fallo, el mensaje sería reencaminado por ASAP a una entidad alternativa. Esta entidad necesitaría emprender las acciones siguientes para todo mensaje que reciba, que no incluya un objeto/bloque de llamada para:

- encontrar la llamada en el "boletín";
- depositar la información de estado y construir un bloque u objeto de control de llamada a llamada;
- continuar procesando el mensaje en nombre del par desaparecido.

Los puntos extremos son entonces completamente transparentes a los escenarios de fallo. No se almacena ningún tipo de conocimiento para recuperar un fallo de controlador de acceso en el punto extremo en sí (que no sea el ASAP).

R.13.3.1.4.3 Aspectos del mantenimiento de estado

Como antes se ha dicho, este ejemplo supone un modelo de mantenimiento máximo de estado. En este modo, las actualizaciones de estado deberían reducirse a la menor cantidad de información posible. En particular, el estado debe ser limitado al menor conjunto de información necesario para reconstruir la llamada Y las actualizaciones deben ser lo más pequeñas posible. En algunos casos un operador puede no querer tener este nivel de redundancia. Para conseguir un sistema robusto con menos estado, podrían eliminarse los siguientes puntos de compartición de estado:

- En los puntos (**A**) y (**D**) – Si el controlador de acceso utiliza alguna otra metodología para calcular la utilización de anchura de banda (además del seguimiento del número de llamadas por cómputo), podrían evitarse estos pasos sin daño alguno. Puede que el operador NO se interese en el control de admisión y que sus controladores de acceso no lo efectúen, en cuyo caso este paso no es necesario.
- En los puntos (**F**) y (**E**) – Ambos puntos son opcionales, puesto que no proporcionan ninguna información digna de mantenerse, es decir, que la llamada está sonando o se está aún estableciendo.
- En los puntos (**B**) y (**C**) – Si el operador NO está interesado en mantener más que las llamadas estables, pueden eliminarse estos dos puntos. En este caso, se perderían todas las llamadas que estaban estableciéndose cuando ocurrió un fallo.

Compromisos como éstos están fuera del alcance de la utilización del ASAP/SCTP y es de la exclusiva decisión del operador/fabricante saber cuánta información de estado puede ser mantenida por una determinada implementación y qué controles/decisiones puede adoptar el operador.

Apéndice I

Muestra de instrucción de modo de comunicación de MC a terminal

I.1 Muestra de escenario de conferencia A

Los puntos extremos A, B y C están en una conferencia distribuida de audio y vídeo utilizando multidifusión. El MC (que podría ser cualquiera de los nodos) ha decidido situar los canales de medios y de control de medios en las siguientes direcciones multidifusión:

Tren	Dirección multidifusión
Audio para todos los puntos extremos	MCA1
Audio de control para todos los puntos extremos	MCA2
Vídeo desde el punto extremo A	MCA3
Datos de control de vídeo acerca del punto extremo A	MCA4
Vídeo desde el punto extremo B	MCA5
Datos de control de vídeo acerca del punto extremo B	MCA6
Vídeo desde el punto extremo C	MCA7
Datos de control de vídeo acerca del punto extremo C	MCA8

I.2 Tabla de modos de comunicación enviada a todos los puntos extremos

Todas las entradas son instrucciones para que puntos extremos abran canales lógicos para transmisión. La **terminalLabel** (**etiqueta del terminal**) sólo está presente cuando la entrada es específica de un solo punto extremo de la conferencia.

```
ENTRADA 1 – CONTROL AUDIO & AUDIO PARA LA CONFERENCIA
sessionID                       1
sessionDescription              Audio
dataType                        Audio Capability
mediaChannel                    MCA1
mediaControlChannel             MCA2

ENTRADA 2 – CONTROL VÍDEO & VÍDEO PARA EL NODO A
sessionID                       2
associatedSessionID             1
terminalLabel                   M/T for A
sessionDescription              Video for Node A
dataType                        Video Capability
mediaChannel                    MCA3
mediaControlChannel             MCA4

ENTRADA 3 – CONTROL VÍDEO & VÍDEO PARA EL NODO B
sessionID                       3
associatedSessionID             1
terminalLabel                   M/T for B
sessionDescription              Video for Node B
dataType                        Video Capability
mediaChannel                    MCA5
mediaControlChannel             MCA6

ENTRADA 4 – CONTROL VÍDEO & VÍDEO PARA EL NODO C
sessionID                       4
associatedSessionID             1
terminalLabel                   M/T for C
sessionDescription              Video for Node C
```

```
dataType                        Video Capability
mediaChannel                    MCA7
mediaControlChannel             MCA8
```

I.3 Muestra de escenario de conferencia B

Los puntos extremos A, B y C están en una conferencia multipunto en la que el audio es unidifundido desde cada punto extremo y mezclado centralmente, pero el vídeo es multidifundido desde los puntos extremos. El MC puede enviar una instrucción de modo de comunicación (CommunicationModeCommand) única a cada punto extremo, o puede enviar el mismo mensaje a todos los puntos extremos y las entradas de la tabla son identificadas por la etiqueta del punto extremo de destino. Para este ejemplo, se supone que se envía el mismo mensaje a todos los puntos extremos.

Tren	Dirección multidifusión
Audio desde el punto extremo A	UCA1
Datos de control de audio acerca del punto extremo A	UCA2
Audio desde el punto extremo B	UCA3
Datos de control de audio acerca del punto extremo B	UCA4
Audio desde el punto extremo C	UCA5
Datos de control de audio acerca del punto extremo C	UCA6
Vídeo desde el punto extremo A	MCA1
Datos de control de vídeo acerca del punto extremo A	MCA2
Vídeo desde el punto extremo B	MCA3
Datos de control de vídeo acerca del punto extremo B	MCA4
Vídeo desde el punto extremo C	MCA5
Datos de control de vídeo acerca del punto extremo C	MCA6

I.4 Tabla de modos de comunicación enviada a todos los puntos extremos

Todas las entradas son instrucciones para que puntos extremos abran canales lógicos para transmisión. **terminalLabel** sólo está presente cuando la entrada es específica de un solo punto extremo de la conferencia.

```
ENTRADA 1 – CONTROL AUDIO & AUDIO PARA EL NODO A
sessionID                       1
sessionDescription              Audio
terminalLabel                   M/T for A
dataType                        Audio Capability
mediaChannel                    UCA1
mediaControlChannel             UCA2

ENTRADA 2 – CONTROL AUDIO & AUDIO PARA EL NODO B
sessionID                       2
sessionDescription              Audio
terminalLabel                   M/T for B
dataType                        Audio Capability
mediaChannel                    UCA3
mediaControlChannel             UCA4

ENTRADA 3 – CONTROL AUDIO & AUDIO PARA EL NODO C
sessionID                       3
sessionDescription              Audio
terminalLabel                   M/T for C
```

```
dataType                          Audio Capability
mediaChannel                      UCA5
mediaControlChannel               UCA6

ENTRADA 4 – CONTROL VÍDEO & VÍDEO PARA EL NODO A
sessionID                         4
associatedSessionID               1
terminalLabel                     M/T for A
sessionDescription                Video for Node A
dataType                          Video Capability
mediaChannel                      MCA1
mediaControlChannel               MCA2

ENTRADA 5 – CONTROL VÍDEO & VÍDEO PARA EL NODO B
sessionID                         5
associatedSessionID               2
terminalLabel                     M/T for B
sessionDescription                Video for Node B
dataType                          Video Capability
mediaChannel                      MCA3
mediaControlChannel               MCA4

ENTRADA 6 – CONTROL VÍDEO & VÍDEO PARA EL NODO C
sessionID                         6
associatedSessionID               3
terminalLabel                     M/T for C
sessionDescription                Video for Node C
dataType                          Video Capability
mediaChannel                      MCA5
mediaControlChannel               MCA6
```

Apéndice II

Procedimientos de reserva de recursos a nivel de transporte

II.1 Introducción

La presente Recomendación recomienda el uso de mecanismos de reserva de recursos a nivel de transporte para cumplir los requisitos de QoS de trenes de vídeo y audio en tiempo real. Aunque los mecanismos de reserva de recursos a nivel de transporte están fuera del alcance de la presente Recomendación, el método general y la coordinación de estos mecanismos a nivel de transporte entre entidades H.323, se describe en este apéndice para evitar dificultades de interoperabilidad.

En este apéndice se describe el uso del protocolo de reserva de recursos (RSVP, *resource reservation protocol*) como posible mecanismo para proporcionar QoS a nivel de transporte sobre redes basadas en el IP. Pueden utilizarse otros protocolos, pero los procedimientos básicos definidos en este apéndice deben seguir siendo aplicables. Los participantes en una conferencia deben poder señalizar sus intenciones, capacidades y requerimientos de una manera normalizada específica del protocolo. Además, la secuencia de señalización de los mecanismos de reserva de recursos debe especificarse de manera que el intervalo de establecimiento de comunicaciones sea mínimo.

RSVP es el protocolo de señalización a nivel de transporte para reservar recursos en redes IP no fiables. Utilizando el RSVP, los puntos extremos H.323 pueden reservar recursos para un determinado tren de tráfico en tiempo real basados en sus propios requisitos de QoS. Si la red no consigue reservar los recursos requeridos, o en ausencia de RSVP, sólo es posible la entrega de los paquetes utilizando el mecanismo de entrega del mayor esfuerzo posible.

II.2 Soporte de QoS para H.323

Cuando un punto extremo solicita la admisión a un controlador de acceso, debe indicar en el mensaje ARQ si es capaz o no de reservar recursos. El controlador de acceso debe entonces decidir, sobre la base de la información que recibe del punto extremo y de la información que tiene sobre el estado de la red, si:

- permite al punto extremo aplicar sus propios mecanismos de reserva para su sesión H.323; o
- efectúa la reserva de recursos en nombre del punto extremo; o
- no se necesita ninguna reserva de recursos. Es suficiente el mejor procedimiento posible.

Esta decisión es transmitida al punto extremo en el mensaje ACF. El punto extremo aceptará la decisión del controlador de acceso a fin de efectuar una llamada.

El controlador de acceso debe rechazar un ARQ de punto extremo, si el punto extremo no indica que es capaz de efectuar la reserva de recursos y el controlador de acceso decide que la reserva de recursos debe ser controlada por el punto extremo. En este caso, el controlador de acceso debe devolver ARJ al punto extremo.

El campo específico en la señalización RAS H.225.0 para permitir esta funcionalidad es el campo **transportQoS** (**calidad de servicio del transporte**).

Además de **transportQoS**, un punto extremo debe también calcular y comunicar la anchura de banda que en ese momento pretende utilizar en todos los canales de la llamada. Esta anchura de banda debe comunicarse en el campo **bandWidth** (**anchura de banda**) del mensaje ARQ independientemente de la decisión del punto extremo de utilizar o no señalización RSVP. Además, si los requisitos de anchura de banda cambian en el curso de la llamada, el punto extremo debe comunicar al controlador de acceso los cambios de requisitos de anchura de banda utilizando BRQ independientemente de la decisión de utilizar RSVP.

Las reservas RSVP sólo pueden ser efectuadas por entidades de red que están en el trayecto del flujo de medios entre puntos extremos. Es posible encaminar, mediante señalización de llamada encaminada por el controlador de acceso, trenes de medios a través de un controlador de acceso. Sin embargo, la mayoría de los canales de medios de tiempo se encaminarán entre puntos extremos sin pasar a través del controlador de acceso. Si un controlador de acceso decide encaminar trenes de medios, los procedimientos seguidos deben entonces ser idénticos a los aplicados para la señalización RSVP directamente desde los puntos extremos. Lo mejor es que las reservas RSVP sean efectuadas directamente por los puntos extremos, ya que así se reservarán recursos a lo largo de todo el trayecto de encaminamiento de la llamada. El resto de este apéndice trata la utilización del RSVP por los puntos extremos H.323.

Algunos de los puntos sobresalientes del RSVP son los siguientes:

- RSVP soporta entornos unidifusión y multidifusión;
- RSVP está ligado a trenes concretos (es decir, pares concretos de direcciones de transportes);
- RSVP es de carácter flexible, por lo cual se adapta dinámicamente al cambio de la composición de los grupos y las rutas;
- RSVP es unidireccional;
- RSVP está orientado al receptor, es decir, el destinatario del tren de medios hace la reserva (escalable).

II.3 Fundamento del RSVP

En la descripción que sigue se expondrá la utilización de alto nivel del RSVP en una conferencia H.323 simple.

En la figura II.1, el punto extremo A desea enviar un tren de medios al punto extremo B. Por tanto, tiene que abrir un canal lógico a B. La señalización RSVP para la reserva de recursos debe ser una parte del procedimiento de apertura de canal lógico. El punto extremo A haría que se enviasen mensajes *Trayecto* RSVP a B. Estos mensajes *Trayecto* van a través de encaminadores y van dejando su "estado" al progresar hacia B. Los mensajes *Trayecto* contienen las direcciones de origen y de destino completas del tren y una caracterización del tráfico que enviará la fuente. El punto extremo B utilizaría la información procedente del *Trayecto* para hacer la petición *Reserva* RSVP a lo largo de todo el trayecto. Los mensajes *Reserva* contienen la reserva propiamente dicha y generalmente serán los mismos que la especificación de tráfico en el mensaje *Trayecto*.

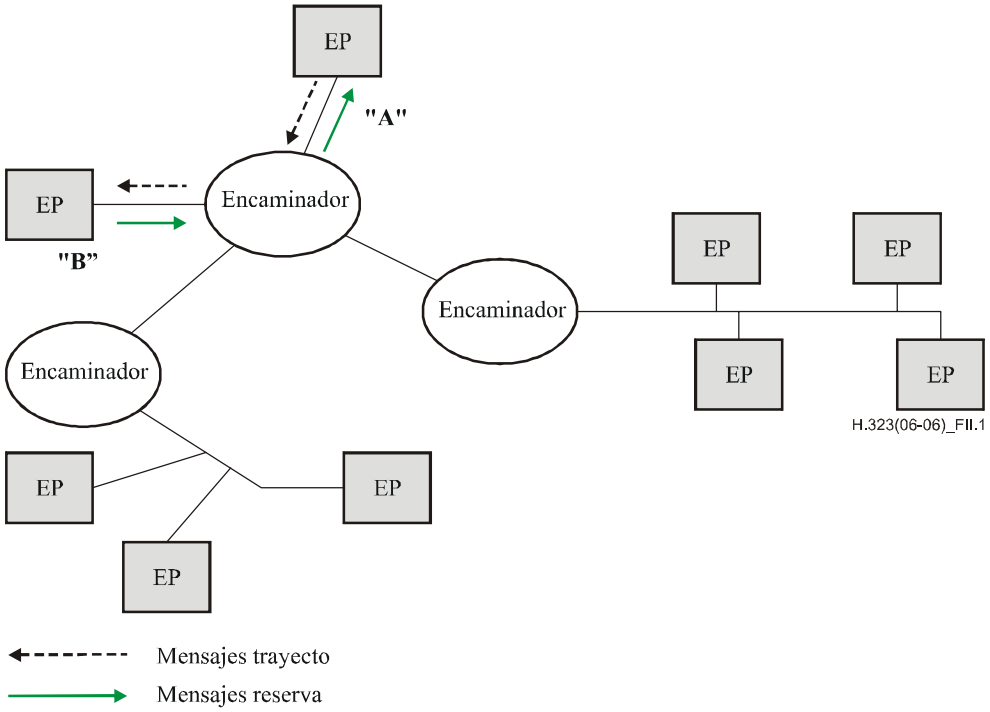


Figura II.1/H.323 – Reserva de recursos para una conexión punto a punto

En la figura II.2, se muestra una conferencia multipunto. Los mensajes *Trayecto* se utilizan de la misma manera que en el caso, más simple, punto a punto. Debe señalarse que las peticiones *Reserva* son agrupadas por los encaminadores para impedir que las peticiones de reserva redundantes viajen hacia el origen.

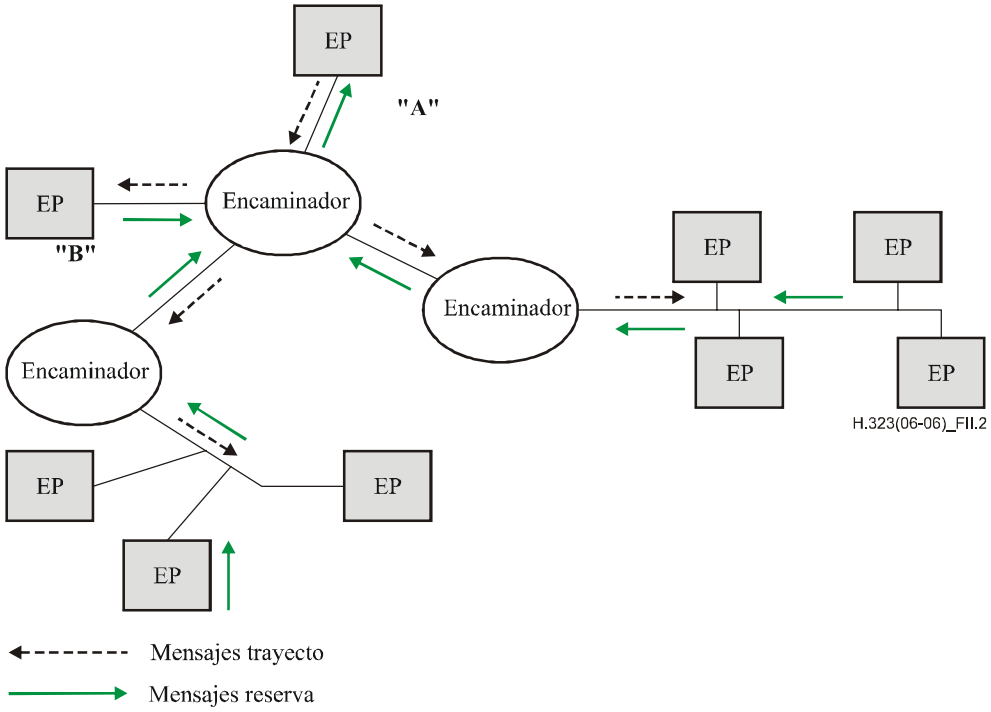


Figura II.2/H.323 – Reserva de recursos para una conexión punto a multipunto

Los mensajes *Trayecto* deben contener las direcciones de destino/origen completas y una especificación de tráfico. Los mensajes *Reserva* contienen los parámetros de reserva y el servicio requerido. Los mensajes *Trayecto* y *Reserva* para un determinado tren de tráfico deben enviarse como parte del procedimiento **openLogicalChannel** para ese tren en particular. La reserva debe liberarse durante el procedimiento **closeLogicalChannel** utilizando los mensajes *Romper Trayecto* (*PathTear*) y *Romper Reserva* (*ResvTear*).

Hay que tener en cuenta que los mensajes RSVP trayecto y reserva utilizan el mismo par dirección/puerto IP que los medios que han de entregarse entre puntos extremos, lo que significa que los puntos extremos deben filtrar estos mensajes del tren de medios. Esto no es competencia de los puntos extremos que hacen el filtrado UDP, ya que los propios mensajes RSVP no son mensajes UDP. Aun así, el emisor de un tren de medios no debe utilizar RSVP cuando el receptor no es capaz de hacer uso de ello. Las capacidades RSVP se intercambian como parte de los procedimientos de intercambio de capacidades y de apertura de canal lógico.

RSVP es sólo un protocolo de señalización. Junto con los servicios QoS apropiados (por ejemplo, servicio de QoS garantizada o de control de carga garantizado), los mecanismos de ordenación (por ejemplo, puesta en cola equitativa ponderada), y el módulo de política de control de admisión (por ejemplo, gestor de política local), el RSVP puede satisfacer los requisitos de QoS de los participantes en una conferencia H.323. Además, RSVP está diseñado para enlaces punto a punto. Si un trayecto atraviesa un enlace compartido, RSVP invoca el mecanismo de reserva de recursos apropiados para el medio compartido concreto, por ejemplo, gestión de anchura de banda de subred (SBM, *subnet bandwidth management*) en el caso de Ethernet. Todos los mecanismos mencionados en este párrafo son controlados completamente desde el propio RSVP. Por tanto, todo lo que un punto extremo H.323 necesita es la señalización RSVP.

II.4 La fase de intercambio de capacidades H.245

Durante la fase de intercambio de capacidades H.245, cada punto extremo indica sus capacidades de transmisión y recepción al otro punto extremo. La **qOSCapability** (**capacidad de calidad de servicio**), es parte del intercambio de capacidades. Sin embargo, no es específica del tren. Por tanto,

si en la **qOSCapability** se especificasen los parámetros RSVP, representarían un agregado de todos los trenes (ya sean los transmitidos o los recibidos). Dichos parámetros no serán de ninguna utilidad para el otro punto extremo. Por tanto, la única información relacionada con el RSVP que un punto extremo debe transmitir al otro punto extremo en el conjunto de capacidades es si está o no capacitado para manejar el RSVP.

Para señalizar la capacidad RSVP, un punto extremo fijará los campos **qOSMode** (**modo de calidad de servicio**) disponibles dentro de la PDU capacidad durante el intercambio de capacidades. Los puntos extremos que no reciben capacidades RSVP del punto extremo receptor no utilizarán RSVP cuando abran canales lógicos.

II.5 Apertura de canal lógico y establecimiento de reservas

En esta cláusula se describen los pasos que deben seguirse para abrir un canal lógico H.245 y reservar recursos para un determinado tren de tráfico. Las reservas se establecen sólo si ambos puntos extremos indican, durante el intercambio de capacidades, que están capacitados para el RSVP. Se considera sólo el caso punto a punto. El caso de conexiones punto a multipunto (multidifusión) se tratará en II.7.

El emisor especificará en el campo **qOSCapability** del mensaje **openLogicalChannel** los parámetros RSVP del tren a transmitir, y los servicios integrados que soporta el emisor. En el caso de un tren punto a punto, el emisor no especifica un ID de puerto receptor en el mensaje **openLogicalChannel**. El receptor selecciona este ID después de recibir el mensaje **openLogicalChannel**, que se devuelve al emisor en el mensaje **openLogicalChannelAck**. Sólo entonces puede el emisor crear una sesión RSVP para ese tren (crear una sesión RSVP para un determinado tren significa que el punto extremo se registra en el RSVP para que se le notifique la llegada de los mensajes que puedan afectar al estado de la reserva RSVP para ese tren), y empezar a emitir mensajes RSVP *Trayecto*. El receptor tiene suficiente información para crear una sesión RSVP para el mismo tren antes de enviar el mensaje **openLogicalChannelAck**. La información necesaria para crear una sesión RSVP e iniciar el procesamiento RSVP es la dirección IP del receptor en caso de punto a punto, o la dirección IP multidifusión de grupo en caso de punto a multipunto, el ID de puerto del receptor y el protocolo (siempre UDP en caso de trenes de audio y vídeo H.323 en redes IP).

Un receptor puede no desear empezar a recibir paquetes de trenes hasta que estén hechas las reservas RSVP. Para conseguirlo, el receptor puede poner el campo booleano **flowcontrolToZero** (**control de flujo a cero**) del mensaje **openLogicalChannelAck** a VERDADERO para indicar que no desea recibir ningún tráfico en ese canal antes de que estén completas las reservas de recursos. Cuando un emisor recibe un mensaje **openLogicalChannelAck** cuyo **flowControlToZero** está puesto a VERDADERO, el emisor no transmitirá ningún tráfico por ese canal.

Cuando el receptor empieza a recibir los mensajes *Trayecto* del emisor, debe iniciar la emisión de mensajes RSVP *Reserva*. Cuando el receptor recibe un mensaje RSVP *Reserva Confirmación* (*ResvConf*) confirmando que se han establecido reservas, puede enviar una **flowControlCommand** (**instrucción de control de flujo**) al emisor irrestringiendo la velocidad binaria del tren de tráfico, es decir, suprimiendo el efecto del campo **flowcontrolToZero** anterior en el mensaje **openLogicalChannelAck**. Cuando el receptor recibe **flowControlCommand**, empieza a transmitir paquetes.

Téngase en cuenta que el mensaje *Reserva Confirmación*, y análogamente todos los demás mensajes RSVP, se transmiten no fiablemente. Por consiguiente, pueden retrasarse e incluso perderse. Un punto extremo debe conocer esa posibilidad, y fijar temporizadores con un valor apropiado mientras se espera un mensaje *Reserva Confirmación*. En caso de que venza la temporización del punto extremo sin haber recibido un mensaje *Reserva Confirmación*, la acción ejercida corresponde a los distintos vendedores de puntos extremos.

Si las reservas RSVP fallan en cualquier punto durante una llamada H.323, el comportamiento de un punto extremo no se especifican en este apéndice, y se deja a criterio de los vendedores. Sin embargo, si falla una reserva RSVP y el punto extremo receptor decide que el nivel de servicio de mayor esfuerzo posible no es aceptable, puede solicitar el cierre de su canal lógico utilizando el mensaje **requestChannelClose** (**petición de cierre de canal**). El campo **closeReason** (**motivo del cierre**) está disponible en el mensaje **requestChannelClose** para que el receptor pueda señalizar al emisor que la reserva RSVP ha fallado. Junto con la indicación de fallo, **requestChannelClose** incluye **qOSCapability**, que puede utilizar el receptor para comunicar al emisor los recursos que en ese momento están realmente disponibles en el trayecto del emisor al receptor. En este punto, el emisor puede decidir tratar de reabrir el canal con un códec de menor anchura de banda y/o formato de datos inferiores y someterse de nuevo a procedimiento de apertura de canal lógico.

Todas las peticiones RSVP *Reserva* utilizarán el mismo estilo de reserva, el estilo de **Fixed Filter** (**filtro fijo**), por los motivos siguientes:

- Los estilos de filtro compartido se reducen a filtros fijos en caso de llamadas punto a punto.
- No pueden mezclarse en la red estilos de reserva diferentes en la misma sesión. Por ejemplo, si en una llamada multipunto algunos de los receptores solicitan reservas de filtros fijos mientras que el resto solicitan reservas explícitas compartidas, fallarán las reservas de filtros fijos o las reservas explícitas compartidas.
- Las reservas compartidas, creadas por estilos de filtro comodín y de filtro explícito compartido, son apropiadas para aquellas aplicaciones multidifusión en las que es improbable que múltiples fuentes de datos transmitan simultáneamente. En las llamadas H.323 multipunto distribuidas, no existe ningún mecanismo que permita exclusivamente a una fuente transmitir en un momento determinado. En cambio, en las llamadas H.323 multipunto centralizadas, la MCU es la única fuente multidifusión. Los estilos de reserva compartida no son adecuados para ninguno de los casos.

Corresponde a los vendedores de puntos extremos elegir qué servicio QoS intserv (QoS garantizada o carga controlada) ha de utilizarse. Sin embargo, cualquier punto extremo H.323 con capacidad de utilizar RSVP, soportará el servicio de carga controlada como el servicio menos común. Este requisito es necesario para evitar problemas de interoperabilidad que puedan surgir de puntos extremos H.323 habilitados para RSVP que no soporten un servicio QoS intserv.

La figura II.3 muestra la secuencia de mensajes en caso de reserva RSVP exitosa.

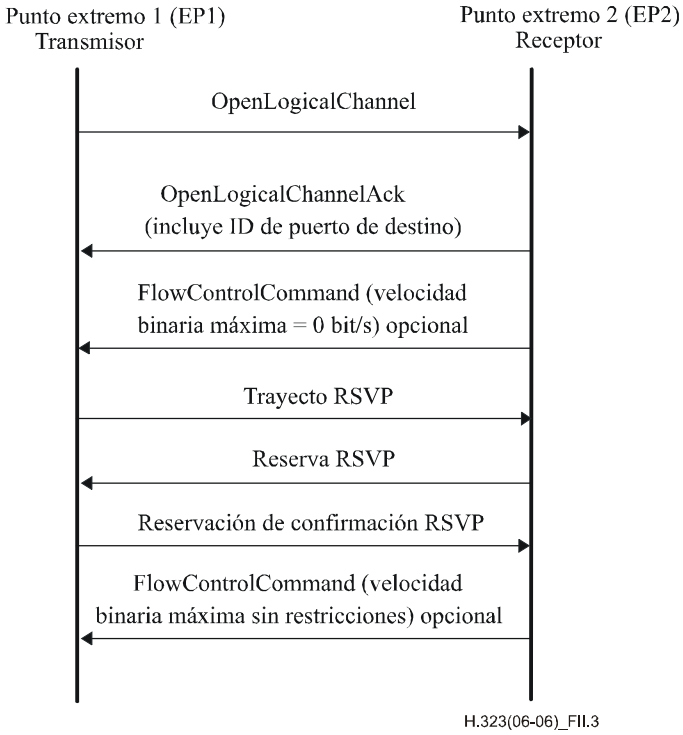


Figura II.3/H.323 – Secuencia de mensajes para abrir un canal lógico unidifusión con RSVP

II.6 Cierre de canal lógico y cancelación de reservas

Antes de enviar un mensaje **closeLogicalChannel** para un determinado tren de tráfico, un punto extremo emisor debe enviar un mensaje *Romper Trayecto* si se ha creado previamente una sesión RSVP para ese tren. Cuando un punto extremo receptor recibe un **closeLogicalChannel** para un determinado tren de tráfico, debe enviar un mensaje *Romper Reserva* si se ha creado previamente una sesión RSVP para ese tren.

II.7 Reserva de recursos para canales lógicos H.323 multidifusión

El procedimiento **openLogicalChannel** H.245 es punto a punto aunque el tren de tráfico correspondiente sea un tren multidifusión. Sin embargo, para que el punto extremo receptor empiece a recibir paquetes de un tren multidifusión, tiene que incorporarse al grupo multidifusión y conectarse al árbol multidifusión del origen. Cuando un receptor recibe un mensaje **openLogicalChannel**, se incorpora al grupo multidifusión y al árbol multidifusión del origen utilizando procedimientos IGMP normalizados. La incorporación al IGMP (utilizando el mensaje IGMP *Report*) tiene lugar antes de que el receptor envíe un **openLogicalChannelAck** de vuelta al emisor.

En el caso de un tren multidifusión, el emisor especifica el ID del puerto receptor en el mensaje **openLogicalChannel** en lugar de recibir el ID de puerto receptor en el mensaje **openLogicalChannelAck**.

El receptor puede poner el campo **flowControlToZero** del mensaje **openLogicalChannelAck** a VERDADERO, análogamente al caso unidifusión. Sin embargo, el emisor (un punto extremo en una conferencia distribuida o una MCU en una conferencia centralizada) debe decidir no interrumpir el tren de datos del canal abierto, si determina que esta interrupción puede afectar a otros receptores del mismo grupo multidifusión que ya está recibiendo este tren. Por consiguiente, en el caso multidifusión, el receptor puede inicialmente recibir los datos por el mejor procedimiento posible hasta que se establezcan las reservas RSVP.

La figura II.4 muestra la secuencia de mensajes requeridos para abrir un canal lógico, incorporarse al árbol multidifusión y reservar recursos para un tren multidifusión.

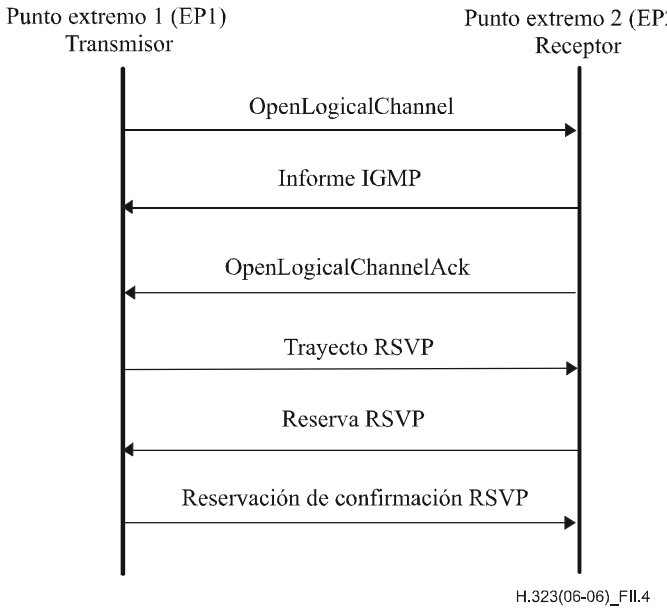


Figura II.4/H.323 – Secuencia de mensajes para abrir un canal lógico multidifusión con RSVP

Antes de enviar un mensaje **closeLogicalChannel** para un determinado tren multidifusión, un punto extremo emisor debe enviar un mensaje RSVP *Romper Trayecto* si el canal lógico que se está cerrando es el último canal que transporta dicho tren multidifusión y si se ha creado previamente una sesión RSVP para ese tren. Cuando un punto extremo receptor recibe un **closeLogicalChannel** para un determinado tren multidifusión, debe enviar un mensaje RSVP *Romper Reserva* y un mensaje IGMP *Abandono*, en caso de que se haya creado previamente una sesión RSVP para ese tren.

II.8 Sincronización de RSVP

La sincronización de RSVP es el proceso de reserva de recursos con RSVP previo a la transición a la fase de aviso de la llamada. En las dos subcláusulas siguientes se analizan la sincronización RSVP sin conexión rápida y con conexión rápida respectivamente. En esta cláusula se presenta el concepto general de lista priorizada de niveles de QoS, expresada para cada punto extremo y de la que se deriva un nuevo conjunto 'D' de niveles de QoS. El conjunto derivado 'D' incluye la intersección de dos conjuntos **QoSMode** (**modo de QoS**) preferidos. Los dos puntos extremos pueden intentar establecer reservas RSVP en función de en un nivel de QoS del conjunto derivado, partiendo del nivel de QoS preferido.

Al generar el conjunto de QoS, el punto extremo llamado suspende la fase de aviso de la llamada hasta que se hayan realizado las reservas en ambos sentidos. Cuando se realiza con éxito la reserva, se puede producir el aviso y se puede retomar el establecimiento de la comunicación. Si se producen fallos, se analiza el nivel más bajo de QoS del conjunto derivado. Si éste es del tipo "mayor esfuerzo posible", se vuelven a poner en marcha los procedimientos de establecimiento; si no es así, se libera la llamada. El envío de una estructura **QoSCapability** (**capacidad de QoS**) con un elemento **QoSMode** en el bloque **rsvpParameters** (**parámetros de rsvp**), indicará que el nivel de QoS es "mayor esfuerzo posible". El elemento **QoSMode** del bloque **rsvpParameters** prioriza la secuencia **QoSMode** con prioridad descendente desde el primer elemento hasta el último. **GuarantedQoS** (**QoS garantizada**) es el nivel superior de QoS que puede recibir un punto

extremo, siendo "mayor esfuerzo posible" el más bajo. Si la QoS preferida que el punto extremo llamante desea recibir es superior a "mayor esfuerzo posible", dicho punto extremo debe iniciar los procedimientos RSVP quedando a la espera de mensajes trayecto procedentes del punto extremo llamado.

El punto extremo llamado examinará la secuencia de las estructuras **QoSCapabilities** y, si existen, la compararán con su propio conjunto de niveles de QoS en base al **QoSMode**. El punto extremo llamado genera entonces un nuevo conjunto de niveles de QoS 'D' basados en el **QoSMode** que representa la intersección de los niveles de QoS de los conjuntos preferidos de los dos puntos extremos. Este nuevo conjunto denota los distintos niveles de QoS con un orden priorizado basado en el **QoSMode** que soportan ambos puntos extremos. Por ejemplo, si el conjunto preferido de los niveles de QoS del punto extremo llamante es {**GuaranteedQoS**, **ControlledLoad**} y el del punto extremo llamado es {**ControlledLoad**, "mayor esfuerzo posible"}, el conjunto intersección de ambos es {**ControlledLoad**}. Se pueden dar distintos casos generales en función de los niveles preferidos de QoS de ambos puntos extremos. En el cuadro II.1 se muestran los distintos casos y los correspondientes tratamientos de la llamada.

Cuadro II.1/H.323 – Tratamiento de llamadas para distintas clases de QoS

Escenario de QoS	Ejemplo	Tratamiento de la llamada
1) El conjunto derivado de QoS 'D' está vacío	Conjunto preferido del punto extremo llamante: {GQ} Conjunto preferido del punto extremo llamado: {CL,BE} Conjunto 'D' de QoS derivado: {}	El punto extremo llamado liberará la llamada.
2) El conjunto derivado de QoS 'D' sólo tiene un nivel de QoS: "mayor esfuerzo posible"	Conjunto preferido del punto extremo llamante: {BE} Conjunto preferido del punto extremo llamado: {CL,BE} Conjunto "D" de QoS derivado: {BE}	El punto extremo llamado no intentará los procedimientos RSVP. No obstante, continuará los procedimientos de establecimiento de comunicación.
3) El conjunto derivado de QoS 'D' tiene al menos un nivel de QoS superior a "mayor esfuerzo posible"	Conjunto preferido del punto extremo llamante: {GQ,CL,BE} Conjunto preferido del punto extremo llamado: {CL,BE} Conjunto 'D' de QoS derivado: {CL,BE}	El punto extremo llamado suspenderá el aviso e intentará el RSVP sincronizado. En los apartados siguientes se describen los procedimientos en detalle.
BE "Mayor esfuerzo posible" (*"best effort"*) CL Carga controlada (*ControlledLoad*) GQ QoS garantizada (*GuarantedQoS*)		

En caso de fallo de los procedimientos RSVP, el punto extremo llamado examinará la QoS preferida siguiente, si existe, del conjunto derivado 'D'. Si existe una QoS distinta a "mayor esfuerzo posible", el punto extremo llamado debe reiniciar las reservas RSVP con dicho nivel de QoS. En el caso de fallos sucesivos, es posible reintentar los procedimientos de reserva RSVP para todos los niveles de QoS (distintos a "mayor esfuerzo posible") del conjunto derivado. Cuando expira el temporizador de reserva del punto extremo llamado o, si el punto extremo llamado falla en el establecimiento de reservas RSVP con el nivel más bajo de QoS del conjunto derivado que no sea "mayor esfuerzo posible", el punto extremo llamado examinará el nivel el nivel de QoS más bajo del conjunto derivado. Si dicho nivel no es "mayor esfuerzo posible", el punto extremo llamado liberará la llamada; en cualquier otro caso, el establecimiento de la comunicación se retoma con el

nivel de QoS "mayor esfuerzo posible". Los fallos de reserva y la expiración del temporizador de reserva se manejan de forma semejante en el punto extremo llamante.

En las dos subcláusulas siguientes se analizan la sincronización de RSVP la sincronización de RSVP con conexión rápida, respectivamente, utilizando el concepto de lista derivada priorizada de **QoSMode**.

II.8.1 Sincronización de RSVP cuando no se utiliza la conexión rápida

Un punto extremo llamante que desee reservar recursos mediante RSVP sincronizado y que no realice la llamada utilizando la conexión rápida, incluirá necesariamente una dirección H.245 en el mensaje Establecimiento. Igualmente, un punto extremo llamado que desee reservar recursos RSVP antes de completar el establecimiento de la comunicación, recuperará la dirección H.245, si existe, del punto extremo llamante del mensaje Establecimiento entrante. Consiguientemente, el punto extremo llamado establecerá el canal de control H.245 e iniciará los procedimientos H.245. Hasta que los procedimientos H.245 y RSVP no se hayan completado, el punto extremo llamado no prosigue con la fase de establecimiento de la comunicación H.225.0. No obstante, se recomienda que el punto extremo llamado devuelva un mensaje llamada en curso al punto extremo llamante para evitar que venza cualquiera de los temporizadores H.225.0 del lado origen.

Si el punto extremo llamado desea realizar la sincronización de RSVP pero el punto extremo llamante no incluye su dirección H.245 en el mensaje Establecimiento de entrada, el punto extremo llamante considerará que el punto extremo de origen no acepta o inicia los procedimientos de sincronización de RSVP. Es responsabilidad del punto extremo llamado decidir cuál es la acción más adecuada que debe tomarse en función del modo de QoS derivado, tal como se analiza en II.8. Igualmente, si el punto extremo llamante desea intentar la sincronización de RSVP y ha incluido su dirección H.245 en el mensaje Establecimiento, pero el punto extremo llamado no ha conseguido establecer el canal de control H.245 y ha retomado los procedimientos H.225.0, es el punto extremo llamante quien determina la acción que debe tomarse en función del modo de QoS derivado, tal como se muestra en el cuadro II.1.

En cualquier otro caso, si el punto extremo llamante ha incluido su dirección H.245 en el mensaje Establecimiento y el punto extremo llamado ha establecido el canal de control H.245, los procedimientos H.245 se realizan como es habitual, es decir, mediante la determinación principal-subordinado y el intercambio de capacidad.

Durante el intercambio de capacidad H.245, los puntos extremos que deseen intentar el RSVP deben incluir una secuencia **qOSCapabilities** (como parte del elemento **transportCapability** de la estructura **H2250Capability**), priorizada según el elemento **qosMode** (por ejemplo, **guaranteedQoS**, **controlledLoad**) de **rsvpParameters**.

Asimismo, cuando se abran los canales lógicos utilizando los procedimientos H.245, cada punto extremo especificará los parámetros RSVP del tren que debe transmitirse en el campo **qOSCapability** del mensaje **openLogicalChannel**.

Cuando recibe un mensaje OLC de su par, y siempre que el par haya indicado durante el intercambio de capacidad que puede trabajar con RSVP, el punto extremo queda a la espera de los mensajes trayecto entrantes. Cuando recibe un mensaje trayecto, el punto extremo responderá enviando un mensaje reserva en el tren de recepción.

Cuando el punto extremo recibe de su par un mensaje acuse de OLC, inicia el envío al mismo de mensajes trayecto en su tren de transmisión. Los procedimientos RSVP se habrán completado con éxito cuando el punto extremo haya recibido un mensaje confirmación de reserva en respuesta a la transmisión de su mensaje reserva, y un mensaje reserva en respuesta a su mensaje trayecto. Si existen varios trenes, (por ejemplo, voz, vídeo y datos), el punto extremo debe esperar la confirmación de la reserva para todos los trenes que requieran QoS basada en RSVP.

Es recomendable que una vez que el punto extremo haya intentado el RSVP, arranque un temporizador durante un tiempo reducido (por ejemplo, cinco o seis segundos). Si el temporizador expira antes de que se hayan completado las reservas RSVP, el punto extremo puede determinar las acciones pertinentes que deben tomarse.

Si los procedimientos RSVP (y por tanto los procedimientos H.245) se han completado con éxito antes del vencimiento del temporizador, el punto extremo llamado puede retomar los procedimientos de establecimiento normales devolviendo un mensaje aviso al punto extremo llamante. No obstante, si el intento de reservar recursos RSVP falla, es responsabilidad de cada punto extremo decidir las acciones adecuadas que deben realizarse en función del conjunto **QoSMode** derivado, tal como se describe en II.8. En cualquier caso, se recomienda que si la llamada ha alcanzado la fase de aviso y la reserva RSVP ha fallado, se permita que se curse la llamada.

La figura II.5 ilustra el flujo de llamada modificado para una sincronización RSVP exitosa cuando no se utiliza la conexión rápida.

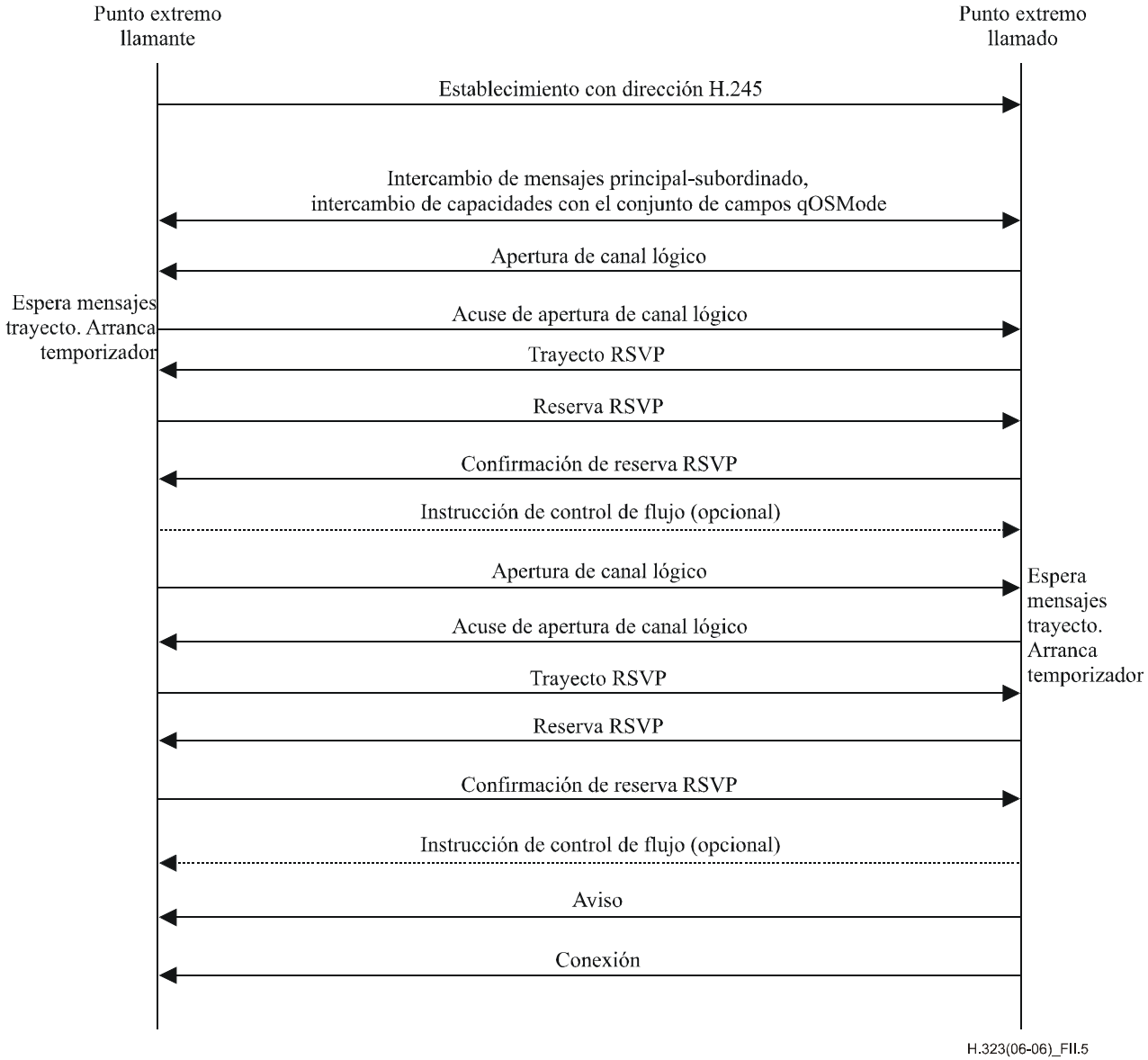


Figura II.5/H.323 – Sincronización de RSVP cuando no se utiliza la conexión rápida

II.8.2 Sincronización RSVP cuando se utiliza la conexión rápida

En esta cláusula se describe la sincronización de los procedimientos de establecimiento de comunicación que utilizan conexión rápida con los procedimientos de reserva RSVP a fin de eliminar el transporte de la señal de llamada dentro de banda antes de que se haya realizado la reserva.

Un punto extremo llamante que desee utilizar RSVP en un procedimiento de conexión rápida, enviará una secuencia de estructuras **QoSCapability** priorizadas en las estructuras **OpenLogicalChannel** del elemento **fastStart** del mensaje Establecimiento.

Al recibir el mensaje Establecimiento de conexión rápida, el punto extremo llamado generará el conjunto **QoSMode** utilizando el mecanismo que se describe en el cuadro II.1. Suponiendo que el conjunto derivado contiene una intersección válida (es decir, que no sea del tipo mayor esfuerzo posible) el punto extremo llamado responderá al mensaje Establecimiento del punto extremo llamante enviando un elemento **fastStart** que sólo incluya las **QoSCapabilities** indicadas en el conjunto de QoS derivado. El elemento **fastStart** se enviará cuanto antes (por ejemplo, en el mensaje llamada en curso) para acelerar la reserva de recursos. El conjunto del punto extremo llamante será un subconjunto de la lista enviada por el mismo en las estructuras **OpenLogicalChannel**, e igualmente, será una secuencia en orden descendente de prioridades de **QoSMode**. Cada **QoSCapability** incluida en el **OpenLogicalChannel** del mensaje de respuesta indica la aceptación de correspondiente nivel de QoS por parte del punto extremo llamado. Las estructuras **OpenLogicalChannel** del elemento **fastStart** también contienen información sobre los puertos de medios utilizados en el punto extremo llamado.

El punto extremo llamado iniciará los procedimientos RSVP enviando un mensaje TRAYECTO a su par en el tren de transmisión. Además, el punto extremo puede utilizar un temporizador de reserva que represente el tiempo total disponible para establecer las reservas RSVP sincronizadas para cualquier nivel de QoS (distinto a "mayor esfuerzo posible") del conjunto derivado. Además, el punto extremo llamado responderá a un mensaje TRAYECTO de entrada con un mensaje reserva en el tren de recepción. Obsérvese que el punto extremo llamado debe suspender la fase de aviso de la llamada y no enviar el mensaje aviso al punto extremo llamante hasta que se hayan realizado las reservas en ambos sentidos. Una vez que se hayan establecido los procedimientos RSVP, el punto extremo llamado continuará con los procedimientos de establecimiento de comunicación H.225.

Cuando el punto extremo llamante recibe el elemento **fastStart**, extraerá la información del puerto de medios de **OpenLogicalChannel** y registrará la lista priorizada de **QoSCapabilities** que devuelve el punto extremo llamado. El punto extremo iniciará el envío de mensajes TRAYECTO a su par con el tren de transmisión. Asimismo, cuando recibe un mensaje TRAYECTO del punto extremo llamado, responderá con un mensaje reserva al tren de recepción. El punto extremo llamante puede arrancar un temporizador de reserva disponible para el establecimiento de reservas RSVP sincronizadas.

Se considera que el establecimiento de reservas RSVP se ha finalizado con éxito cuando el punto extremo llamado recibe un mensaje RESERVA en respuesta a su mensaje TRAYECTO y un mensaje CONFIRMACIÓN DE RESERVA en respuesta a su mensaje RESERVA. En cuanto los procedimientos RSVP se han completado con éxito, el punto extremo llamado detiene el temporizador de reserva y retoma los procedimientos de establecimiento de comunicación. Ulteriormente envía mensajes Aviso/Conexión al punto extremo llamante. En la figura II.6 se ilustra el flujo de llamada para una llamada de conexión rápida sincronizada exitosa.

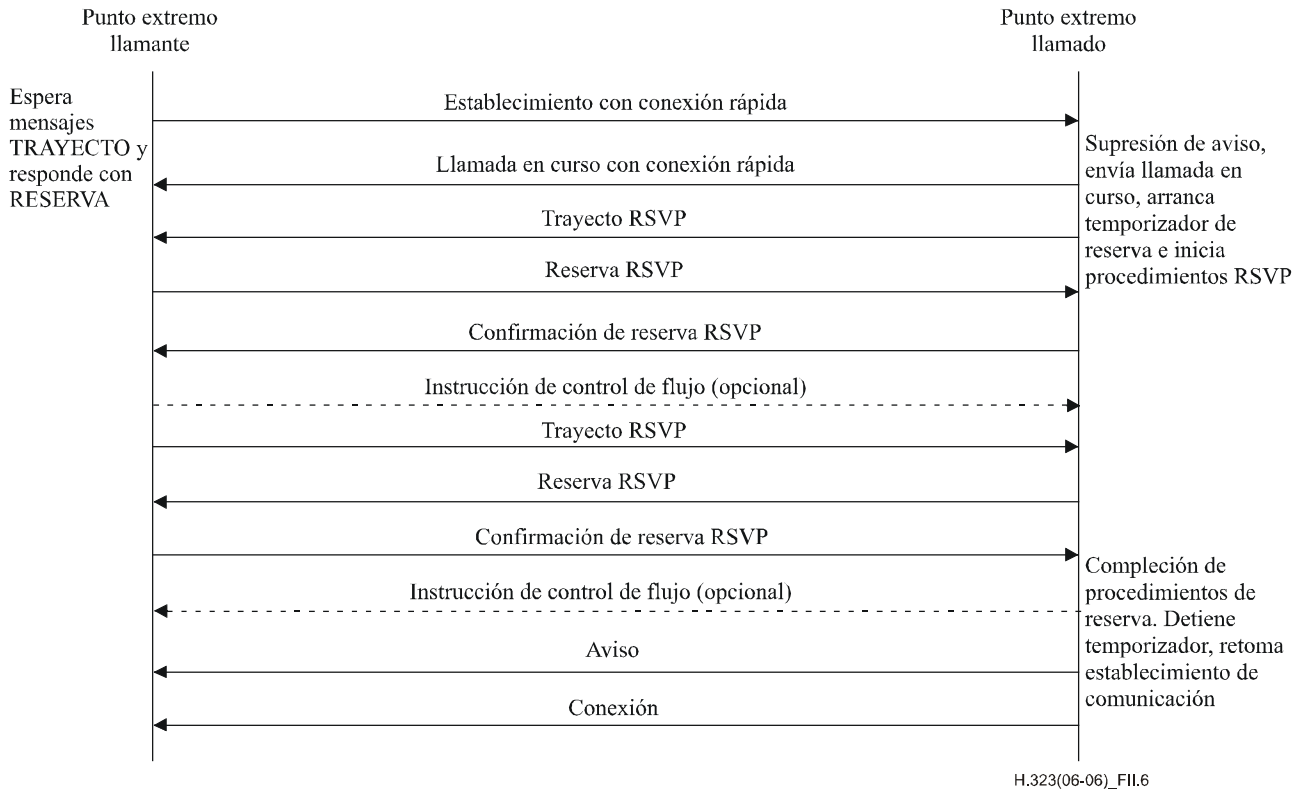


Figura II.6/H.323 – Sincronización de RSVP cuando se utiliza conexión rápida

En caso de un fallo de RSVP, el punto extremo llamado toma las acciones necesarias de acuerdo con el conjunto **QoSMode**, tal como se describe en II.8.

Apéndice III

Localización de usuarios por el controlador de acceso

III.1 Introducción

Este apéndice contiene ejemplos de cómo un controlador de acceso, o su mandatario, puede implementar los servicios de localización de usuarios. Estos servicios dependen del controlador de acceso que usa el modelo de señalización de llamada encaminada por controlador de acceso.

III.2 Señalización

En el escenario presentado en la figura III.1, el controlador de acceso implementa un servicio de "desviación en caso de no respuesta". El punto extremo 1 llama al punto extremo 2 con el canal de señalización de llamada encaminado a través del controlador de acceso. Si no hay respuesta después de transcurrido algún plazo, el controlador de acceso desvía la llamada a un punto extremo alternativo. Los mensajes (1) a (5) muestran al controlador de acceso intentando establecer una comunicación entre el punto extremo 1 y el punto extremo 2. En este ejemplo el punto extremo 2 no responde, por lo que el controlador de acceso liberó la llamada al punto extremo 2 enviando liberación completa (6). El controlador de acceso prueba entonces con el punto extremo 3 enviando establecimiento (7). Cuando el punto extremo 3 responde a la llamada utilizando conexión (9), el controlador de acceso devuelve el mensaje Conexión (10) al punto extremo 1.

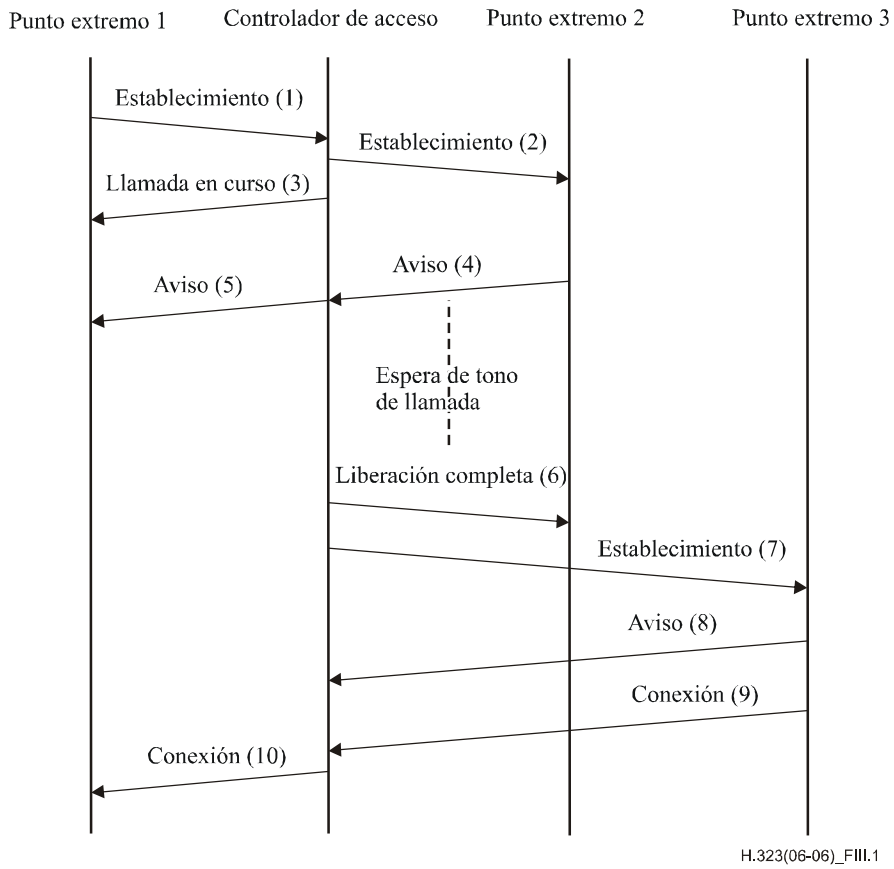


Figura III.1/H.323 – Ejemplo de localización de usuario utilizando señalización de llamada H.225.0 (por razones de claridad no se muestra la señalización RAS)

Puede utilizarse un método similar para proporcionar el servicio "desviación en caso de ocupado". En este caso, el punto extremo 2 devolvería un mensaje Liberación Completa indicando que está ocupado. El controlador de acceso intentaría entonces establecer una comunicación con el punto extremo 3.

En el escenario presentado en la figura III.2, el controlador de acceso intenta establecer contacto simultáneamente con los puntos extremos 2 y 3 enviando los mensajes de Establecimiento (2) y (3). En este ejemplo, el usuario en el punto extremo 3 responde enviando Conexión (8). El controlador de acceso remite la Conexión (9) de vuelta al punto extremo 1 y libera el intento de llamada al punto extremo 2 utilizando Liberación Completa (10). El controlador de acceso debe ignorar cualquier mensaje Conexión recibido del punto extremo 2 que llegue después del mensaje Conexión (9) desde el punto extremo 3 para que sólo se complete una llamada.

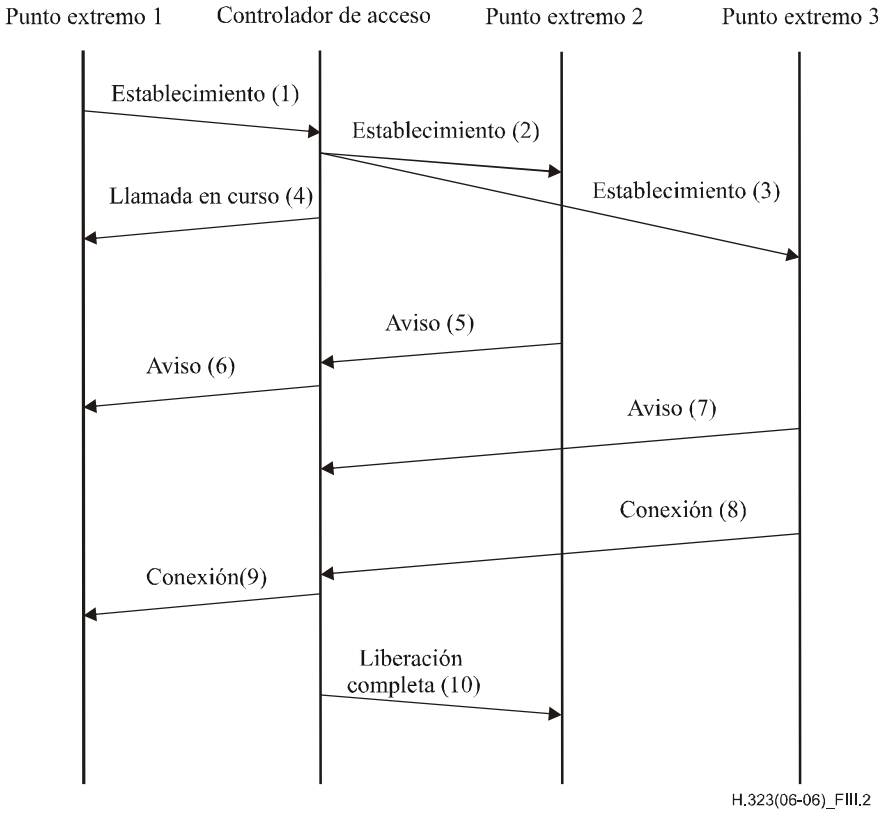


Figura III.2/H.323 – Ejemplo de localización de usuario utilizando señalización de llamada H.225.0 (por razones de claridad no se muestra la señalización RAS)

Hay que tener en cuenta que si el controlador de acceso está efectuando este tipo de algoritmo de localización de usuario, no debe pasar el campo **h245Address** (**dirección h245**) en ninguno de los mensajes acuse de Establecimiento, Llamada en curso o Aviso procedentes del punto extremo 2 o del punto extremo 3 al punto extremo 1, ya que esto puede producir un resultado incorrecto.

Apéndice IV

Señalización de canales lógicos alternativos priorizados en H.245

IV.1 Introducción

En este apéndice se describe un método sencillo de señalización para los canales lógicos alternativos. No es preciso introducir cambios de codificación o de tipo semántico.

El método depende del orden de entrega garantizado que proporciona el TCP y es, en consecuencia, aplicable igualmente a la señalización H.245 tunelizada o no tunelizada. La señalización tunelizada depende además del orden de procesamiento garantizado en el que múltiples mensajes H.245 se tunelizan en un único mensaje de señalización de llamada H.225.0.

IV.2 Señalización

Todos los canales lógicos alternativos se identifican mediante la utilización de un **forwardLogicalChannelNumber** común en los mensajes de **openLogicalChannel**, un canal alternativo por mensaje. Los mensajes pueden ser enviados vía túnel H.245 (uno o más mensajes OLC por mensaje de señalización de llamada) o utilizando una conexión H.245 separada. Los canales lógicos alternativos se señalizan en orden de conveniencia decreciente, es decir, el primer mensaje OLC especifica el **tipo de datos** que el emisor del OLC preferiría utilizar en el canal lógico.

No es preciso que el receptor de estos mensajes OLC sepa que se está utilizando este método de proposiciones alternativas. Antes de la recepción de una petición de OLC aceptable, rechazará las peticiones de OLC inaceptables, normalmente, con un código de causa de **dataTypeNotSupported** (**tipo de datos no soportado**), **dataTypeNotAvailable** (**tipo de datos no disponible**) o **unknownDataType** (**tipo de datos desconocido**). Cuando se reciba una petición de OLC aceptable, el punto extremo responderá con un mensaje de **openLogicalChannelAck**. Cualesquiera mensajes OLC alternativos recibidos subsiguientemente son rechazados por el receptor con el código de causa **unspecified** (**no especificado**), ya que el número de canal lógico pedido se corresponderá con un canal que esté abierto en ese momento.

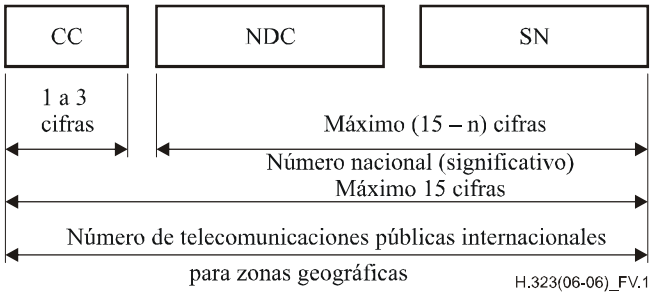
El emisor de una secuencia priorizada de mensajes **openLogicalChannel** como la indicada debe llevar la cuenta del número de mensajes de OLC rechazados recibidos antes de recibir un mensaje **openLogicalChannelAck** a fin de determinar cuál de las alternativas propuestas fue aceptada por la entidad par.

Apéndice V

Utilización de los planes de numeración E.164 e ISO/CEI 11571

V.1 Plan de numeración E.164

El UIT-T define los números E.164 de la forma siguiente para las distintas zonas geográficas (véase la figura V.1):



CC Indicativo de país para zonas geográficas
n Número de cifras del indicativo de país
NDC Indicativo nacional de destino (opcional)
SN Número abonado

NOTA – Los prefijos nacional e internacional no forman parte del número de telecomunicaciones públicas internacionales para zonas geográficas.

Figura V.1/H.323 – Estructura del número de telecomunicaciones públicas internacionales para zonas geográficas

Existen descripciones similares para números no asociados a zonas geográficas. La Rec. UIT-T E.164 define los indicativos de país (CC, *country codes*) para todos los países y regiones del mundo.

Un número internacional E.164 siempre comienza por un indicativo de país y su longitud total es siempre igual o inferior a 15 cifras, y lo que es más importante, no incluye ningún prefijo que forme parte del plan de marcación (por ejemplo, "011" para una llamada internacional realizada desde los Estados Unidos de América o "1" para una llamada nacional de larga distancia), ni incluye la utilización de "#" ni "*". El número "49 30 345 67 00" es un número E.164 cuyo CC es 49 que corresponde a Alemania. El número nacional es el número internacional al que se le ha suprimido el indicativo de país, en este caso es "30 345 67 00". El número de abonado es el número nacional al que se le ha suprimido indicativo nacional de destino, en este ejemplo "345 67 00".

Un número E.164 tiene un significado global: cualquier número E.164 puede ser alcanzado desde cualquier lugar del mundo. Sin embargo, una "secuencia de cifras marcadas" sólo tiene significado en un dominio específico. Por ejemplo, en un plan de numeración privado de una empresa, un prefijo como el "9" puede indicar que la llamada es saliente de dicho ámbito, a partir de lo cual se debe seguir el plan de numeración de la compañía telefónica local. Cada compañía telefónica o red privada puede elegir su propio plan de marcación. También es libre para cambiarlo – como así sucede con frecuencia (por ejemplo, añadiendo nuevos indicativos de área).

En una típica red limitada geográficamente en la que los usuarios realizan la marcación de los números telefónicos de forma manual y en la que los usuarios no viajan demasiado, el hecho de que existan planes de marcación distintos en distintos lugares constituye normalmente un problema. Sin embargo, para que un usuario que viaja pueda realizar llamadas, debe conocer el plan de marcación de la red en cuyo ámbito se encuentra. Cuando la marcación la realiza de forma automática una computadora, el usuario debe adaptar el soporte lógico para cada una de las regiones o de las redes.

Debido a los aspectos anteriores, relativos a los planes de marcación variables y a la marcación automática, es esencial poder hacer referencia a un "número de teléfono" en términos absolutos, en lugar de "lo que usted debe marcar para alcanzarlo desde un localidad específica". Una utilización adecuada de los números E.164 puede resolver estas cuestiones. Muchos sistemas utilizan números E.164 en lugar de cifras marcadas: por ejemplo, una centralita privada (PBX) puede capturar los números marcados por un usuario e iniciar una llamada hacia la compañía telefónica local utilizando un número E.164 en el elemento de información número de la parte llamada especificado en Q.931. Cuando se completa el elemento de información número de la parte llamada, el hecho de especificar que el plan de numeración es "Plan de numeración RDSI/telefonía (Rec. UIT-T E.164)" indica que se trata de un número E.164. Si el tipo de número se especifica como "desconocido" y el plan de numeración se especifica como "desconocido", ello indica que se trata de números marcados.

A continuación se recogen un conjunto de definiciones extraídas de la Rec. UIT-T E.164:

V.1.1 número: Una cadena de cifras decimales que indica singularmente el punto de terminación de la red pública. El número contiene la información necesaria para encaminar la llamada a este punto de terminación.

Un número puede tener un formato determinado a nivel nacional o un formato internacional. El formato internacional se conoce como número de telecomunicaciones públicas internacionales, que incluye el indicativo de país y las cifras subsiguientes, pero no el prefijo internacional.

V.1.2 plan de numeración: Un plan de numeración especifica el formato y la estructura de los números utilizados en ese plan. Típicamente consta de cifras decimales separadas en grupos a fin de identificar elementos específicos utilizados para la identificación y el encaminamiento y en las capacidades de tasación. Por ejemplo, en el plan de numeración E.164, a fin de identificar países, destinos nacionales y abonados.

Un plan de numeración no incluye prefijos ni sufijos ni información adicional necesaria para completar una llamada.

Un plan de numeración nacional es la implementación nacional del plan de numeración E.164.

V.1.3 plan de marcación: Una cadena o combinación de cifras decimales, símbolos e información adicional que definen el método según el cual se utiliza el plan de numeración. Un plan de marcación incluye la utilización de prefijos, sufijos e información adicional, complementaria del plan de numeración y necesaria para completar la llamada.

V.1.4 dirección: Una cadena o combinación de cifras decimales, símbolos e información adicional que identifica el(los) punto(s) de terminación específico(s) de una conexión en una(s) red(es) pública(s) o, donde proceda, en una(s) red(es) privada(s) interconectada(s).

V.1.5 prefijo: Un prefijo es un indicador compuesto por una o más cifras que permite la selección de diferentes tipos de formatos de números, redes y/o servicio.

V.1.6 prefijo internacional: Una cifra o combinación de cifras utilizada para indicar que el número que sigue es un número de telecomunicaciones públicas internacionales.

V.1.7 indicativo de país (CC) para áreas geográficas: La combinación de una, dos o tres cifras que identifica a un país determinado, a países de un plan de numeración integrado o a una determinada área geográfica.

V.1.8 número nacional (significativo)[N(S)N, *national (significant) number*]: La porción del número que sigue al indicativo de país para zonas geográficas. El número nacional (significativo) se compone del indicativo nacional de destino (NDC) seguido por el número del abonado (SN). La función y el formato del N(S)N se determina a nivel nacional.

V.1.9 indicativo nacional de destino (NDC, *national destination code*): Un campo de código opcional a nivel nacional, dentro del plan de numeración E.164, que combinado con el número del abonado (SN), constituirá el número nacional (significativo) del número de telecomunicaciones públicas internacionales para áreas geográficas. El NDC tendrá una función de selección de indicativo de red y/o interurbano.

El NDC puede ser una cifra decimal o una combinación de cifras decimales (sin incluir ningún prefijo) que identifica una zona de numeración dentro de un país (o de un grupo de países incluidos en un plan de numeración integrado o en una área geográfica determinada) y/o redes/servicios.

V.1.10 prefijo (interurbano) nacional: Una cifra o combinación de cifras utilizada por un abonado llamante que efectúa una llamada a un abonado de su propio país pero que está fuera de su propia zona de numeración. Permite tener acceso a los equipos automáticos interurbanos de salida.

V.1.11 número de abonado (SN, *subscriber number*): El número que identifica a un abonado en una red o zona de numeración.

V.2 Números de red privada

Los números de redes privadas se utilizan en redes telefónicas privadas o redes privadas virtuales, como por ejemplo, una red corporativa formadas por PBX y líneas privadas virtuales.

En ISO/CEI 11571 de define que un plan de numeración privado (PNP, *private numbering plan*) se compone de hasta tres niveles regionales.

Un número PNP se compone de una secuencia de x cifras decimales (0,1,2,3,4,5,6,7,8,9) con la posibilidad de que distintos números del mismo PNP puede tener distintos valores de x. El valor máximo de x será el mismo que el del plan de numeración público RDSI, véanse la Rec. UIT-T E.164 y la figura V.2.

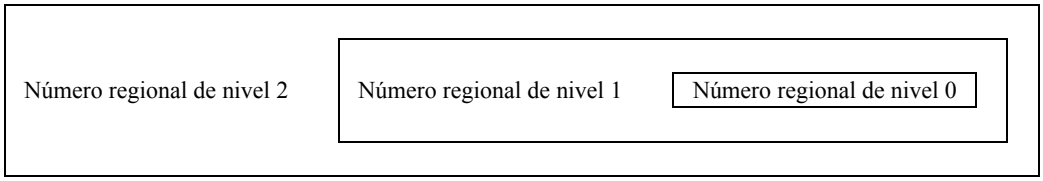


Figura V.2/H.323 – Estructura de un número PNP con tres niveles de regiones

Un número regional (RN, *regional number*) de nivel n sólo tendrá significado en la región de nivel n en la que es aplicable. Cuando dicho número se utiliza fuera de dicha región de nivel n, se hará en forma de un RN de nivel superior a n. Sólo un número completo tendrá sentido en todo el ámbito del PNP.

Un ejemplo típico en Norteamérica es la utilización de números de "extensiones" de 4 cifras como número regional de nivel 0; un "indicativo de localidad" de 3 cifras combinado con la "extensión" de 4 cifras constituiría el número regional de nivel 1. No existiría el número regional de nivel 2.

También se podría utilizar un prefijo para indicar qué número regional se utiliza, y éste no sería parte del número regional propiamente dicho, sino sólo del plan de marcación. Un ejemplo típico sería la utilización de la cifra "6" para acceder al número regional de nivel 1, sin utilizar cifra alguna para el número regional de nivel 0.

Las definiciones siguientes han sido extraídas de ISO/CEI 11571:

V.2.1 plan de numeración privado (PNP, *private numbering plan*): Plan de numeración específico de un dominio de numeración privado, definido por el administrador PISN de dicho dominio.

V.2.2 número PNP: Un número que pertenece a un PNP.

V.2.3 región: Todo el domino de un PNP o un subdominio del mismo. Una región no se corresponde necesariamente con la zona geográfica de un PNP.

V.2.4 indicativo de región (RC, *region code*): Son las primeras cifras de un número PNP que identifican una región. El RC puede omitirse con el fin de disponer de una forma abreviada de un número PNP para ser usado internamente en dicha región.

V.2.5 número regional (RN, *regional number*): Forma particular de un número PNP que resulta inequívoco dentro de la región en cuestión.

V.2.6 número completo: Un número que resulta inequívoco en todo el PNP, es decir, que corresponde al nivel regional más elevado utilizado en dicho PNP.

V.3 Utilización de las versiones 1, 2 y 3 de H.323

Los sistemas realizados en base a las versiones 1, 2 y 3 presentaban un problema de terminología con respecto a las cifras marcadas y a los números E.164 reales. Las referencias a las direcciones E.164 que se realizaban en dichas versiones hacían de hecho referencia a los números marcados y no a las cifras E.164, se refieren actualmente al número E.164 real se ubicaba en el campo **publicNumber** (**número público**) y no en el campo **e164**. El campo **e164** se correspondía, por tanto, con una secuencia de cifras marcadas.

En la versión 4 de esta Recomendación, el campo **e164** se ha rebautizado como **dialledDigits** (**cifras marcadas**) y el campo **publicNumber** se ha rebautizado como **e164Number** (**número e164**). El cambio de nombre pretende indicar más explícitamente que las cifras marcadas deberán almacenarse en el campo **dialledDigits** y que los números E.164 deberán almacenarse en el campo **e164Number**.

Apéndice VI

Descripción de un sistema H.323 típico por IP

Este apéndice describe una pila típica H.323. La figura VI.1 ilustra cómo se implementan los medios y la señalización de llamadas H.225.0 y RAS utilizando la infraestructura IP.

La flecha entre H.245 y H.225.0 indica que H.245 se puede tunelizar en H.225.0.

La flecha entre la señalización de llamada H.225.0 y RAS H.225.0 indica que la señalización de llamada H.225.0 se puede tunelizar en RAS H.225.0.

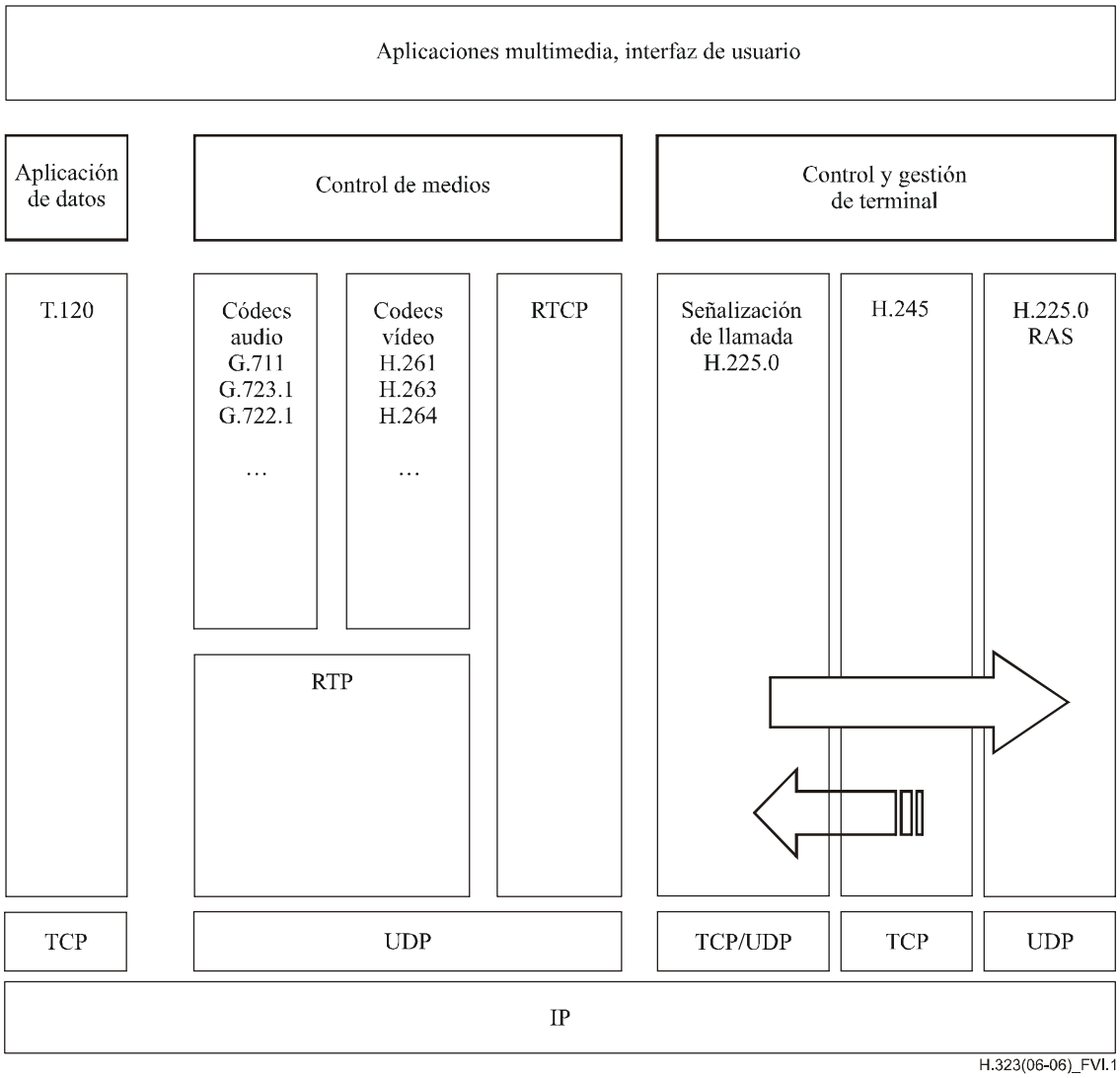


Figura VI.1/H.323 – Una pila H.323 típica por IP

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2007