2. El estándar H.323

2.1 Documentación y pila de protocolos

El estándar **H.323**, desarrollado por la **ITU-T** desde 1996, es un documento "paraguas" que describe el uso de un conjunto de especificaciones para el transporte de servicios de conferencia multimedia basados en paquetes [52]. La pila de protocolos completa para H.323 se muestra en la figura 7:

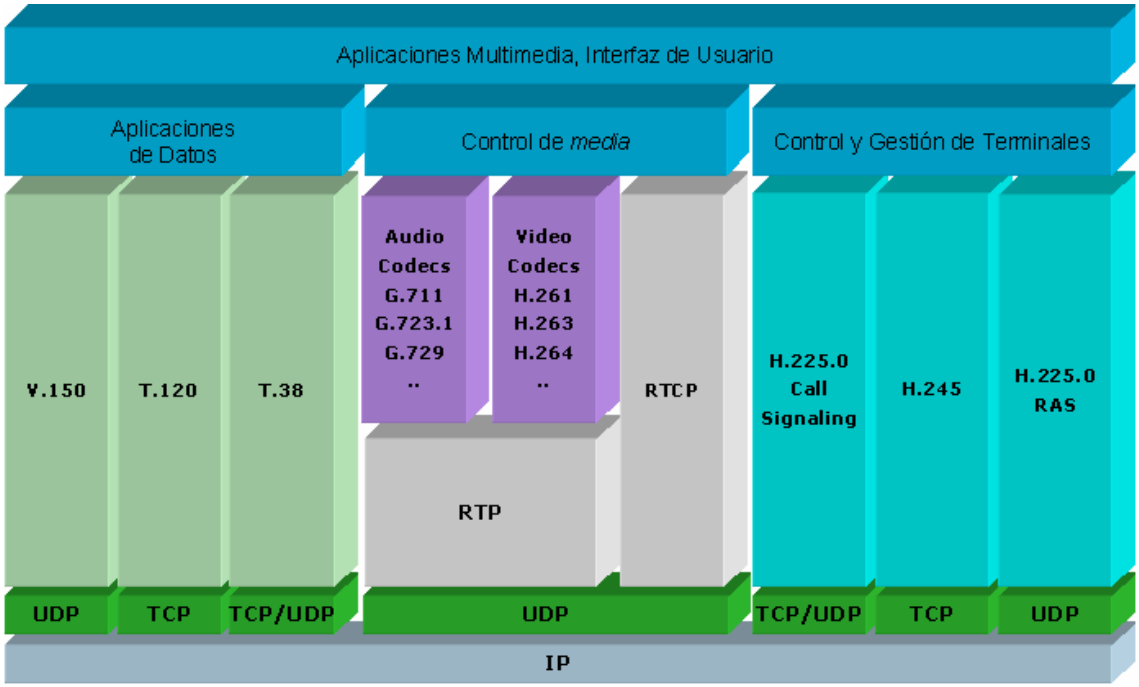

Figura 7: Pila de protocolos H.323.

Los documentos base para la descripción del protocolo H.323, conjuntamente con el estándar H.323 propiamente dicho, son los estándares H.225.0 y H.245:

- **H.225.0** describe el uso de tres protocolos de señalización: RAS (Registro, Admisión, eStado), señalización de llamada Q.931, y el protocolo conocido como Anexo G (o como Anexo G/H.225.0).
- El estándar **H.245** describe un protocolo de control multimedia; es común a los estándares "paraguas" H.310, H.323 y H.324.

Las especificaciones "base" para definir el protocolo de comunicaciones H.323 son, por lo tanto, la especificación H.323 propiamente dicha, la H.225.0 y la H.245.

Por otro lado, se utiliza ASN.1 (*Abstract Syntax Notation* 1) para definir una sintaxis abstracta de representación de los datos de señalización y control, así como las PER[34] que transforman estos datos en un flujo binario. ASN.1 se encuentra disponible en las especificaciones X.680-683, y las PER, en la X.691, de la ITU-T.

Para manejar los flujos de audio y vídeo se utiliza el protocolo de transporte en de datos en tiempo real RTP *Real-Time Transport Protocol*, (así como su apartado de control, RTCP[35]), desarrollado por la IETF.

En cuanto al transporte, H.323 usa comunicaciones fiables para algunas comunicaciones de control (típicamente TCP) y no fiables para el resto de las comunicaciones (especialmente para los flujos de audio y vídeo, RTP/RTCP, y que típicamente se llevarán a cabo con UDP). Igualmente, aunque estas comunicaciones se efectúan típicamente sobre IP, el estándar no refiere ningún protocolo de red específico.

Por último, para la transmisión de audio y de vídeo se utilizan algoritmos de compresión y códecs, siendo obligatorios el soporte de los algoritmos G.711 para audio y H.261 para vídeo (ambos de la ITU-T). Para conferencias de datos se utiliza el estándar T.120, el V.150 para comunicaciones de módem y el T.38 para fax (todos de la ITU), entre otros.

Como documentación adicional, H.323 incluye también los estándares:

- H.235, estándar que describe mecanismos de seguridad en redes basadas en sistemas de control H.245.
- H.248, MEGACO, en donde se describe la comunicación interna de los elementos de las pasarelas entre H.323 y otras redes.
- H.450.x, en donde se describen algunos servicios suplementarios.
- H.460.x, con algunas extensiones de H.323.
- H.501, para gestión de la movilidad y comunicaciones inter/intra dominio.
- H.510, documento en el que se describen el usuario, el terminal y el servicio de movilidad.
- H.530, donde se describen mecanismos de seguridad para H.510.

Además, las *H.323-Series Implementers Guides*, es decir las guías de implementación H.323, se refieren a temas cubiertos inadecuadamente por las recomendaciones, así como correcciones de las mismas. Estas guías se actualizan cada nueve meses aproximadamente y deben ser leídas conjuntamente con las especificaciones.

Y, por último, los anexos y los apéndices. Los anexos son normativos (es decir, que forman parte de la recomendación), mientras que los apéndices sólo son de carácter informativo.
En la figura 8 se enuncian todos los anexos y apéndices de cada una de las especificaciones base de H.323, de cuyos nombres pueden extraerse los apartados cubiertos por cada uno, y

[34] PER: *Packet Encoding Rules*, reglas de codificación de paquetes.
[35] RTCP: *Real-Time Transport Control Protocol*, protocolo de control para el transporte de datos en tiempo real, anejo a RTP y dedicado al control de características de retardo y de *jitter* en las comunicaciones RTP.

que pueden resultar muy útiles cuando se necesite consultar alguna cuestión relacionada con ellos:

Los anexos de la especificación H.323 son:
- Annex A – Mandatory H.245 messages
- Annex B – Procedures for layered video codecs
- Annex C – H.323 on ATM
- Annex D – Fax
- Annex E – UDP for Call Signaling
- Annex F – Simple Endpoint Type (SET)
- Annex G – Text telephony
- Annex I – Error prone channels *(work in progress)*
- Annex J – Secure SET
- Annex K – HTTP-based service control
- Annex L – Stimulus control protocol
- Annex M.x – Tunneling of various protocols within H.323
- Annex N – QoS *(work in progress)*
- Annex O – Use of DNS *(work in progress)*
- Annex P – Modem over IP
- Annex Q – Far-end camera control
- Annex R – Robustness

Los apéndices son:
- Appendix I – Sample MC/terminal communications
- Appendix II – Usage of RSVP
- Appendix III – Gatekeeper based user location
- Appendix IV - Signaling prioritized alternative logical channels in H.245
- Appendix V - Use of E.164 and ISO/IEC 11571 numbering plans

Mientras, para la especificación H.225.0 se especifican los siguientes anexos:
- Annex A – RTP/RTCP (RFC 1889)
- Annex B – RTP profile (RFC 1890)
- Annex C – RTP payload for H.261
- Annex D – RTP payload for H.261A
- Annex E – Video packetization
- Annex F – Audio and multiplexed packetization
- Annex G – Communication between and within Administrative Domains
- Annex H – ASN.1 Syntax
- Annex I – H.263+ packetization
- Y los apéndices:
- Appendix I – RTP/RTCP algorithms (reference to RFC 1889)
- Appendix II – RTP profile (reference to RFC 1890)
- Appendix III – H.261 packetization (reference to RFC 2032)
- Appendix IV – TCP/IP/UDP usage
- Appendix V – ASN.1 usage

Por último, para la especificación H.245, los anexos:
- Annex A – ASN.1 syntax
- Annex B – Semantic definition of messages
- Annex C – Procedures
- Annex D – Object identifier assignments
- Annex E to M – Various “generic capability” definitions, including some codecs

Y los apéndices:
- Appendix I – Overview of ASN.1
- Appendix II – Example of H.245 procedures
- Appendix III – Timers and counters
- Appendix IV – H.245 extension procedure
- Appendix V – Using “replacementFor”
- Appendix VI – Example H.263 capabilities
- Appendix VII – Procedures and template for generic capabilities
- Appendix VIII – List of generic capabilities for H.245 defined in other Recommendations

```
• Appendix IX – Usage of ASN.1 in H.245
```

Figura 8: Lista completa de los Anexos y apéndices de H.323.

Sólo los textos que suponen el núcleo de H.323 suponen más de mil ochocientas páginas. A pesar de que su implementación es directa (gracias a las definiciones ASN.1 y a la estandarización de las máquinas de estado para cada servicio H.323), la revisión de todos y cada uno de los aspectos relacionados con H.323, a la hora de elaborar un producto compatible, resulta muy costosa.

2.2 Grupos de estudio en la ITU-T

El estudio y desarrollo de servicios y sistemas multimedia, por parte de la ITU-T, sigue tomándose lugar en el *Study Group* 16, organizado en cuatro WPs (*Working Parties*). En el contexto de H.323, los más importantes son los WP2 y WP4. La figura 9 muestra una visión general de las Cuestiones más importantes que, en dichos grupos de estudio, se refieren a H.323.

La Cuestión B/16 en el WP4 define un marco de trabajo en el que se establecen las arquitecturas básicas comunes a diferentes sistemas multimedia (H.323, H.320, H.324), intentando identificar las sinergias que puedan existir entre ellos. La Cuestión C/16 identifica y describe servicios y aplicaciones multimedia que funcionen sobre sistemas multimedia. El estándar H.323 y sus protocolos núcleo se estudian en la Cuestión 2/16. Detalles de interoperabilidad se estudian en las cuestiones D/16 y 3/16, incluyéndose la interoperabilidad con la PSTN y entre los diferentes servicios suplementarios.

Muchas otras Cuestiones en el WP2 estudian cómo resolver temas más generales, como QoS, movilidad o seguridad, en los sistemas multimedia. Esto comprende la integración y el uso de los protocolos y métodos ya descritos así como la definición de otros nuevos.

Cuestión	Título	Tareas	Estándares (ejemplos)
Working Party 2: Plataformas Multimedia e Interoperabilidad			
D/16	Interoperabilidad entre Sistemas y Servicios Multimedia	Interoperabilidad de servicios (como los servicios suplementarios), y de sistemas multimedia entre sí y con GSTN; medidas para aumentar la interoperabilidad de las distintas implementaciones.	H.246
F/16	Calidad de Servicio y Rendimiento extremo a extremo en Sistemas Multimedia	Necesidades de QoS en sistemas multimedia; métodos de señalización de QoS; aplicaciones comunes para distintos métodos de señalización; aspectos de rendimiento extremo a extremo según la percepción del usuario.	Contribuciones a estándares de otras Cuestiones
G/16	Seguridad en Sistemas y Servicios Multimedia	Análisis de amenazas de sistemas y servicios multimedia; definición de un marco de trabajo para seguridad; contribuciones a las arquitecturas multimedia para incorporar seguridad.	H.235
1/16	Sistemas Multimedia, Terminales y Conferencias de Datos	Mejoras de las comunicaciones audiovisuales sobre redes fijas y móviles, y RDSI; intercambio de datos; mejoras en el uso de las codificaciones de audio y vídeo.	H.310, H.320, H.321, H.324, T.120

2/16	Multimedia sobre Redes de Paquetes usando sistemas H.323	Protocolos núcleo de H.323, y servicios suplementarios.	H.323, H.225, H.245, H.332
3/16	Infraestructura e Interoperabilidad para Multimedia sobre Sistemas basados en Redes de Paquetes	Pasarelas H.323 e interoperabilidad con la PSTN y con SS7; descomposición de pasarelas; MCUs; gestión de sistemas H.323; H.323 MIB; actualizaciones de la señalización de control.	H.245, H.246, H.248, H.341
4/16	Conferencias de Vídeo y Datos usando servicios de Internet	Arquitectura de protocolos para integración de funciones de conferencia de vídeo y datos, e integración con servicios de Internet; mecanismos de sincronización entre presentaciones audiovisuales y otros servicios; multiconferencias.	Ninguno, por el momento
5/16	Movilidad para Sistemas y Servicios Multimedia	Desarrollo avanzado de movilidad para H.323 y H.324; consideraciones de protocolo; consideraciones sobre terminales y servicios.	H.501, H.510, y contribuciones a estándares de otras Cuestiones
Working Party 4: Marco de trabajo Multimedia			
B/16	Arquitecturas Multimedia	Marco de trabajo común para arquitecturas de proyectos multimedia; consistencia entre sistemas multimedia; elementos de soporte común a protocolos y arquitecturas (como H.245).	Marco de trabajo para arquitecturas multimedia
C/16	Aplicaciones y Servicios Multimedia	Identificación de servicios y aplicaciones multimedia; descripciones de servicios (servicios de distribución, servicios de mensajería, de emergencia, de pago, de comercio electrónico, aplicaciones de telemedicina, etc).	Series F

Figura 9: Algunas de las actividades más importantes relacionadas con H.323 en el ITU-T SG16

2.3 Características fundamentales de H.323

Las características que ofrece este estándar, en cuanto a comunicaciones multimedia, son:

- **Interoperabilidad entre distintos fabricantes**. En realidad, éste es el ánimo de todos los estándares de comunicaciones; sin embargo, precisamente debido a su complejidad, H.323 intenta acotar todas las posibilidades de la comunicación, de las capacidades y de la funcionalidad de cada elemento de la red, incluso las posibles ampliaciones de sí mismo, de forma que en la comunicación exista al menos un conjunto fundamental común a cualquier elemento de la comunicación.
- **Independencia de la red**. La definición de H.323 hace referencia a redes de paquetes que no provean calidad de servicio, pero no especifica ningún protocolo de red en concreto.
- **Independencia de la plataforma y de la aplicación**. Siempre que se cumplan los requisitos y procedimientos descritos en las especificaciones, podrá hacer uso de H.323 cualquier plataforma, hardware o sistema operativo deseado.
- **Soporte para multiconferencias**. Aunque H.323 permite mantener multiconferencias sin el uso de unidades especializadas, las MCUs (*Multipoint Control Units*)

proporcionan una arquitectura más robusta y flexible para el mantenimiento de multiconferencias.

- **Gestión del ancho de banda**. El tráfico de audio y de vídeo resulta costoso en cuanto a recursos de ancho de banda, y podría colapsar la red. H.323 permite la gestión del ancho de banda, pudiendo limitar el número de conexiones H.323 simultáneas, así como especificarles el ancho de banda disponible a aplicaciones y terminales H.323.
- **Soporte para transmisión en multicast**. Multicast es un método de transporte que permite enviar un solo paquete hacia un conjunto de destinos sin replicación (frente a unicast, que utilizaría múltiples transmisiones punto a punto, y a broadcast, que enviaría el paquete a todas los destinos), haciendo un uso mucho más eficiente del ancho de banda.
- **Soporte para el establecimiento de conferencias entre distintas redes multimedia**. H.323 establece mecanismos para unir sistemas basados en comunicaciones LAN con sistemas RDSI[36], así como con las redes PSTN, tanto en audio como en videoconferencias. Esto se consigue gracias a la especificación de un terminal de red encargado de estas interconexiones: las pasarelas o *gateways*.
- **Seguridad**. Mediante H.235, se establecen procedimientos de autenticación, integridad de los paquetes, privacidad (mediante mecanismos de encriptación) y no repudio (es decir, medios de protección contra la afirmación de no haber participado en una conferencia).
- **Establecimiento de llamada rápido (*Fast Call*)**. H.323 también establece mecanismos para que la llamada quede establecida con un mínimo de dos paquetes.
- **Intercambio de requerimiento de calidad de servicio**. Un destino puede especificar una calidad de servicio deseada para sus flujos de audio y vídeo, incluyéndose parámetros RSVP[37] (RFC 2205 [53]).
- **Capacidades para la redundancia de la red**. Mediante servidores de direccionamiento alternativos ("*alternate* Gatekeepers") la red podrá soportar la caída de estos equipos críticos, sin pérdida de comunicación.
- **Descripción genérica de capacidades**. Mediante esta especificación ASN.1, pueden describirse códecs y formatos de audio o vídeo genéricos, sin perturbar las capacidades de comunicación dentro de los estándares más habituales.
- **Gestión del direccionamiento entre dominios administrativos**. Se establecen flexibles mecanismos de escalado para el establecimiento de llamadas entre grandes redes internacionales, mediante la definición, entre los Gatekeepers encargados del direccionamiento de la red, de los llamados elementos de borde o *border elements*.
- **Terminales simples, SET (*Simple Endpoint Type*)**. Como la especificación H.323 puede resultar demasiado extensa para terminales sencillos, la especificación H.341 recoge los mecanismos mínimos para asegurar la comunicación en redes H.323 de terminales con una funcionalidad básica.
- **Servicios suplementarios**. Dentro de los servicios asociados a conferencias, H.323 añade numerosas posibilidades, entre las cuales se destacan:
    - **Transferencia de llamada**: permite que una conferencia establecida entre A y B pase a establecerse entre B y C.

[36] RDSI: Red Digital de Servicios Integrados.
[37] RSVP: *Resource reSerVation Protocol*, protocolo de reserva de resursos.

  - **Desvío de llamada**: ante cierto estado del receptor, la llamada se desvía a otro número antes de establecerse.
  - **Llamada *On Hold***: una llamada puede dejarse inactiva durante un tiempo, para recuperarse la comunicación más tarde, sin necesidad de colgarla ni de establecerla de nuevo.
  - **Conferencia sin consulta**: es el caso, por ejemplo, de una llamada que pasa por una secretaria, y que luego ésta conecta con el destino verdaderamente deseado.
  - **Llamada en espera**: mientras se tiene una llamada activa, un terminal puede recibir una nueva llamada, que se queda como llamada entrante hasta que este terminal decide descolgarla (colgando la anterior llamada, o dejándola *on hold*, por ejemplo).
  - **Identificación del número llamante**.
  - **Establecimiento de prioridades**: posibilidad de establecer prioridades entre las distintas llamadas.
  - **Control de los planes de marcado**: establecimiento, de manera centralizada, de qué números se permiten como destinos rutables, y de cuáles deben ser rechazados de inmediato con sólo ser marcados.

- **Mecanismos de control basados en HTTP**. Mediante el Anexo K/H.323, se permite a los proveedores de servicio mostrar páginas web con contenidos obtenidos desde la red H.323, mediante comunicaciones de control sobre HTTP.
- **Capacidades de gestión de llamadas a crédito**. A partir de la versión 4 se establecen mecanismos para la comunicación de información relativa a llamadas a crédito en el mismo protocolo RAS (como, por ejemplo, mediante tarjetas prepago).
- **Uso de DNS**[38] **para la resolución de direcciones**. En la versión 5 se describen mecanismos para la solución de direcciones mediante servidores DNS a partir de alias de destinos del tipo URL[39].
- **Descripción genérica de servicios suplementarios**. Mediante el *Stimulus Control Protocol* (protocolo de control por estímulos) descrito en el Anexo L/H.323, pueden definirse servicios suplementarios para puntos finales, sin cargo añadido en su software H.323. Para ello, hace uso de un servidor de capacidades o *Feature Server*, que hace de proxy entre este terminal y sus comunicaciones H.323.
- **Robustez**. El Anexo R/H.323 describe mecanismos para asegurar la robustez de las comunicaciones ante errores sencillos en la comunicación.
- **Monitorización de la calidad de servicio**. Con la especificación H.460.9, perteneciente a la versión 5, los Gatekeepers pueden informar de las características de calidad de servicio en tiempo real.
- **Mecanismos para gestión de la movilidad**. Mediante las especificaciones H.501, H.510 y H.530.

Muchas de estas características son opcionales; además, algunos equipos sólo se adaptan a versiones tempranas de la especificación H.323; y otros sencillamente no permiten la configuración de algunos de los servicios H.323 ofrecidos.

[38] DNS: *Domain Name System*, sistema de nombres de dominios.
[39] URL: *Universal Resource Locator*, cadena de caracteres que refiere la dirección de un recurso de Internet.

2.4 Arquitectura de H.323

H.323 define cuatro elementos fundamentales en la arquitectura de red (figura 10):

- Terminales.
- Pasarelas o *gateways*.
- Gatekeepers y *border elements*.
- Y MCUs.

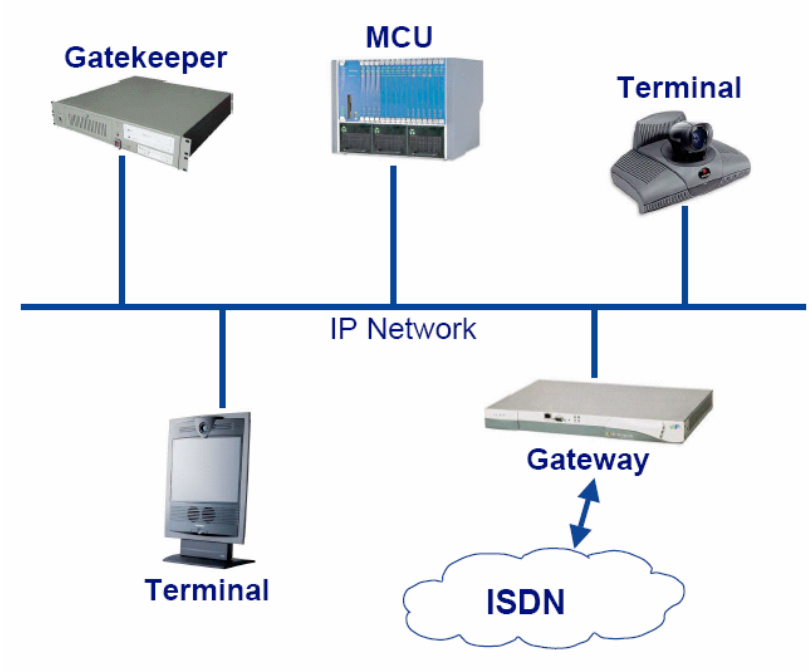

Figura 10: Elementos de una red H.323.

2.4.1 Terminales

Los terminales son puntos finales de la red que permiten comunicaciones bidireccionales en tiempo real. Todo terminal debe permitir comunicaciones de voz, mientras que los vídeos o los datos son opcionales. También debe soportar H.245, que es el protocolo usado para negociar el uso de los canales y las características de los datos. También serán obligatorios otros tres componentes: Q.931 para señalización de llamada, RAS para comunicaciones con un Gatekeeper, y soporte para RTP/RTCP para la secuenciación de paquetes de audio y de vídeo.

Los terminales más habituales que pueden encontrarse son teléfonos, videoteléfonos, dispositivos IVR (*Interactive Voice Response*), sistemas de buzón de voz o teléfonos software.

2.4.2 Pasarelas

Las pasarelas son los elementos de la red H.323 preparados para la interoperabilidad con otras redes. Se distinguen dos elementos en la arquitectura interna de una pasarela:

- El **MGC** (*Media Gateway Controller*), es el encargado de la gestión y traducción de los elementos de la comunicación relativos a la señalización de llamada en ambos extremos (como H.225.0 y SS7, por ejemplo). Controla así la facción de más de alto nivel de las comunicaciones de la pasarela.
- El **MG** (*Media Gateway*), que maneja y traduce los formatos de audio, vídeo o datos sobre las distintas interfaces, controlando la facción de más bajo nivel.

La comunicación entre el MGC y los MGs se lleva a cabo mediante una especificación separada, la H.248, también conocida como MEGACO (*MEdia GAteway COntrol*), y, como resultado de la colaboración entre el IETF y la ITU-T, también disponible en la RFC 3015.

Como ejemplos de pasarelas, las pasarelas analógicas con la PSTN, las pasarelas digitales con RDSI, o incluso pasarelas con otras redes H.323 (*proxys* de red). Entre otras capacidades, las pasarelas con la PSTN deberán poder reconocer señales DTMF[40] y transmitirlas por H.323.

2.4.3 Gatekeepers

Los Gatekeepers son los elementos más importantes de una red H.323, a pesar de que su existencia es opcional. Actúan como punto central para todas las llamadas de su Zona, y proporciona servicios de control de llamadas a todos los puntos finales registrados en él. De esta forma, una Zona es el grupo de terminales, pasarelas y MCUs gestionados por un Gatekeeper.

- El servicio de control de llamadas más importante que realiza un Gatekeeper es la traducción de direcciones, de alias de red (entre los cuales se pueden encontrar números marcados, secuencias de caracteres, direcciones URL o emails), a direcciones de transporte (típicamente, direcciones IP). De esta forma, en una red sin Gatekeepers los terminales tendrían que conocer la dirección de transporte de cada destino de sus comunicaciones. El Gatekeeper también tiene la capacidad de modificar el alias a que se refirió el terminal que inició la llamada.
- Pero también se encarga del control de accesos: si existe un Gatekeeper en la Zona H.323, cada uno de los terminales que deseen comenzar o recibir una llamada deberá solicitar acceso a su Gatekeeper.
- La tercera de sus tareas base es el control del ancho de banda de la red H.323, permitiendo o denegando llamadas en los casos en los que el tráfico supere ciertos límites, previamente configurados. El Gatekeeper dispone de mecanismos para conocer numerosos detalles acerca de cada llamada activa en su Zona. Incluso, si fuera necesario, podría cortar una llamada durante el transcurso de una comunicación.

[40] DTMF: *Dual-Tone Multi-Frecuency*, transmisión de tonos dual, es decir que cada dígito se configura con dos tonos simultáneos.

Por último, el Gatekeeper desempeñará funciones de gestión de Zona, encargándose de:

- Comunicar e intercambiar las tablas de rutas relativas a su Zona con otros Gatekeepers.
- Comunicar estadísticas relativas a la calidad de servicio de los terminales en su Zona en tiempo real
- Distribuir planes de marcado entre estos terminales.

Al resultar un elemento tan imprescindible en las comunicaciones de una red H.323, el estándar dispone potentes capacidades de redundancia para estos elementos: se trata de los *alternate Gatekeepers*, una lista de Gatekeepers alternativos de que dispone cada terminal en caso de caída de su Gatekeeper, para que en ningún momento se carezca de las informaciones de direccionamiento.

Además, los Gatekeepers pueden mantener entre sí varios niveles jerárquicos, mediante los llamados elementos de borde, que permiten la comunicación de informaciones de direccionamiento entre ellos de forma efectiva:

2.4.3.1 Border Elements

Los elementos de borde suponen un nivel más en la jerarquía de direccionamiento H.323, dotando de mayor flexibilidad y potencia a la gestión de rutas. En realidad su funcionamiento es como el de cualquier Gatekeeper, sólo que, además, guardan en su interior la información de tablas de rutas de todos los Gatekeepers dentro de su Dominio Administrativo, participando además de la autorización de llamada entre estos dominios. Un Dominio Administrativo no es, en definitiva, sino un conjunto de Zonas bajo el control de un único elemento de borde.

Por lo demás, el elemento de borde comparte el resto de funciones del Gatekeeper, existiendo, por ejemplo, la posibilidad de definir *alternate Border Elements* en cada Gatekeeper.

2.4.4 MCUs

Las **MCU**s (*Multipoint Control Units*, unidades de control multipunto) soportan la gestión de las multiconferencias. Son elementos opcionales, pero su uso resulta una potente capacidad para administrar y gestionar multiconferencias de forma robusta.

Una MCU se descompone en un **MC** (*Multipoint Controller*, controlador multipunto), y en cero o varios **MP**s (*Multipoint Processors*). El MC gestiona la señalización de las llamadas entre todos los terminales, estableciendo las capacidades para procesado de audio y vídeo entre todos, y determinando qué flujos se establecerán en multicast. Mientras, los MPs mezclarán, conmutarán y procesarán los flujos de datos en tiempo real.

Las multiconferencias pueden establecerse en varias formas, según las necesidades de la red H.323 y de las capacidades de los terminales participantes:

- **Centralizada**: Requieren la existencia de una MCU. Todos los terminales enviarán audio, vídeo, datos y flujos de control a la MCU en formato punto a punto. El MC centralizará la gestión de la multiconferencia, y el MP se encargará del mezclado de audio, la distribución de los datos y la conmutación y mezclado del vídeo, enviando los flujos resultantes a cada uno de los participantes de la multiconferencia, punto a punto o multipunto (sólo para el flujo de vídeo). El MP también permitirá conversiones de formatos (códecs). Se muestra un diagrama de este tipo de multiconferencia, aplicado a comunicaciones de vídeo, en la figura 11.

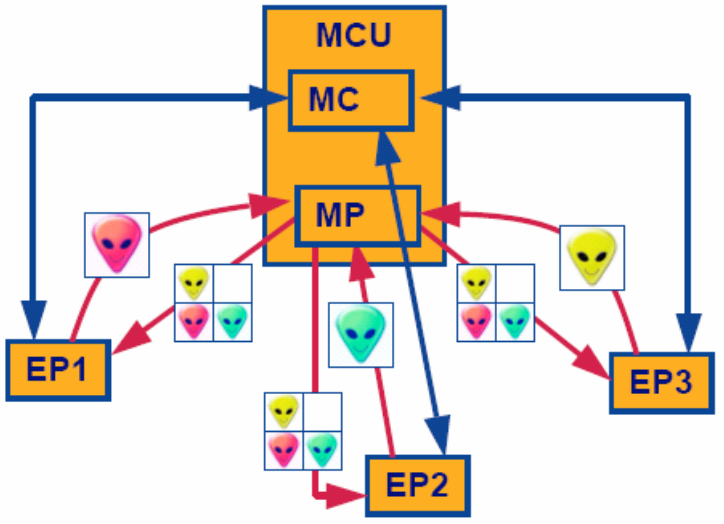

Figura 11: Multiconferencia centralizada. Transmisiones de datos unicast.

- **Descentralizada**: En este caso se podrá hacer uso de la tecnología multicast, mediante la que cada terminal envía los datos al resto de los participantes. Ahora, son cada uno de los terminales los encargados de procesar los múltiples flujos entrantes de audio y de vídeo, mediante funciones internas de MP. Mientras, el MC se encarga aún de la gestión y control de la multiconferencia, comunicándose punto a punto con todos los canales de control de cada participante y llevando a cabo funciones tan interesantes como el control de silla (*chair control*) y la selección de vídeo. La figura 12 muestra un esquema para este tipo de multiconferencias:

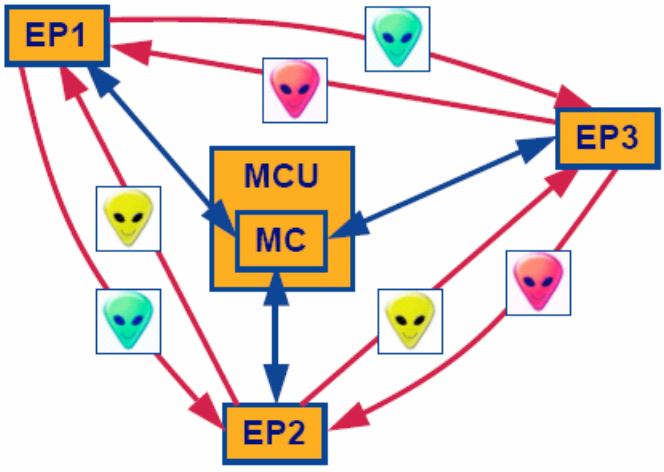

Figura 12: Multiconferencia descentralizada. Transferencia de los datos multicast.

- **Híbrida**: Una multiconferencia híbrida usará una determinada combinación de las capacidades de gestión centralizada y descentralizada. La MCU podría mezclar sólo el audio, dejando el vídeo en formato descentralizado. Por otro lado, en una multiconferencia híbrida también podría haber participantes que mantuvieran una multiconferencia centralizada a la par que otros participantes de la misma multiconferencia sólo utilizaran multicast; el nexo de unión sería la MCU. Así, cada terminal sólo debe preocuparse de la forma de conferencia en que envía y recibe, nunca de la naturaleza mixta de la multiconferencia.

2.5 Protocolos de comunicación H.323

2.5.1 Introducción

Las comunicaciones en H.323 son una combinación de señales de audio, vídeo, datos, y de señalización y control. Las capacidades de audio, señalización de llamada Q.931, control RAS y señalización H.245 son obligatorias en todos los terminales.

Las funciones de control de llamada son el núcleo de un terminal H.323. Estas funciones incluyen señalización para establecimiento de llamada, intercambio de capacidades, señalización de comandos e indicaciones, y mensajes de apertura y descripción del contenido de los canales lógicos. Éstas son las funciones que llevan a cabo los protocolos H.225.0, RAS y H.245:

- La función de señalización **RAS** establece un canal para las comunicaciones entre los terminales y su Gatekeeper, el cual los registra y admite, y además guarda información relativa al estado de cada terminal de su Zona.
- El canal de señalización de llamada se basa en **Q.931**, y sirve para establecer la primera conexión entre dos terminales.
- El canal de control **H.245** es un canal confiable que transporta señales de control que gobiernan las operaciones de la entidad H.323, incluyendo intercambio de capacidades, apertura y cierre de canales lógicos, peticiones de preferencias y mensajes de control de flujo, entre otros comandos e indicaciones. Tras el diálogo H.245 se abren los canales lógicos que transportarán todos los datos multimedia por RTP.

En los siguientes capítulos se estudiarán cada uno de estos protocolos con más detalle.

2.5.2 Usando la notación abstracta ASN.1 para H.323

El lenguaje sintáctico abstracto 1 (*Abstract Syntax Notation* 1) se encarga de la definición de estructuras de datos que, junto con las reglas de codificación de paquetes PER que traducen estos datos a una codificación binaria apta para ser transmitida directamente por el medio de transporte, permiten que el protocolo (situado dentro de estas estructuras de datos, es decir definido mediante las mismas) sea independiente de esta codificación.

De esta forma se consigue que la definición del lenguaje H.323 no necesite de representación binaria, como por ejemplo hace RTP, sino que sólo será necesario definir las estructuras de los paquetes (computacionalmente tratables como objetos o clases), sobre los que a posteriori se aplicaría una función de “encode()” para transmitir, o de “decode()” para la recepción (funciones que se encargarían de traducir a las PER).

En ASN.1 se definen módulos para cada protocolo de H.323. Por otro lado, un módulo podrá adoptar definiciones de otros módulos: para esto, computacionalmente hablando, hará falta usar un compilador ASN.1.

Los módulos ASN.1 son un conjunto de elementos formados por partes, usados para la definición de tipos extensos que, además, permiten la exportación e importación de algunas partes entre sí. La figura 13 muestra la definición de módulo se presenta con los siguientes elementos (tomado directamente de la X.680):

```
   ModuleDefinition ::=
          ModuleIdentifier
          DEFINITIONS
          TagDefault
          ExtensionDefault
          "::="
          BEGIN
          ModuleBody
          END

-- a continuación, pasa a definirse cada una de las partes:
   ModuleIdentifier ::=
          modulereference
          DefinitiveIdentifier

   DefinitiveIdentifier ::=
          "{" DefinitiveObjIdComponentList "}"
          | empty

   DefinitiveObjIdComponentList ::=
          DefinitiveObjIdComponent
          | DefinitiveObjIdComponent DefinitiveObjIdComponentList

   DefinitiveObjIdComponent ::=
          NameForm
          | DefinitiveNumberForm
          | DefinitiveNameAndNumberForm

   DefinitiveNumberForm ::= number

   DefinitiveNameAndNumberForm ::= identifier "(" DefinitiveNumberForm ")"

   TagDefault ::=
          EXPLICIT TAGS
          | IMPLICIT TAGS
          | AUTOMATIC TAGS
          | empty

   ExtensionDefault ::=
          EXTENSIBILITY IMPLIED
          | empty

   ModuleBody ::=
          Exports Imports AssignmentList
          | empty
```

```
Exports ::=
       EXPORTS SymbolsExported ";"
       | EXPORTS ALL ";"
       | empty

SymbolsExported ::=
       SymbolList
       | empty

Imports ::=
       IMPORTS SymbolsImported ";"
       | empty

SymbolsImported ::=
       SymbolsFromModuleList
       | empty

SymbolsFromModuleList ::=
       SymbolsFromModule
       | SymbolsFromModuleList SymbolsFromModule

SymbolsFromModule ::=
SymbolList FROM GlobalModuleReference

GlobalModuleReference ::=
modulereference AssignedIdentifier

AssignedIdentifier ::=
       ObjectIdentifierValue
       | DefinedValue
       | empty

SymbolList ::=
       Symbol
       | SymbolList "," Symbol

Symbol ::=
       Reference
       | ParameterizedReference

Reference ::=
       typereference
       | valuereference
       | objectclassreference
       | objectreference
       | objectsetreference

AssignmentList ::=
       Assignment
       | AssignmentList Assignment

Assignment ::=
       TypeAssignment
       | ValueAssignment
       | XMLValueAssignment
       | ValueSetTypeAssignment
       | ObjectClassAssignment
       | ObjectAssignment
       | ObjectSetAssignment
       | ParameterizedAssignment
```

Figura 13: Definición ASN.1 de módulo H.323.

A continuación, y con el fin de que el lector pueda hacerse una idea del formato de codificación ASN.1 para H.323, se mostrará en la figura 14 una pequeña parte de la

definición del protocolo H.225.0 que se ofrece en el Anexo H/H.225.0 (la descripción completa, sólo para este protocolo, ocupa 36 páginas):

```
   H323-MESSAGES DEFINITIONS AUTOMATIC TAGS ::=
      BEGIN

      IMPORTS
              SIGNED{},
              ENCRYPTED{},
              HASHED{},
              ChallengeString,
              TimeStamp,
              RandomVal,
              Password,
              EncodedPwdCertToken,
              ClearToken,
        CryptoToken,
        AuthenticationMechanism
      FROM H235-SECURITY-MESSAGES
        DataProtocolCapability,
        T38FaxProfile
      FROM MULTIMEDIA-SYSTEM-CONTROL;

   H248PackagesDescriptor ::= OCTET STRING

   H248SignalsDescriptor  ::= OCTET STRING

   H323-UserInformation   ::= SEQUENCE
-- aquí se describe la raíz común para todos los mensajes de
-- señalización de llamada H.225.0 en ASN.1:
   {
      h323-uu-pdu       H323-UU-PDU,
      user-data         SEQUENCE
      {
         protocol-discriminator    INTEGER      (0..255),
         user-information          OCTET STRING (SIZE(1..131)),
         ...
      } OPTIONAL,
      ...
   }

   H323-UU-PDU ::= SEQUENCE
   {
      h323-message-body   CHOICE
      {
         setup                Setup-UUIE,
         callProceeding       CallProceeding-UUIE,
         connect              Connect-UUIE,
         alerting             Alerting-UUIE,
         information          Information-UUIE,
         releaseComplete      ReleaseComplete-UUIE,
         facility             Facility-UUIE,
         ...,
         progress             Progress-UUIE,
         empty                NULL,
         status               Status-UUIE,
         statusInquiry        StatusInquiry-UUIE,
         setupAcknowledge     SetupAcknowledge-UUIE,
         notify               Notify-UUIE
      },
      nonStandardData         NonStandardParameter OPTIONAL,
      ...,
      h4501SupplementaryService    SEQUENCE OF OCTET STRING OPTIONAL,

      h245Tunneling           BOOLEAN,
      h245Control             SEQUENCE OF OCTET STRING OPTIONAL,
      nonStandardControl      SEQUENCE OF NonStandardParameter OPTIONAL,
```

```
      callLinkage             CallLinkage OPTIONAL,
      tunnelledSignallingMessage   SEQUENCE
      {
         tunnelledProtocolID  TunnelledProtocol,
         messageContent       SEQUENCE OF OCTET STRING,
         tunnellingRequired   NULL OPTIONAL,
         nonStandardData      NonStandardParameter OPTIONAL,
         ...
      } OPTIONAL,
      provisionalRespToH245Tunneling    NULL OPTIONAL,
      stimulusControl                   StimulusControl OPTIONAL,
      genericData                       SEQUENCE OF GenericData OPTIONAL
   }
-- a partir de aquí, se siguen describiendo todas las PDUs de cada
-- protocolo H.323:
   ...
-- también se muestran nuevas definiciones de tipos:
   GloballyUniqueID      ::=   OCTET STRING (SIZE(16))
   ConferenceIdentifier  ::=   GloballyUniqueID
   RequestSeqNum         ::=   INTEGER (1..65535)
   GatekeeperIdentifier  ::=   BMPString (SIZE(1..128))
   BandWidth             ::=   INTEGER (0..4294967295)
   CallReferenceValue    ::=   INTEGER (0..65535)
   EndpointIdentifier    ::=   BMPString (SIZE(1..128))
   ProtocolIdentifier    ::=   OBJECT IDENTIFIER
   ...
-- se muestran, para terminar, la referencia al mensaje BRQ (Bandwidth
-- ReQuest):
   BandwidthRequest ::= SEQUENCE --(BRQ)
   {
       requestSeqNum            RequestSeqNum,
       endpointIdentifier       EndpointIdentifier,
       conferenceID             ConferenceIdentifier,
       callReferenceValue       CallReferenceValue,
       callType                 CallType OPTIONAL,
       bandWidth                BandWidth,
       nonStandardData          NonStandardParameter OPTIONAL,
       ...,
       callIdentifier           CallIdentifier,
       GatekeeperIdentifier     GatekeeperIdentifier OPTIONAL,
       tokens                   SEQUENCE OF ClearToken OPTIONAL,
       cryptoTokens             SEQUENCE OF CryptoH323Token OPTIONAL,
       integrityCheckValue      ICV OPTIONAL,
       answeredCall             BOOLEAN,
       callLinkage              CallLinkage OPTIONAL,
       capacity                 CallCapacity OPTIONAL,
       usageInformation         RasUsageInformation OPTIONAL,
       bandwidthDetails         SEQUENCE OF BandwidthDetails OPTIONAL,
       genericData              SEQUENCE OF GenericData OPTIONAL
   }
   ...

   END
```

Figura 14: Definición ASN.1 del protocolo H.225.0 (fragmento).

2.5.3 RAS Registration/Admission/Status

El protocolo RAS (*Registration Admission Status*, es decir registro, admisión y estado) se utiliza para definir las comunicaciones entre cada terminal y su Gatekeeper, en cada Zona.

Es así como el Gatekeeper controla la administración de su Zona, admitiendo o denegando llamadas mediante la resolución de direcciones de red. También hay algunos mensajes RAS destinados a compartir direcciones entre Gatekeepers.

Cada mensaje RAS tiene tres tipos: Request (petición), y sus dos posibles respuestas Reject (rechazo) y Confirm (confirmación). Se abrevian xRQ, xRJ y xCF. También existen las siguientes excepciones:

- Information: ante un mensaje InformationRequest, se responde con un InformationResponse, y éste se confirma o rechaza con mensajes InformationAck o InformationNack.
- ResourceAvailable: tiene sólo las partes Indicate y Confirm (RAI, RAC).
- ServiceControl: tiene sólo las partes Indication y Response.
- Por último, existen mensajes simples: son RequestInProgress (RIP), nonStandardMessage y unknownMessage.

De entre los puertos UDP que la IANA[41] ([54]) ha asignado al estándar H.323, RAS usa el 1719 para transmisiones unicast, y el 1720 para transmisiones multicast, (aunque deben admitirse recepciones unicast en ambos puertos). Por otro lado, los únicos mensajes multicast permitidos son el GRQ (GatekeeperRequest) y el LRQ (LocationRequest).

A continuación, se pasará a estudiar los mensajes RAS más importantes:

- **GRQ**: GatekeeperRequest. Cuando se enciende un terminal (a no ser que éste, raramente, desee establecerse en solitario sin requerir Gatekeeper), tratará de encontrar a su Gatekeeper: esto puede hacerse mediante GRQ en multicast (procedimiento llamado *Gatekeeper discovery*, es decir localización de Gatekeeper); o mediante GRQ en unicast habiéndole suministrado la dirección de transporte de dicho Gatekeeper, típicamente direcciones IP o URL mediante consultas DNS (esta última opción se describe en el Anexo O/H.225.0).

  El contenido ASN.1 del mensaje GRQ se muestra en la figura 15:

```
GatekeeperRequest ::= SEQUENCE
{
    requestSeqNum            RequestSeqNum,
    protocolIdentifier       ProtocolIdentifier,
    nonStandardData          NonStandardParameter OPTIONAL,
    rasAddress               TransportAddress,
    endpointType             EndpointType,
    GatekeeperIdentifier     GatekeeperIdentifier OPTIONAL,
    callServices             QseriesOptions  OPTIONAL,
    endpointAlias            SEQUENCE OF AliasAddress OPTIONAL,
    ...,
    alternateEndpoints       SEQUENCE OF Endpoint OPTIONAL,
    tokens                   SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens             SEQUENCE OF CryptoH323Token OPTIONAL,
    authenticationCapability SEQUENCE OF AuthenticationMechanism OPTIONAL,
    algorithmOIDs            SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,
    integrity                SEQUENCE OF IntegrityMechanism OPTIONAL,
    integrityCheckValue      ICV OPTIONAL,
    supportsAltGK            NULL OPTIONAL,
    featureSet               FeatureSet OPTIONAL,
```

[41] IANA: *Internet Assigned Numbers Authority*, autoridad de números asignados para Internet.

```
    genericData             SEQUENCE OF GenericData OPTIONAL
}
```

Figura 15: Contenido ASN.1 del mensaje RAS GRQ.

Para rechazar una petición GRQ, el Gatekeeper hace uso del mensaje GRJ, el cual contiene múltiples razones para afirmar su rechazo (como se muestra en la figura 16):

```
GatekeeperReject ::= SEQUENCE
{
    requestSeqNum         RequestSeqNum,
    protocolIdentifier    ProtocolIdentifier,
    nonStandardData       NonStandardParameter OPTIONAL,
    GatekeeperIdentifier  GatekeeperIdentifier  OPTIONAL,
    rejectReason          GatekeeperRejectReason,
    ...,
    altGKInfo             AltGKInfo OPTIONAL,
    tokens                SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens          SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue   ICV OPTIONAL,
    featureSet            FeatureSet OPTIONAL,
    genericData           SEQUENCE OF GenericData OPTIONAL
}
GatekeeperRejectReason ::= CHOICE
{
    resourceUnavailable        NULL,
    terminalExcluded           NULL,
    invalidRevision            NULL,
    undefinedReason            NULL,
    ...,
    securityDenial             NULL,
    genericDataReason          NULL,
    neededFeatureNotSupported  NULL
}
```

Figura 16: Código ASN.1 con las razones de RAS GRJ.

Asimismo, para aceptarla se dispone del mensaje GCF, con una serie de elementos que posteriormente serán utilizados por el terminal durante el transcurso de la llamada (figura 17):

```
GatekeeperConfirm ::= SEQUENCE
{
    requestSeqNum         RequestSeqNum,
    protocolIdentifier    ProtocolIdentifier,
    nonStandardData       NonStandardParameter OPTIONAL,
    GatekeeperIdentifier  GatekeeperIdentifier  OPTIONAL,
    rasAddress            TransportAddress,
    ...,
    alternateGatekeeper   SEQUENCE OF AlternateGK OPTIONAL,
    authenticationMode    AuthenticationMechanism OPTIONAL,
    tokens                SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens          SEQUENCE OF CryptoH323Token OPTIONAL,
    algorithmOID          OBJECT IDENTIFIER OPTIONAL,
    integrity             SEQUENCE OF IntegrityMechanism OPTIONAL,
    integrityCheckValue   ICV OPTIONAL,
    featureSet            FeatureSet OPTIONAL,
    genericData           SEQUENCE OF GenericData OPTIONAL
}
```

Figura 17: Mensaje RAS GCF, en ASN.1.

Hasta aquí se han mostrado el contenido de estos mensajes ASN.1 con fines exclusivamente didácticos. Todos estos mensajes se encuentran especificados en este formato en el Anexo H/H.225.0.

- **RRQ**: RegistrationRequest. Tras encontrar uno o varios Gatekeepers, el terminal decide registrarse en uno de ellos mediante este mensaje. Que el Gatekeeper le enviase un mensaje de rechazo RRJ significaría que este terminal no recibirá los servicios de este Gatekeeper, (no que le deniegue el uso de la red).

  Si se admite a este terminal en el Gatekeeper, éste le asignará un identificador (*endpoint identifier*), el cual se usará en posteriores comunicaciones entre ellos. El terminal le suministrará asimismo una serie de direcciones alias (*alias addresses*), que luego les servirán a otros terminales para localizar a éste sin necesidad de usar su incómoda dirección de transporte:

  H.323 proporciona una enorme variedad de alias para la descripción del destino deseado en las llamadas:

  - dialedDigits (también llamados números E.164 por representar esta numeración internacional para la PSTN, representada por la ITU-T).
  - h323-ID (cuyo uso sólo tiene sentido en el ámbito entre el Gatekeeper y el terminal).
  - url-ID (para resolución vía DNS).
  - transportID (dirección de transporte).
  - email-ID (cuenta de correo electrónico).
  - partyNumber (refiriéndose tanto a numeración privada como a números E.164).
  - mobileUIM (un número que identifique a un terminal de telefonía móvil de segunda y tercera generación).

  Estos alias, sin embargo, no están diseñados para distinguir a un terminal: sólo para ser traducidos a una dirección de transporte. Además, esta gran variedad puede resultar causa de interoperabilidad entre fabricantes.

  Otra característica de RAS que puede dar lugar a errores es la redundancia en el registro contra el Gatekeeper de cada terminal de su Zona. No puede olvidarse que este elemento de direccionamiento es fundamental para el establecimiento de la conexión porque los terminales H.323 no están preparados para almacenar esta información de direccionamiento. El hecho de que el Gatekeeper pueda rechazar al terminal en los mensajes GRJ y en RRJ resulta crítica ante pérdidas de paquetes o caídas de segmentos de la red.

  En el mensaje de respuesta del Gatekeeper RCF, éste puede indicarle al terminal qué *alias addresses* ha aceptado, de la lista ofrecida por el terminal. También se comunican en el RRQ un tiempo de vida TTL para este registro en el Gatekeeper, y en el RCF éste podrá asignar un TTL menor. Para renovar el estado de registro en el Gatekeeper antes de la expiración de este TTL pueden usarse tramas LW RRQ (*Lightweight* RRQ), es decir tramas faro, que contienen una cantidad de información menor que la usada para los mensajes RRQ.

Por último, en estos mensajes también puede dársele al terminal el permiso necesario para llevar a cabo llamadas dentro de su área sin necesitar de elaborar una petición al Gatekeeper para ello (es decir, sin el uso de los mensajes ARQ/ACF que se comentan a continuación). En efecto, para esto ese terminal necesitará conocer previamente la dirección de transporte del destino. A este terminal se le llamará terminal *pre-granted* (pre-admitido).

- **ARQ**: AdmissionRequest. Tras su registro en el Gatekeeper, el terminal sólo podrá iniciar o aceptar una llamada tras pedirle permiso a su Gatekeeper (a no ser que se trate de un terminal pre-admitido). Es ahora cuando se realiza la traducción del alias a la dirección de transporte del destino.

  El terminal generará y asignará en este instante del proceso de generación de llamada varios identificadores de llamada:

  - Un CRV (callReferenteValue) único para esa llamada, con validez en el enlace (entre el éste y el Gatekeeper).
  - Un CallID de significado globalmente único.
  - Y un CID (conferenceID) que servirá para identificar cada conferencia de forma única, e igual para todos los participantes de esa conferencia. Todos estos identificadores serán utilizados posteriormente en las diversas fases de la llamada y por otros protocolos, como el de señalización de llamada H.225.0.

  Aquí también puede especificar el terminal el ancho de banda deseado de reserva para su comunicación, y bajar esta especificación el Gatekeeper en su respuesta.

- **LRQ**: LocationRequest. Este mensaje puede ser enviado hacia el Gatekeeper por un terminal o por otro Gatekeeper, y sirve para solucionar la dirección IP de un *alias address* desconocido.

  A continuación se presenta, en la figura 18, un diagrama de la participación del protocolo RAS en el establecimiento de una comunicación entre dos terminales situados en dos Zonas distintas (mediante el uso de mensajes LRQ/LCF entre Gatekeepers):

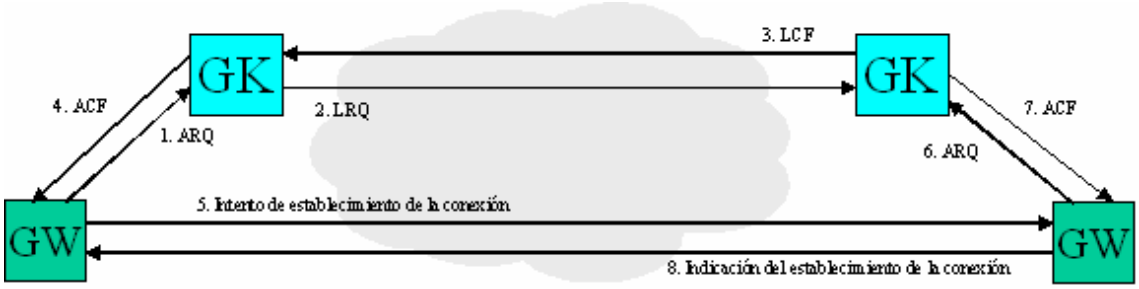

Figura 18: Mensajes RAS en el establecimiento de una llamada H.323.

- **DRQ**: DisengageRequest. Sirve para indicar, sobre el canal RAS, que la llamada se ha completado. Puede ser invocado tanto desde el terminal, como desde el Gatekeeper.

- Por último, los mensajes unknownMessage sirven para responder a mensajes no reconocibles; y los **nonStandardMessages** servirán incluso para que Gatekeepers y terminales se intercambien mensajes no estándares (como sucede, por ejemplo, entre equipos Quintum).

El resto de mensajes RAS que se especifican en el protocolo son: **BRQ** (BandwidthRequest), **IRQ** (InformationRequest), **RAI** (ResourceAvailabilityIndication), **RIP** (RequestInProgress) y **SCI** (ServiceControlIndication).

Se muestra para finalizar en la figura 19 una tabla de temporizadores y reintentos RAS por defecto (algunos equipos permiten su definición, como es el caso de las pasarelas Quintum Tenor):

Mensaje RAS	Temporizador (s)	Número de reintentos
GRQ	5	2
RRQ	3	2
URQ	3	1
ARQ	5	2
BRQ	3	2
IRQ	3	1
IRR	5	2
DRQ	3	2
LRQ	5	2
RAI	3	2
SCI	3	2

Figura 19: Tabla de temporizadores y reintentos RAS.

2.5.4 El Anexo G/H.225.0 para comunicaciones interdominio

El Anexo G de la especificación H.225.0 describe las comunicaciones entre dominios administrativos, es decir, entre los elementos de borde H.323 (o *border elements*). También se habla de esta comunicación en la especificación H.501.

Este Anexo se creó con la intención de resolver comunicaciones entre distintos espacios de direccionamiento, como comunicaciones interLANs que tengan que atravesar Internet.

La diferencia fundamental con la comunicación de mensajes RAS LRG/LCF es que éstos se limitan a solucionar direcciones. El Anexo G, además, permite la propagación de la

información de rutados, la presentación de informes de uso, e incluso la descripción de autorización de accesos.

Los elementos llamados *peer elements* (frente a los *border elements*) son Gatekeepers que utilizan mensajes Anexo G/H.225.0 para la comunicación de informaciones de direccionamiento; es decir, que no establecen comunicaciones interdominio.

La definición de la funcionalidad de cada elemento de la red H.323 que participa de la comunicación de mensajes Anexo G/H.225.0 se especifica en interfaces. La arquitectura resultante se muestra a continuación (figura 20):

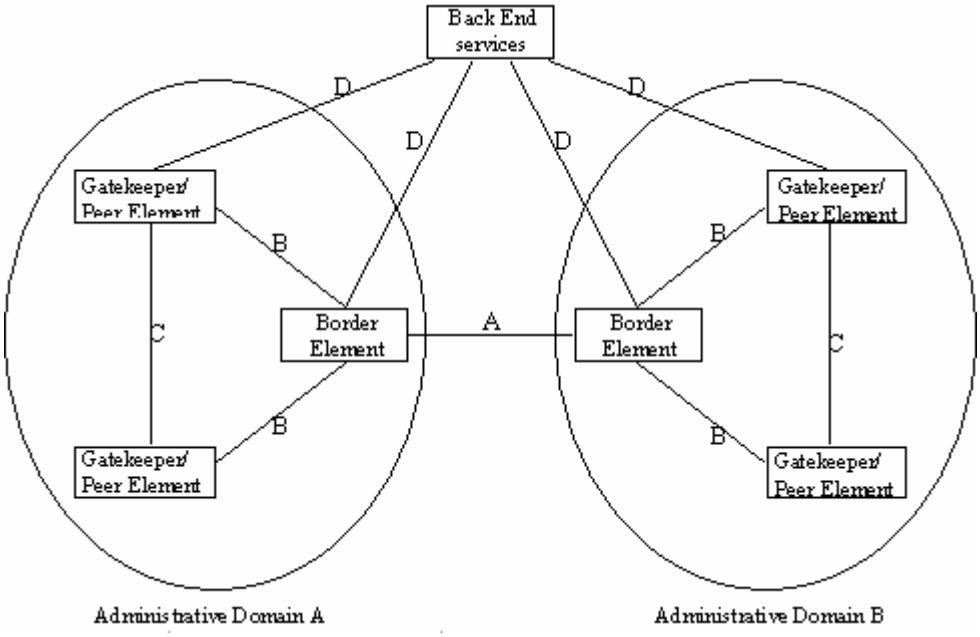

Figura 20: Esquema e Interfaces en comunicaciones Anexo G/H.225.0. La interfaz D está fuera del alcance de la especificación.

Para finalizar, y dado que de sus nombres se puede extraer aproximadamente una definición sobre su comportamiento, se mostrará la lista completa de los mensajes Anexo G/H.225:

- ServiceRequest
- ServiceConfirmation
- ServiceRejection
- ServiceRelease
- DescriptorRequest
- DescriptorConfirmation
- DescriptorRejection
- DescriptorIDRequest
- DescriptorIDConfirmation
- DescriptorIDRejection
- DescriptorUpdate

- DescriptorUpdateAck
- AccessRequest
- AccessConfirmation
- AccessRejection
- RequestInProgress
- NonStandardRequest
- NonStandardConfirmation
- NonStandardRejection
- UnknownMessageResponse
- UsageRequest
- UsageConfirmation
- UsageRejection
- UsageIndication
- UsageIndicationConfirmation
- UsageIndicationRejection
- ValidationRequest
- ValidationConfirmation
- ValidationRejection

2.5.5 Señalización de llamada H.225.0

El protocolo de señalización de llamada H.225.0 se utiliza para establecer llamadas entre dos entidades H.323. Se deriva del protocolo de control de llamada para la RDSI, Q.931, aunque se ha modificado para adaptarse a redes de paquetes. Mediante ASN.1, H.225.0 también se apropia de mensajes Q.932 (que define servicios suplementarios RDSI).

El formato de los mensajes se muestra a continuación, desde un nivel TCP (figura 21):

Figura 21: Formato de los mensajes H.225.0.

El significado de los paquetes involucrados es:

- TPKT: Los cuatro octetos necesarios para separar los mensajes TCP son 0x03, 0x00, HH y LL. HH y LL representan la longitud total del mensaje, incluyendo la misma cabecera TPTK, en *network byte order*.

- Cabecera Q.931: Todos los mensajes tendrán una cabecera Q.931, la cual incluye un octeto discriminador de protocolo (0x08), tres octetos para definir el identificador de llamada CRV (0x02, HH y LL, donde 0x02 representa la longitud del CRV, y HH y LL son los dos octetos del CRV en *network byte order*) y un último octeto con el que se indica el tipo de mensaje.
- IE: Se incluyen varios elementos de información (IEs), que dependerán de cada tipo de mensaje. Los elementos de información IEs transportan información adicional relativa a cada mensaje específico, aunque su uso no tiene por qué ser exclusivo de un tipo específico de mensaje; por ejemplo, un mensaje de Setup contendrá, entre otras cosas, los elementos de información "Calling Party Number" IE, "Called Party Number" IE, "Display" IE, etc. Aunque H.225.0 define qué IEs se corresponden con cada mensaje, la transmisión de algún otro IE no daría como resultado un fallo del protocolo.
- UUIE: *User-User Information Element*, es un elemento de información extremo a extremo. Deberá ser el último elemento del mensaje H.225.0. Se compone de los octetos 0x7E, HH, LL, PD y DATA. 0x7E es el identificador del elemento extremo-extremo entre los demás IEs. HH y LL contienen las longitudes de DATA en *network byte order*, PD es un discriminador de protocolo para ASN.1 (0x05) y DATA contiene el objeto H323-UserInformation codificado PER en ASN.1.

A continuación se muestran la lista de mensajes H.225.0 (ya familiares para los conocedores del protocolo de señalización Q.931, usado también en la RDSI):

- Setup
- Call Proceeding
- Alerting
- Information
- Release Complete
- Facility
- Progress
- Status
- Status Inquiry
- Setup Acknowledge
- Notify
- Connect

El establecimiento de llamada H.225.0 puede resultar tan sencillo como el uso de sólo dos mensajes: Setup y Connect. El resto de los mensajes servirán principalmente para prevenir errores por temporizadores, o para proporcionar anuncios y tonos en banda (o *in-band tones*), es decir, comunicación de tonos en el mismo canal que el propio canal de comunicación de la voz, tonos como el de llamada o el de ocupado; esto se realiza principalmente en el mensaje Progress, mediante el Progress Indicator IE.

Se muestra a continuación (figura 22) un diagrama de establecimiento de llamada en el protocolo de señalización de llamada H.225.0:

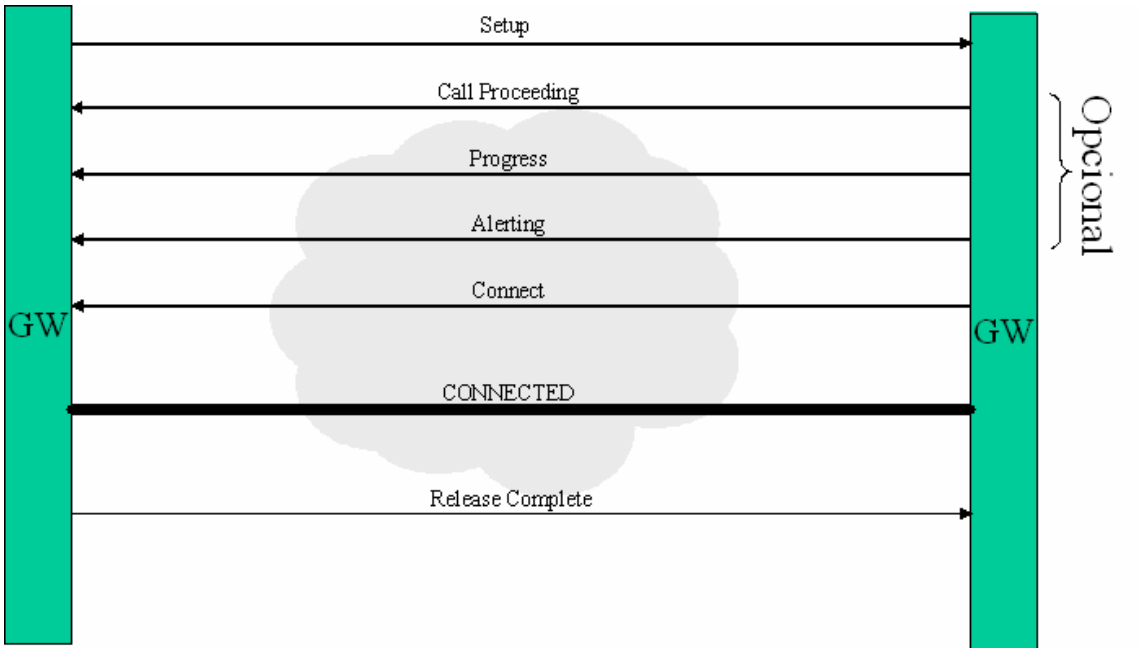

Figura 22: Diagrama de establecimiento de llamada H.225.0

Y, también, las comunicaciones completas de establecimiento de llamada H.225.0, junto con algunos mensajes RAS (figura 23):

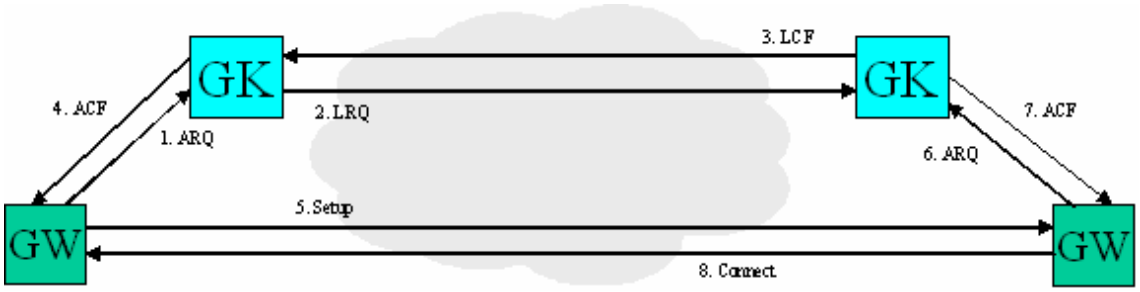

Figura 23: Diagrama de establecimiento de llamada RAS + H.225.0

Las especificaciones H.450 describen una serie de servicios suplementarios para H.323. Entre éstos se incluyen los servicios de transferencia de llamada, llamada en espera, indicación de mensaje en espera, etcétera. Todos estos servicios se transmitirán "tunelizados" en IEs que serán transmitidos en el interior de mensajes H.225.0.

El funcionamiento de H.450 se verá con más profundidad en el capítulo 2.5.8. Se muestra a continuación el funcionamiento del servicio suplementario de redirección simple: en la especificación H.450.2 se define cómo, tras recibir un mensaje de Setup, un mensaje Facility puede indicar un nuevo destino para esa llamada (siempre que se envíe antes del mensaje Connect). Puede verse en la figura 24:

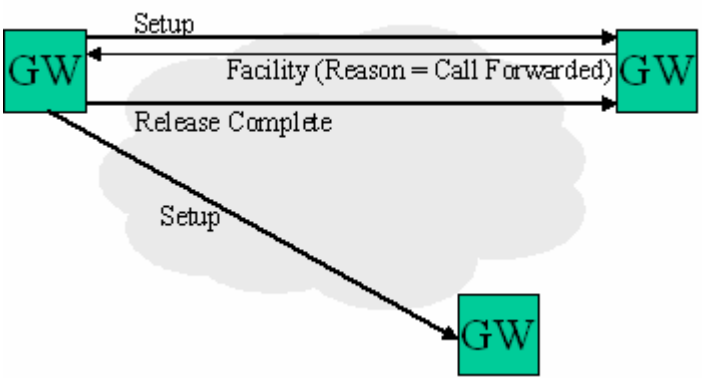

Figura 24: Mensajes involucrados en una transferencia de llamada H.450.2

Es reseñable que muchas de estas facilidades no se encuentran implementadas en todos los fabricantes, y que su uso, en tales casos, puede ocasionar problemas de interoperabilidad.

2.5.6 El canal de control H.245

El H.245 es el protocolo de control de llamada para comunicaciones multimedia que utiliza H.323. Este protocolo es compartido por un cierto número de protocolos H.32x, como el H.324M, usado en conferencias multimedia en redes 3G móviles. Pero H.323 no utiliza todas las características y facilidades que ofrece el estándar H.245; para contemplar cuáles de estos mensajes H.245 son usados por H.323 hay que referirse al Anexo A/H.323.

H.245 es una señalización que debe realizarse en paralelo con H.225.0 y, preferiblemente, antes del mensaje Connect (si no, podrían perderse algunos de los datos transmitidos). H.245 controla la sesión multimedia, encargándose de:

- El intercambio de capacidades de los terminales.
- La determinación del maestro y el esclavo de la comunicación.
- El control y composición de la señalización de canal lógico.

Por canal lógico se entiende un camino (*path*, es decir, una dirección de transporte habilitada, una conexión) para la transmisión de información entre dos terminales. En efecto, este protocolo puede asimilarse a la capa OSI de sesión.

Todos los mensajes H.245 se transportan por un canal especial, llamado el canal de control H.245. La apertura de este canal es, sin embargo, opcional, gracias a la posibilidad de usar el método *Fast Connect*: aunque a menudo este canal supone una conexión TCP separada, puede ser "tunelizado" dentro del canal de señalización de llamada H.225.0, en sus elementos de información IEs. De hecho, cuando se usa UDP para la señalización de llamada, el canal de control H.245 debe obligatoriamente ser "tunelizado". En el capítulo siguiente se estudiará este método en profundidad.

El formato de trama H.245, a nivel TCP, es el mostrado en la figura 25:

Figura 25: Formato de los mensajes H.245

Los significados de los paquetes involucrados son:

- TPKT: Los cuatro objetos necesarios para separar los mensajes TCP, son 0x03, 0x00, HH y LL. HH y LL representan la longitud total del mensaje, incluyendo la misma cabecera TPTK, en *network byte order*.
- H.245 PDU: Los mensajes H.245 son codificados mediante ASN.1 PER, y continúan a la cabecera TPTK. Existe la posibilidad de codificar PDUs H.245 adicionales a continuación de la primera, aunque muchas implementaciones podrían fallar ante esta posibilidad: es, por tanto, recomendable enviar PDUs H.245 separadas por cabeceras TPTK y, al mismo tiempo, prepararse ante la posibilidad de que éstas lleguen de forma continua.

En H.245 se distinguen cuatro tipos distintos de mensajes:

- Request (por ejemplo, masterSlaveDetermination, y terminalCapabilitySet).
- Response (como los mensajes masterSlaveDeterminationAck, y terminalCapabilitySetAck).
- Command (como el mensaje sendTerminalCapabilitySet).
- Indication (caso del mensaje userInput).

Una de las funciones más importantes del canal de control H.245 es permitir el intercambio de capacidades, es decir, la decisión sobre:

- El formato de los datos multimedia, como el tipo de codificación (G.711, G.723, H.261 o T.120).
- El número máximo de muestras de audio por paquete.
- O si se admite soporte para la supresión de silencios.
- Así, los terminales pueden escoger la codificación que mejor se adapta a las necesidades de cada comunicación.

Los primeros mensajes que se envían por el canal H.245 son uno o varios **Terminal Capability Set** (**TCS**), mensaje en el que se describen los códecs y las capacidades multimedia (*Capability Set*) que soporta cada terminal. Cada capacidad (*capability*) se relaciona con un número de las tablas de capacidades descritas en la especificación H.245; todas las posibles capacidades de todos los terminales se encuentran descritos en tablas.

H.323 contiene mecanismos para describir nuevas capacidades (como en el caso de los códecs no descritos a priori en las tablas de la especificación), en los Anexos E al M, de H.245.

En la descripción de las capacidades de cada terminal, hay también que especificar cuáles de estas capacidades pueden soportarse *a la vez*. Así, cada terminal comunicará una serie de descriptores de capacidades, cada uno de los cuales contendrá una serie de entradas de las tablas de capacidades descritas anteriormente; y cada descriptor de capacidades indicará que todos sus contenidos podrán ejecutarse simultáneamente en el terminal.

Otras de las funciones fundamentales de H.245 es la determinación de maestro y esclavo. El maestro de una conferencia punto a punto es el que puede indicar cuándo los canales entran en conflicto (es decir, cuándo el otro terminal intenta abrir un canal incompatible). El esclavo deberá ceder a las indicaciones del maestro y reconfigurar los canales adecuadamente. Otra forma de funcionar en la determinación de maestro y esclavos es, ante multiconferencias, mediante una topología *peer to peer*.

Para la señalización de canal lógico, los canales se abren intercambiando mensajes **openLogicalChannel** (**OLC**); este mensaje contendrá una de las capacidades que anteriormente le comunicó el otro terminal. Cada terminal debe transmitir un OLC; esto permite la comunicación asimétrica en códecs (es decir, que en transmisión se utilice un formato para la codificación de los datos multimedia distinto al usado en recepción). Con cada OLC se asigna un SessionID, es decir un identificador de sesión; por defecto, la sesión 1 se asigna al audio, la 2 a vídeo y la 3 a datos; y futuros SessionIDs serán asignados por el maestro de la comunicación. Para cada SessionID se abre una sesión RTP/RTCP.

El protocolo H.245 completo resulta muy complejo. Presenta en total 53 mensajes H.245 distintos (además de otros 15 que representan mensajes de respuesta). Pero, desde luego, esta parte del protocolo es la que guarda mayor grado de implicación entre los puntos finales, y por esto es necesario que se cubran todos los apartados posibles. Algunos de estos mensajes (que se enumeran para hacer ver algunas de las posibilidades del protocolo) son:

- requestMultiplexEntry.
- roundTripDelayRequest.
- encryptionCommand.
- conferenceCommand.
- flowControlIndication.
- nonStandardParameter.

H.323 especifica que para cerrar el canal de control H.245 el terminal deberá cerrar todos los canales lógicos y esperar los Acks (*acknowledgements*) respectivos. Tras esto, podrá enviar el comando endSession, y esperar asimismo su Ack.

A continuación se muestra un diagrama de llamada H.323 completo, contemplando todos los protocolos involucrados en ella (figura 26):

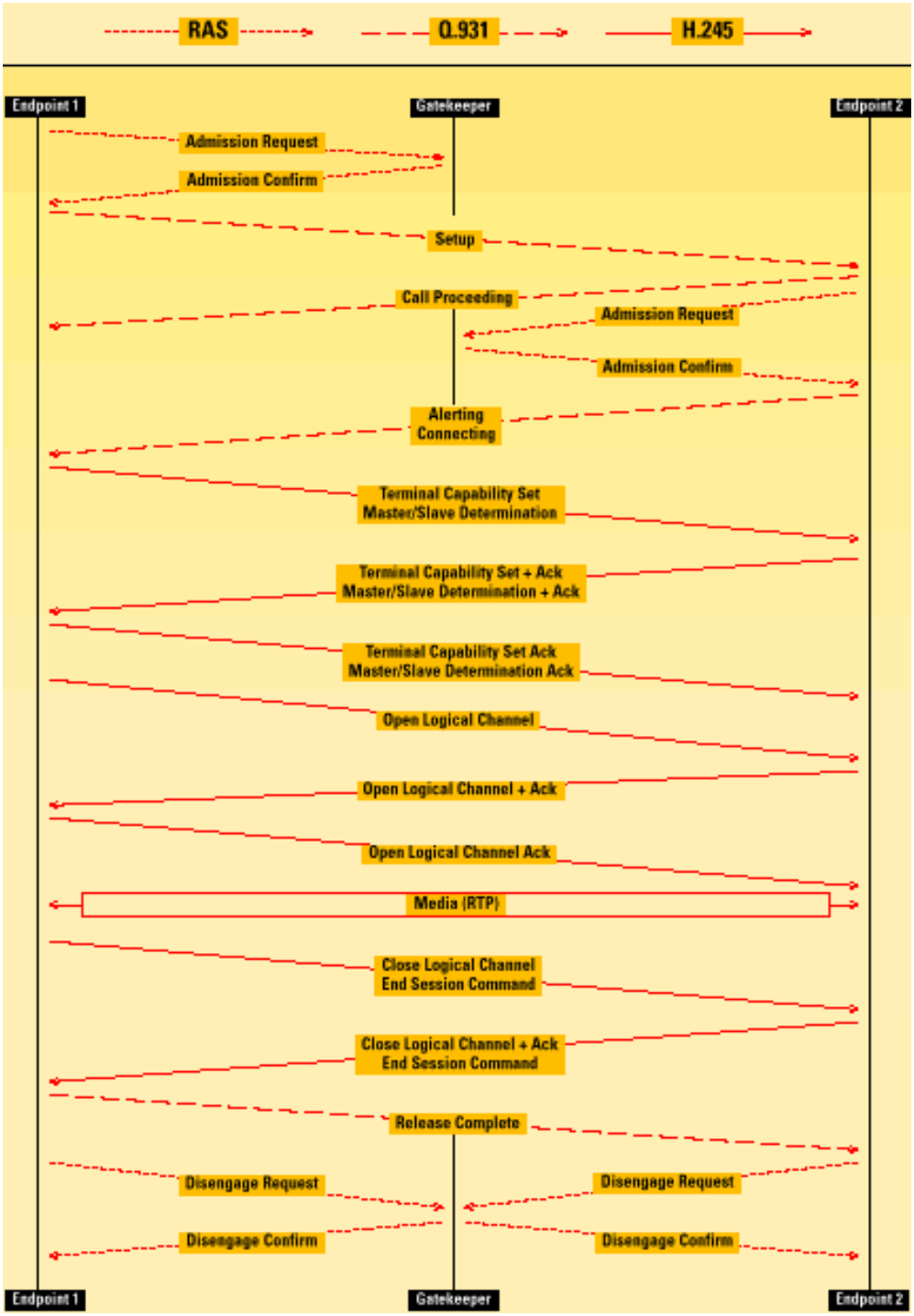

Figura 26: Diagrama completo de llamada H.323

2.5.7 El método Fast Connect

El método *Fast Connect* es un medio que propone H.323 para establecer una llamada con un mínimo de dos paquetes. Así, ni siquiera será necesario abrir un canal de control H.245, permitiéndose que todos los *media* se negocien dentro de este procedimiento rápido.

Para conseguirlo, se "tunelizarán" todos los mensajes OLC H.245 en el mensaje de Setup H.225.0, en uno o varios Fast Connect IEs, representando cada uno de ellos una proposición de canal con el mismo identificador de sesión (1, 2 ó 3, para audio, vídeo o datos respectivamente).

Para aceptar un *Fast Connect* se escoge uno de los OLCs recibidos y se devuelve otro elemento *Fast Connect* en cualquier mensaje dirigido al llamante, (para el caso más rápido, en el interior de un mensaje H.225.0 Connect). Para rechazar el *Fast Connect*, basta con iniciarse procedimientos H.245.

La llamada de dos paquetes requerirá que:

- Ambos elementos involucrados en la llamada estén pre-admitidos por sus Gatekeepers en sus respectivas Zonas.
- El terminal que inicia la llamada conozca la dirección de transporte del destino.
- Que ambos soporten *Fast Connect*.
- Y que los OLCs "tunelizados" en los mensajes Setup y Connect H.225.0 sean aceptados, respectivamente, por cada uno de los elementos.

La versión 4 de H.323 incluye ciertos mecanismos que impiden algunas condiciones de carrera existentes detectadas en versiones anteriores de este *Fast Connect*. Esto supone que en algunos casos prácticos este método no pueda utilizarse, como sucederá con las plataformas de interfonía que se desarrollarán en el siguiente capítulo.

2.5.8 Servicios Suplementarios: H.450

Aunque en el presente Proyecto no va a hacerse uso de ninguno de estos servicios suplementarios H.323, se incluirá a continuación el siguiente estudio sobre H.450 para que el lector pueda conocer la potencialidad y estructuración de la arquitectura H.323 en cuanto a estos servicios, en la medida en que son éstos los que pueden marcar la diferencia de la VoIP con respecto a las redes POTS.

El estándar H.450 posee una arquitectura descentralizada para los servicios suplementarios, y lo más separada posible de la arquitectura de los servicios básicos.

Las entidades H.323 involucradas en estos servicios se comunican directamente mediante señalización H.450, sin requerir del control centralizado de la red, excepto en los casos en los que resulte necesaria alguna capacidad centralizada. En estos casos, se hará uso de un servidor H.323/H.450 de servicios suplementarios, como sucede, por ejemplo, con el servidor de mensajería, o con el servidor distribuidor automático de llamadas.

Además de un control de servicios suplementarios completamente distribuido, H.450 describe también un modelo en el que parte de la funcionalidad H.450 puede llevarse a cabo en *proxies* H.450 entre los terminales. Un *proxy* H.450 podría ser colocado, por ejemplo, en el interior de un Gatekeeper.

Otro de los objetivos más importantes en el diseño de H.450 fue la simplificación de los requerimientos de intercomunicación con las redes conmutadas privadas (QSIG[42]) y públicas (RDSI).

H.450 ha sido diseñado con el objetivo de conseguir un protocolo enormemente flexible, definiendo diversos mecanismos para permitir la interoperabilidad entre fabricantes que presenten distintos grupos de características. Entre estos mecanismos, se encuentra el uso de una arquitectura que separa las máquinas de estado de servicios suplementarios de las máquinas de estado de la llamada básica. Un esquemático de la integración de ambas arquitecturas se muestra en la figura 27:

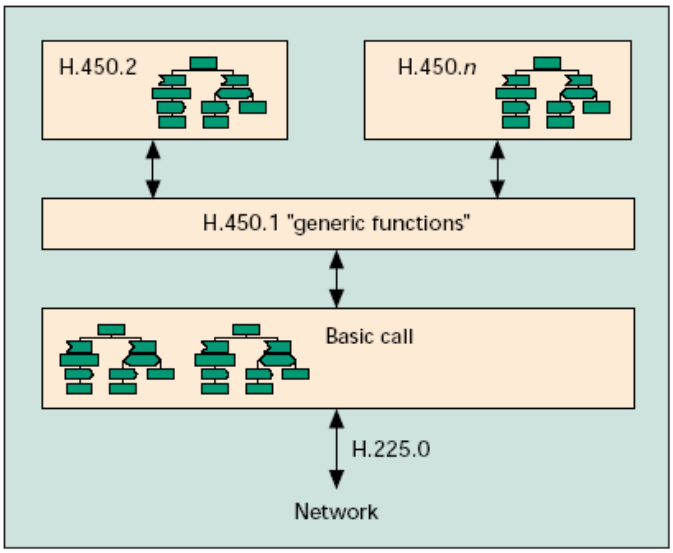

Figura 27: Arquitectura H.323/H.450 en los terminales

El estándar H.450.1 describe servicios genéricos comunes para todos los servicios suplementarios, tanto estándares como específicos de cada fabricante; a estos servicios se les conoce también como funciones genéricas. También describe los comportamientos de cada terminal ante APDUs desconocidas.

Otro estándar que facilita la interoperabilidad entre fabricantes es el H.450.12, que permite el intercambio de las capacidades soportadas por cada terminal. Esto también podría usarse como una reacción por adelantado, como por ejemplo la capacidad de una aplicación para no presentarle al usuario la posibilidad de transferir una llamada si el otro extremo de esa llamada no soportase este servicio suplementario.

Una lista con todos los servicios suplementarios soportados por cada estándar H.450.x es presentado en la figura 28.

[42] QSIG: *Q Signalling*, protocolo para comunicaciones RDSI basado en el estándar Q.931, usado para resolver la señalización entre centralitas digitales.

Estándar	Servicio suplementario	Subfunciones
H.450.1	Funciones genéricas para servicios suplementarios en H.323	
H.450.2	Transferencia de llamada para H.323	Transferencia en un solo paso Transferencia con consulta
H.450.3	Desvío de llamada para H.323	Redirección de llamada incondicional Redirección de llamada cuando ocupado Redirección de llamada cuando no hay respuesta Desvío de llamada
H.450.4	*Call Hold* para H.323	*Call Hold* local *Call Hold* remoto
H.450.5	*Call Park* y *Call Pickup* en H.323	*Park* y *Pickup* dirigidos *Park* y *Pickup* en grupos *Pickup* ante llamadas entrantes.
H.450.6	Llamada en espera para H.323	
H.450.7	Indicación de mensaje en espera para H.323	Sistema de mensajería Reproducción de mensajes en espera
H.450.8	Identificación de nombres para H.323	
H.450.9	Finalización de llamada para H.323	Finalización de llamada cuando ocupado Finalización de llamada cuando no hay respuesta
H.450.10	Ofrecimiento de llamada para H.323	
H.450.11	Intromisión de llamada para H.323	Conexión tipo conferencia Conexión tipo sostenido Monitorización de silencios Liberación de llamada forzada
H.450.12	Información común para H.323	

Figura 28: Lista de servicios suplementarios estandarizados en H.450.

La información de servicio suplementario H.450 es enviada en unidades de datos del protocolo de aplicación (APDUs) “tunelizadas” en cualquier mensaje de control de llamada H.225.0 (mediante IEs específicos, como se vio que sucedía con el método Fast Connect), sin ninguna influencia sobre el estado de la llamada H.225.0.

Entre otra información, las APDUs H.450 contienen referencias a operaciones del Servicio de Operaciones Remotas (ROS, *Remote Operations Service*), las cuales definen la semántica de los servicios suplementarios.

Como sucede con los otros componentes del protocolo H.323, las APDUs H.450 se especifican y codifican usando ASN.1: así, las APDUs H.450 pueden ser extendidas mediante el uso de información específica del fabricante (nonStandardData), en la forma de elementos de información adicionales o incluso la especificación de nuevas operaciones. Ésta es la forma de definir nuevos servicios suplementarios.

El funcionamiento de H.450 es el siguiente: la información H.450 se pasa a la entidad H.450.1. A continuación se identifican los servicios genéricos, y las operaciones del ROS son entonces pasadas a sus respectivas entidades de servicio suplementario. Es también en la entidad de funciones genéricas H.450.1 donde pueden activarse, coordinarse o bloquearse

servicios simultáneos. Cada servicio suplementario se define en una máquina de estado descrita mediante diagramas SDL[43] [55].

Finalmente, una de las ideas básicas de los servicios H.450 es una definición que permita usarlos conjuntamente con la llamada básica, en la forma de bloques constructivos. De esta forma, mediante combinaciones de los bloques básicos, pueden construirse características y servicios más avanzados. Por ejemplo, una consola de atención automática podría construirse a partir de la combinación de los bloques de Llamada básica (con una línea de entrada múltiple y un efectivo control de pulsos DTMF), más *Call Hold*, más Transferencia de llamada, más Mensajería en espera.

2.5.9 El Generic Extensibility Framework

El estándar H.323 permite ampliaciones de protocolo mediante el GEF: El GEF es el *Generic Extensibility Framework* (marco de trabajo genérico para extensibilidad), introducido en la versión 4 de H.323. Se diseñó para suplir la posibilidad de ampliar H.323 con características de interés no necesariamente horizontal (es decir, para casos particulares).

Las capacidades GEF pueden señalizarse como deseadas o como requeridas; si un terminal requiere de específicamente una capacidad GEF que su interlocutor no posee, la llamada no se establecerá.

GEF se basa en el uso de elementos de la comunicación H.323 de tipo genérico, GenericData, tipo de elemento que siempre acaba existiendo de forma opcional en cada protocolo involucrado en H.323. Explica el uso de tablas para definir las características o procedimientos que serán luego necesarios para resolver la comunicación, así como la definición y el uso de elementos genéricos sobre el propio lenguaje ASN.1.

Entre otras cosas, dentro del GEF se han descrito mecanismos para:

- La portabilidad del número en movilidad.
- El establecimiento de prioridades en las llamadas.
- Petición de rutas alternativa.
- Reportes de parámetros para la monitorización de la calidad de servicio.
- Para “tunelizado” de RAS en H.225.0.
- Para atravesar cortafuegos.

El GEF se especifica en la recomendación H.460.x.

[43] SDL: *Specification and Description Language,* Lenguaje de Descripción y Especificación, de la ITU.

2.6 Cinco versiones del estándar H.323

El estándar H.323, en constante desarrollo y adaptación a las necesidades que van surgiendo, ha sufrido hasta ahora 5 revisiones fundamentales (H.245 lleva 9 revisiones). El hecho de que algunos fabricantes hayan elaborado sus productos en base a una documentación que con el paso del tiempo ha ido quedándose obsoleta ha llevado a que numerosas aplicaciones y capacidades de este potente y complejo protocolo no resulten compatibles entre distintos fabricantes, (a pesar de que la especificación se preocupe de que así lo sean). De hecho, una de las primeras cuestiones a la hora de analizar cómo un producto H.323 se adecúa a las necesidades de un determinado proyecto debe ser qué versión del protocolo cumple.
Precisamente por esto, parece imprescindible revisar a continuación, y para finalizar el capítulo teórico, qué han aportado cada una de las versiones a las capacidades estudiadas en los capítulos anteriores.

- Versiones 1 y 2: En estas versiones se establece la base del protocolo H.323. En realidad, la versión 1 por sí sola resulta ya tan anticuada que, a pesar de que cualquier versión H.323 siempre permanece compatible con las anteriores, es preferible obviar la posibilidad de adquirir un producto que sólo se acoja a esta especificación. La versión 2 del protocolo se aprobó en enero de 1998, y contempla:
    - Los mecanismos básicos de H.225.0 (incluyéndose el uso del mensaje Progress de señalización de llamada, o del paquete RIP -*Request In Progress*- y del temporizador Time To Live en el RAS, así como terminales pre-admitidos, paquetes InformationRequest y ResourceAvailability) y H.245.
    - La definición de Gatekeepers alternativos.
    - H.235 (seguridad en cuanto a autenticación, integridad, privacidad y no repudio).
    - El mecanismo *Fast Connect*
    - El "tunelizado" de canales en H.225.0.
    - Algunos servicios suplementarios H.450 (en concreto, la transferencia de llamada especificada en H.450.2 y H.450.3).
    - El uso del identificador de llamada CRV, y de varios alias (en concreto, el H323ID, email, PartyNumber, URL y TransportID).
    - Y la introducción de varios códecs (como el GSM[44]) y de capacidades T.120 (datos) y H.263 (vídeo).

- Versión 3: Aprobada en septiembre de 1999, presenta nuevas características, a saber:
    - Conferencia *out of consultation* (es decir, cuando una llamada pasa por una secretaria antes de ser comunicada con su destino; una especie de transferencia de llamada).

[44] GSM: *Global System for Mobile Communications.*

- Definición la característica CallerID que permite al llamante definir qué información será presentada en el destino y su monitorizado en el Gatekeeper.
- Definición de capacidades genéricas GEF.
- La descripción del Anexo G/H.225.0 para comunicaciones interdominios.
- La definición de SETs Simple Enpoint Types en el Anexo F/H.323 para terminales reducidos.
- Y algunos servicios suplementarios adicionales como llamada en espera y mensajes de indicación de espera.

- Versión 4: Desde noviembre del 2000, la versión 4 de H.323 nos presenta:
  - Una nueva forma de descomponer las pasarelas (*Gateways*) en MG y MGCs, así como la comunicación entre ellos mediante H.248.
  - Mecanismos para la multiplexión de canales de vídeo y audio en un único canal RTP/RTCP.
  - Nuevos y potentes servicios suplementarios, como el Anexo K/H.323 que define mecanismos de control vía HTTP y el Anexo L/H.323 para la comunicación mediante estímulos (como pulsación de teclas o clicks de ratón).
  - Nuevas capacidades para la definición de la identidad llamante y de llamada en espera.
  - Nuevos mecanismos para la definición y uso de tonos y anuncios *in-band.*
  - Mensajes RAS UsageInformation para la generación de estadísticos.
  - Soporte para la gestión del ancho de banda en multiconferencias.
  - Uso de RSVP para gestión de la calidad de servicio.
  - Extensiones del protocolo mediante GEF.
  - Capacidades para la gestión de llamadas a crédito.
  - Una como mejor gestión de cambios de “tunelizado” a status normal para H.245.

- Versión 5: La última versión, hasta la fecha, del protocolo H.323, salió a la luz en julio de 2003. En ella se incluyen los Anexos M hasta el R, así como una extensa revisión del GEF. Entre estas nuevas características cabe destacar:
  - El uso de DNS para resolución de direcciones.
  - Nuevos mecanismos de robustez.
  - Mecanismos para monitorización.
  - Peticiones GEF para rutas alternativas.

El conjunto de todas estas definiciones para procedimientos de comunicaciones multimedia H.323 es tan extenso que, habitualmente, los fabricantes sólo permiten la configuración de algunas de ellas, repartidas entre todas las versiones.

Esto, en general, da lugar a costosas interoperabilidades, que redundan en la reducción progresiva de las capacidades de cada terminal a medida que se amplia el rango de productos de distintos fabricantes empleado para resolver nuestro proyecto de VoIP.

En realidad, esta interoperabilidad es piedra angular en el presente proyecto, como se analizará en el apartado 3.6.