UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.225.0

(07/2003)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Multiplexación y sincronización en transmisión

Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes

Recomendación UIT-T H.225.0

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

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.399
SERVICIOS SUPLEMENTARIOS PARA MULTIMEDIOS	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 multimedios de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedios	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedios	H.530–H.539
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedios	H.540–H.549
Procedimientos de interfuncionamiento de la movilidad	H.550–H.559
Procedimientos de interfuncionamiento de colaboración en móviles multimedios	H.560–H.569
SERVICIOS DE BANDA ANCHA Y DE TRÍADA MULTIMEDIOS	
Servicios multimedios de banda ancha sobre VDSL	H.610–H.619

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

Recomendación UIT-T H.225.0

Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes

Resumen

Esta Recomendación trata los requisitos técnicos de los servicios videotelefónicos de banda estrecha definidos en las Recomendaciones de la serie H.200 y F.720, en aquellas situaciones en las que el trayecto de transmisión incluye una o más redes de paquetes, cada una de las cuales está configurada y gestionada para ofrecer una calidad de servicio (QoS) no garantizada que no es equivalente a la de la RDSI de banda estrecha, de manera que los mecanismos de protección o recuperación adicionales que van más allá de los prescritos por la Rec. UIT-T H.320 han de proporcionarse en los terminales. Hay que señalar que la Rec. UIT-T H.322 trata el tema de la utilización de algunas otras LAN que pueden proporcionar la calidad de funcionamiento subyacente no presupuesta por las Recomendaciones UIT-T H.323 y H.225.0.

Esta Recomendación describe cómo puede gestionarse la información de audio, vídeo, datos y control en una red de paquetes para proporcionar servicios conversacionales en equipos H.323.

El anexo G describe métodos que permiten la resolución de dirección entre dominios administrativos en los sistemas H.323 para completar llamadas entre dominios administrativos. Un determinado dominio administrativo se presenta a los otros dominios administrativos a través de un tipo de elemento lógico conocido como elemento de frontera.

Los productos que pretendan ser conformes con la versión 5 de la Recomendación H.225.0 (esta versión) deberán cumplir todos los requisitos obligatorios de esta Recomendación. Los productos conformes con la versión 5 pueden identificarse por mensajes H.225.0 que contienen un valor **protocolIdentifier** de {itu-t (0) recommendation (0) h (8) 2250 version (0) 5}.

Orígenes

La Recomendación UIT-T H.225.0 fue aprobada por la Comisión de Estudio 16 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8 el 14 de julio de 2003.

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.

ÍNDICE

Página

Recomendación UIT-T H.225.0

Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes

El UIT-T,

considerando

la extendida adopción y el creciente uso de la Rec. UIT-T H.320 para los servicios de videotelefonía y de videoconferencia por redes conformes con las características de la RDSI de banda estrecha especificadas en las Recomendaciones de la serie I,

reconociendo

la conveniencia y ventajas de permitir el transporte de los servicios indicados, total o parcialmente, por redes de área local, pero manteniendo también la capacidad de interfuncionamiento con terminales H.320,

y advirtiendo

las características y prestaciones de los muchos tipos de red de área local que son de interés potencial,

recomienda

que se utilicen sistemas y equipos que cumplen los requisitos de la Rec. UIT-T H.322 o la Rec. UIT-T H.323 para proporcionar estas facilidades.

1 Alcance

Esta Recomendación describe los métodos por los que se asocian, codifican y paquetizan las señales de audio, vídeo, datos y control para su transporte entre equipos H.323 por una red de paquetes. Esto incluye la utilización de una pasarela H.323, que a su vez puede conectarse a terminales H.320, H.324 o H.310/H.321 por la RDSI de banda estrecha, RTPC o RDSI de banda ancha, respectivamente. Las descripciones de equipos, y los procedimientos se describen en la Rec. UIT-T H.323, mientras que la presente Recomendación trata los protocolos y formatos de mensaje. Es también posible la comunicación a través de una pasarela H.323 hacia una pasarela H.322 para las LAN de calidad de servicio (QoS, *quality of service*) garantizada, y por tanto a puntos extremos H.322.

La presente Recomendación está destinada a operar con una amplia variedad de redes de paquetes diferentes, inclusive IEEE 802.3, Token Ring, etc. De este modo, la presente Recomendación se define como algo que está por encima de la capa de transporte tal como TCP/IP/UDP, SPX/IPX, etc. En el apéndice IV se incluyen perfiles específicos para determinadas sucesiones de protocolos de transporte. ***Así, el alcance de la comunicación H.225.0 se halla entre entidades H.323 en la misma red de paquetes, utilizando el mismo protocolo de transporte***. Esta red de paquetes puede ser un único segmento o anillo, o podría lógicamente ser una red de datos empresarial que comprenda múltiples redes de paquetes puenteadas o encaminadas para crear una red interconectada. Debe destacarse que el funcionamiento de los terminales H.323 en la Internet completa, o incluso varias redes de paquetes conectadas, pueden dar lugar a prestaciones mediocres. El posible medio por el que la calidad de servicio podría ser asegurada en esta red de paquetes, o en la Internet en general cae fuera del alcance de esta Recomendación. Sin embargo, esta Recomendación proporciona un medio al usuario de equipo H.323 de determinar que los problemas de calidad son resultado de la congestión de las redes de paquetes, así como procedimientos para

acciones correctivas. Se señala también que el uso de múltiples pasarelas H.323 conectadas por la red RDSI pública es un método directo para aumentar la calidad de servicio.

La Rec. UIT-T H.323 y esta Recomendación están destinadas a extender las conferencias/conexiones H.320 y H.221 al entorno de la red de paquetes con QoS no garantizada. Como tal, el modelo de conferencia primario[1] es un modelo de tamaño comprendido entre algunos participantes y algunos miles, a diferencia de las operaciones de difusión en gran escala, con riguroso control de admisión y estricto control de la conferencia.

Esta Recomendación hace uso del protocolo en tiempo real/protocolo de control en tiempo real (RTP/RTCP, *real-time transport protocol/real-time transport control protocol*) para la paquetización y sincronización de medios de todas las redes de paquetes subyacentes (véanse los anexos A, B y C). Adviértase que la utilización de RTP/RTCP especificada en esta Recomendación no está vinculada en modo alguno a la utilización de TCP/IP/UDP. La presente Recomendación supone un modelo de llamada en el que se utiliza señalización inicial en una dirección de transporte no RTP para establecimiento de comunicaciones y negociación de capacidad (véanse las Recomendaciones UIT-T H.323 y H.245), seguida por el establecimiento de una o más conexiones RTP/RTCP. Esta Recomendación contiene detalles de la utilización de RTP/RTCP.

En la Rec. UIT-T H.221, las señales de audio, vídeo, datos y control se multiplexan en una o más llamadas RCC físicas sincronizadas. En el lado red de paquetes de una llamada H.323, no se aplica ninguno de estos conceptos. No hay necesidad de trasladar desde el lado RCC el concepto H.221 de una llamada P × 64 kbit/s, por ejemplo 2 por 64 kbit/s, 3 por 64 kbit/s, etc. Así, en el lado red de paquetes, por ejemplo hay llamadas de una sola "conexión" con una velocidad máxima limitada a 128 kbit/s, y no llamadas a velocidad fija 2 × 64 kbit/s. Otro ejemplo tiene llamadas red de paquetes de una sola "conexión" con una velocidad máxima limitada a 384 kbit/s interfuncionando con 6 × 64 kbit/s en el lado RCC[2]. La principal justificación de este planteamiento es añadir complejidad en la pasarela y no en el terminal y evitar extenderse a las características de la red de paquetes H.320 que están estrechamente vinculadas a la RDSI, a menos que sea necesario.

En general, los terminales H.323 no conocen directamente la velocidad de transferencia H.320, aunque interfuncionan a través de una pasarela H.323; en su lugar, la pasarela utiliza mensajes **FlowControlCommand** H.245 para limitar la velocidad de los medios en cada canal lógico en uso a la permitida por el múltiplex H.221. La pasarela puede permitir que las velocidades de vídeo lado red de paquetes estén substancialmente por debajo de las velocidades del lado RCC (o al contrario) mediante la utilización de una función reductora de velocidad y tramas de relleno H.261; los detalles de dichas operaciones caen fuera del alcance de la Rec. UIT-T H.323 y esta Recomendación. Adviértase que el terminal H.323 está indirectamente al corriente de las velocidades de transferencia H.320 por medio de los campos vídeo de máxima velocidad binaria de la Rec. UIT-T H.245, y no deberá transmitir a velocidades que excedan de éstas.

---

1 Hay en estudio un modelo opcional de difusión sólo conferencia; necesariamente el modelo de difusión no permite un riguroso control de admisiones ni un estricto control de conferencia.

2 Adviértase que las velocidades de vídeo y de datos en el lado LAN deben concordar con las velocidades de vídeo y de datos del lado RCC del múltiplex H.320; las velocidades de audio y de control no necesitan concordar. Dicho de otro modo, esperaríamos normalmente que, utilizando control de flujo H.245, la pasarela LAN/RCC obligará a las velocidades de vídeo y de datos a encajar en el múltiplex RCC H.221. Sin embargo, dado que el audio puede transcodificarse a menudo en la pasarela, encontraremos frecuentemente que la velocidad de audio LAN y la velocidad RCC no concuerdan. Además, no habría ninguna esperanza de que la velocidad binaria H.221 para control (800 bit/s) concuerde en general con la velocidad binaria H.245 en el lado LAN. Adviértase también que la velocidad LAN puede quedar por debajo de la velocidad RCC para vídeo o/y datos, pero no puede rebasar la cantidad máxima que encaja en el múltiplex del lado RCC.

Esta Recomendación está concebida de manera que, con una pasarela H.323, es posible la interoperabilidad con terminales H.320 (1990), H.320 (1993) y H.320 (1996). Sin embargo, algunas características de esta Recomendación pueden orientarse a permitir operaciones mejoradas con futuras versiones de la Rec. UIT-T H.320. Es también posible que la calidad de servicio en el lado H.320 pueda variar en base a las características y capacidades de la pasarela H.323 (véase la figura 1).

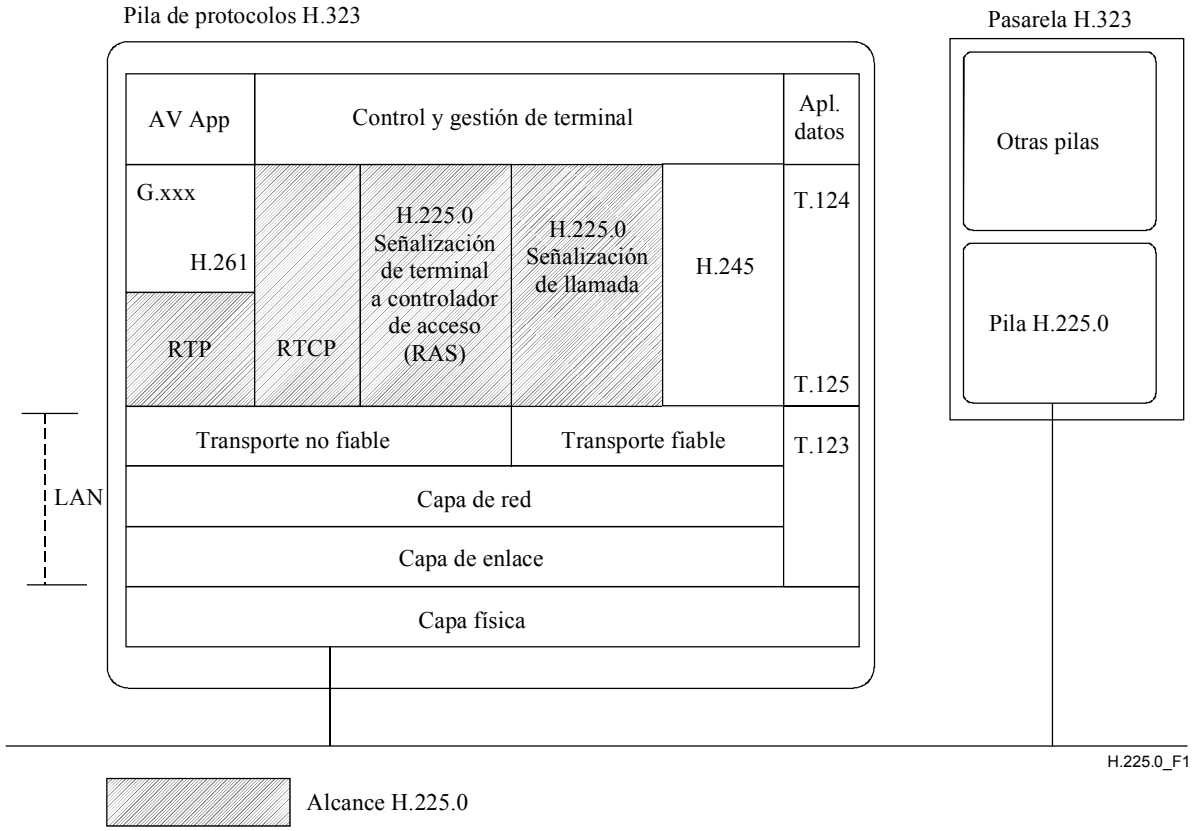


Figura 1/H.225.0 – Alcance H.225.0

El planteamiento general de esta Recomendación consiste en proporcionar un medio de sincronizar paquetes que haga uso de las facilidades de la red de paquetes/de transporte subyacentes. Esta Recomendación no exige que todos los medios y el control se mezclen en un solo tren, que es luego paquetizado. Los mecanismos de trama de la Rec. UIT-T H.221 no se utilizan por las siguientes razones:

- No utilizar H.221 permite a cada medio recibir diferente tratamiento de errores, si así conviene.
- H.221 es relativamente sensible a la pérdida de grupos aleatorios de bits; la paquetización permite mayor solidez en el entorno de la red de paquetes.
- H.245 y mensajes de señalización de llamada H.225.0 pueden enviarse por enlaces fiables proporcionados por la red de paquetes.
- La flexibilidad y la potencia de H.245 comparada con H.242.

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 acutalmente 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 G.711 (1988), *Modulación por impulsos codificados (MIC) de frecuencias vocales*.

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

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

[4] Recomendación UIT-T G.723.1 (1996), *Codificadores vocales: Códec de voz de doble velocidad para la transmisión en comunicaciones multimedios a 5,3 y 6,3 kbit/s.*

[5] 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*.

[6] Recomendación UIT-T H.221 (1999), *Estructura de trama para un canal de 64 a 1920 kbit/s en teleservicios audiovisuales*.

[7] Recomendación UIT-T H.230 (1999), *Señales de control e indicación con sincronismo de trama para sistemas audiovisuales*.

[8] Recomendación UIT-T H.233 (1995), *Sistemas con confidencialidad para servicios audiovisuales*.

[9] Recomendación UIT-T H.242 (1999), *Sistema para el establecimiento de comunicaciones entre terminales audiovisuales con utilización de canales digitales de hasta 2 Mbit/s*.

[10] Recomendación UIT-T H.243 (2000), *Procedimientos para el establecimiento de comunicaciones entre tres o más terminales audiovisuales con utilización de canales digitales de hasta 1920 kbit/s*.

[11] Recomendación UIT-T H.245 (2003), *Protocolo de control para comunicación multimedios*.

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

[13] Recomendación UIT-T H.263 (1998), *Codificación de vídeo para comunicación a baja velocidad binaria*.

[14] Recomendación UIT-T H.320 (1999), *Sistemas y equipos terminales videotelefónicos de banda estrecha*.

[15] Recomendación UIT-T T.122 (1998), *Servicio de comunicación multipunto – Definición de los servicios*.

[16] Recomendación UIT-T T.123 (1999), *Pilas de protocolos de datos específicos de la red para conferencias multimedios*.

[17] Recomendación UIT-T T.125 (1998), *Especificación de protocolo del servicio de comunicación multipunto*.

[18] 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)*.

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

[20] Recomendación UIT-T H.324 (1998), *Terminal para comunicación multimedios a baja velocidad binaria*.

[21] Recomendación UIT-T H.310 (1998), *Sistemas y terminales de comunicación audiovisual de banda ancha*.

[22] 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*.

[23] 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*.

[24] Recomendación UIT-T X.680 (2002) | ISO/CEI 8824-1:2002, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.

[25] Recomendación UIT-T X.681 (2002) | ISO/CEI 8824-2:2002, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información*.

[26] Recomendación UIT-T X.691 (2002) | ISO/CEI 8825-2:2002, *Tecnología de la información – Reglas de codificación en notación de sintaxis abstracta uno – Especificación de las reglas de codificación compactada*.

[27] Recomendación UIT-T E.164 (1997), *Plan internacional de numeración de telecomunicaciones públicas*.

[28] ISO/CEI 10646-1:2000, *Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane*.

[29] Recomendación UIT-T Q.850 (1998), *Utilización de los elementos de información causa y ubicación en el sistema de señalización digital de abonado N.° 1 y en la parte usuario de RDSI del sistema de señalización N.° 7*.

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

[31] Recomendación UIT-T H.235 (2000), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.

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

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

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

[35] IETF RFC 1766 (1995), *Tags for the Identification of Languages*.

[36] Recomendación UIT-T H.248 (2000), *Protocolo de control de las pasarelas*.

[37] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[38] IETF RFC 3551 (2003), *RTP: RTP Profile for Audio and Video Conferences with Minimal Control*.

[39] IETF RFC 2032 (1996), *RTP: Payload format for H.261 Video Streams*.

[40] Recomendación UIT-T X.690 (2002), | ISO/CEI 8825-1:2002, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida*.

3 Definiciones

Véanse las definiciones de la Rec. UIT-T H.323. En la Rec. UIT-T H.323, el término "punto extremo" se utiliza para referirse a los terminales, pasarelas y unidades de control multipunto como elementos capaces de recibir o iniciar llamadas. En la presente Recomendación, el término "terminal" se utiliza a menudo de manera general en descripciones de establecimiento de la comunicación y debe entenderse que se refiere a un elemento que puede tomar parte en el establecimiento de la comunicación, incluida una pasarela o unidad de control multipunto.

4 Convenios

En esta Recomendación se emplea el tiempo futuro de los verbos para indicar un requisito obligatorio y se emplea el verbo modal "deber" para sugerir que una característica o procedimiento son facultativos. Se utiliza el verbo modal "poder" para hacer alusión a una acción o acontecimiento facultativos sin expresar una preferencia.

Cuando se utiliza un término tal como "MCU", se hace alusión a un MCU H.323. Si se desea hacer alusión a un MCU H.231, se hará explícitamente.

En esta Recomendación, kilobits/segundo se abrevia por kbit/s y se expresa en unidades de 1000. Así, 64 kbit/s significa 64 000 bits por segundo.

A menos que se indique otra cosa, la variante alineada de las reglas de codificación compactada (PER) de la ASN.1 se utilizará para todas las ASN.1 especificadas en esta Recomendación.

Los nombres de mensajes Q.931 aparecen en letras mayúsculas. La ASN.1 aparece en **negritas**.

5 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

5.1 Abreviaturas generales

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

CIF Formato intermedio común (*common intermediate format*)

CRV Valor de referencia de llamada (*call reference value*)

ECS Señal de control de criptación (*encryption control signal*)

GOB Grupo de bloques (*group of blocks*)

H-MLP Protocolo multicapa de alta velocidad (*high speed multi-layer protocol*)

HSD Datos de alta velocidad (*high speed data*)

IA5 Alfabeto Internacional N.° 5 (*international alphabet No. 5*)

IE Elemento de información (*information element*)

IETF Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)

IP Protocolo Internet (*Internet protocol*)

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

LD-CELP Predicción lineal con excitación por código con bajo retardo (*low delay – code excited linear prediction*)

LSB Bit menos significativo (*least significant bit*)

LSD Datos a baja velocidad (*low speed data*)

MB Macro bloque (véase la Rec. UIT-T H.261)

MBE Extensión de multibyte (*multi-byte extension*)

MCC Instrucción multipunto de conferencia (*multipoint command conference*)

MCN Instrucción multipunto de negación (*multipoint command negating*)

MCS Instrucción multipunto de transmisión de datos simétrica (*multipoint command symmetrical data transmission*)

MCS Servicio de comunicación multipunto (*multipoint communication service)*

MCU Unidad de control multipunto (*multipoint control unit*)

MF Multitrama (*multiframe*)

MIC Modulación por impulsos codificados

MLP Protocolo multicapa (*multi-layer protocol*)

MPI Intervalo de imagen mínimo (*minimum picture interval*)

MSB Bit más significativo (*most significant bit*)

NA No aplicable (*not applicable*)

NS No normalizado (*non-standard*)

NSAP Punto de acceso al servicio de red (*network service access point*)

PDU Unidad de datos de protocolo (*protocol data unit*)

QCIF Cuarto de formato intermedio común (*quarter common intermediate format*)

QoS Calidad de servicio (*quality of service*)

RAS Registro, admisión y estado (*registration, admission and status*)

RCC Red con conmutación de circuitos

RTCP Protocolo de control de transporte en tiempo real (*real-time transport control protocol*)

RTP Protocolo de transporte en tiempo real (*real-time transport protocol*)

SBE Extensión de un solo byte (*single byte extension*)

SC Canal de servicio (*service channel*)

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

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

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

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

URL Localizador de recurso uniforme (*uniform resourse locator*)

VCF Instrucción de vídeo de "petición de congelación de imagen" (*video command "freeze picture request"*)

VCU Instrucción de vídeo de "petición de actualización rápida" (*video command "fast update request"*)

5.2 Abreviaturas de mensajes RAS

ACF Confirmación de admisiones (*admissions confirm*)

ARJ Rechazo de admisiones (*admissions reject*)

ARQ Petición de admisiones (*admissions request*)

BCF Confirmación de anchura de banda (*bandwidth confirm*)

BRJ Rechazo de anchura de banda (*bandwidth reject*)

BRQ Petición de anchura de banda (*bandwidth request*)

DCF Confirmación de desligamiento (*disengage confirm*)

DRJ Rechazo de desligamiento (*disengage reject*)

DRQ Petición de desligamiento (*disengage request*)

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

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

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

IACK Acuse de recibo de petición de información (*information request acknowledgement*)

INAK Acuse de recibo negativo de petición de información (*information request negative acknowledgement*)

IRQ Petición de información (*information request*)

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

LCF Confirmación de localización (*location confirm*)

LRJ Rechazo de localización (*location reject*)

LRQ Petición de localización (*location request*)

RAC Confirmación de disponibilidad de recurso (*resource availability confirmation*)

RAI Indicación de disponibilidad de recurso (*resource availability indication*)

RCF Confirmación de registro (*registration confirm*)

RIP Petición en curso (*request in progress*)

RRJ Rechazo de registro (*registration reject*)

RRQ Petición de registro (*registration request*)

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

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

UCF Confirmación de desregistro (*unregistration confirm*)

URJ Rechazo de desregistro (*unregistration reject*)

URQ Petición de desregistro (*unregistration request*)

6 Mecanismo de paquetización y de sincronización

6.1 Planteamiento general

Antes de que se efectúen llamadas, un punto extremo puede descubrir/registrarse en un controlador de acceso. Si así ocurre, es conveniente que el punto extremo conozca la antigüedad del controlador de acceso en el que se registra. También es conveniente que el controlador de acceso conozca la antigüedad de los puntos extremos que se registran en él. Por estas razones, el *descubrimiento* y las secuencias de registro contienen un IDENTIFICADOR DE OBJETO de estilo H.245 que permite determinar la antigüedad en términos de la versión de la Rec. UIT-T H.323 implementada. Esta secuencia puede también contener partes opcionales de mensaje no normalizadas para permitir que los puntos extremos establezcan relaciones no normalizadas. Al final de esta secuencia, los

controladores de acceso y los puntos extremos conocen mutuamente los números de versión y la situación normalizada de sus correspondientes interlocutores.

El número de versión es obligatorio y la información no normalizada es opcional en la secuencia de establecimiento/conexión descrita a continuación, para permitir a los dos puntos extremos e informarse entre sí de su antigüedad y situación no normalizada. Adviértase, sin embargo, que todos los mensajes de señalización de llamada H.225.0 tienen un campo para un mensaje opcional no normalizado en el elemento de información usuario-usuario, y que todos los mensajes de canal RAS tienen un campo opcional para información no normalizada. Además, se ha definido un mensaje RAS no normalizado que puede enviarse en cualquier momento.

El canal no fiable para registro, admisiones y mensajería de situación se denomina el canal RAS. El procedimiento general para iniciar una llamada es enviar una petición de admisión obligatoria por el canal RAS[3], seguida por un mensaje Establecimiento inicial en una dirección de transporte de canal fiable (esta dirección puede haber sido devuelta en el mensaje de confirmación o admisión o puede haberle resultado conocida al terminal llamante). De resultas de este mensaje inicial, comienza una secuencia de establecimiento de la comunicación sobre la base de operaciones de señalización de llamada H.225.0 con las mejoras descritas más adelante. La secuencia está completa cuando el terminal recibe en el mensaje Conexión una dirección de transporte fiable en la cual enviar mensajes de control H.245[4].

Cuando los mensajes se envían por el canal de señalización de llamada H.225.0 fiable, se enviará únicamente un mensaje completo dentro de los límites definidos por el transporte fiable; no habrá ninguna fragmentación de mensajes H.225.0 en las PDU de transporte. (En las implementaciones IP descritas en el apéndice IV, esta PDU es definida por TPKT.)

Una vez que se ha establecido el canal de control H.245 fiable, pueden establecerse canales adicionales para audio, vídeo y datos a tenor del resultado de intercambio de capacidades utilizando procedimientos de canal lógico H.245. Además, la naturaleza de la conferencia multimedios en el lado red de paquetes (centralizada o bien distribuida/multidifusión) es negociada conexión por conexión[5]. Esta negociación se efectúa según el medio, en el sentido de que, por ejemplo, el audio/vídeo puede ser distribuido, mientras que los datos y el control son centralizados.

Cuando los mensajes se envían por el canal de control H.245 fiable, puede enviarse más de un mensaje dentro de los límites definidos por el transporte fiable mientras se envíen mensajes completos; no habrá ninguna fragmentación de mensajes H.245 en las PDU de transporte. (En las implementaciones IP descritas en el apéndice IV, esta PDU es definida por TPKT.)

Los terminales H.225.0 serán capaces de enviar audio y vídeo utilizando RTP a través de canales no fiables para minimizar el retardo. Puede aplicarse ocultación de errores u otra acción de recuperación para superar la pérdida de paquetes; en general, los paquetes de audio/vídeo no se retransmiten, pues se originaría así un retardo excesivo en el entorno de la red de paquetes[6]. Se supone que los errores de bit son detectados en las capas inferiores, y que en los paquetes con error

---

[3] Un terminal que no se ha registrado en un controlador de acceso no necesita enviar una petición de admisiones.

[4] Adviértase que la dirección H.245 puede enviarse en el mensaje de aviso o progresión de la llamada para acortar el tiempo de establecimiento de la comunicación. Obsérvese que el canal H.245 se puede abrir inmediatamente después de la recepción de la dirección H.245 en el mensaje Establecimiento.

[5] La conferencia en el lado LAN puede ser en parte centralizada y en parte distribuida, según decida la MC que controla la conferencia. Sin embargo, el terminal no conoce este dato. Generalmente, por supuesto, todos los terminales verán el mismo modo de comunicaciones seleccionado (SCM, *selected communications mode*) (véase en la Rec. UIT-T H.243 una definición).

[6] La actualización rápida de tramas completas MB o GOB puede solicitarse mediante señalización H.245.

no son enviados hasta H.225.0. Adviértase que el audio/vídeo y la señalización de llamada/control H.245 nunca se envían por el mismo canal, y no comparten una estructura de mensaje común. Los terminales H.225.0 serán capaces de enviar y recibir audio y vídeo en direcciones de transporte separadas utilizando ejemplares separados de RTP para permitir números de secuencia de trama específicos de los medios y tratamiento separado de calidad de servicio para cada medio. Sin embargo, queda en estudio un modo opcional en el que se mezclen paquetes de audio y vídeo en una sola trama que se envía a una única dirección de transporte.

Las capacidades T.120 se negocian utilizando H.245, y al recibo de mensajes apropiados, se establecen conferencias T.120 utilizando las pilas de transporte/red de paquetes T.123, si así conviene. T.120 se transportará por la red de paquetes entre puntos extremos en otra dirección de transporte. El cuadro 1 muestra el número de identificadores de TSAP utilizados para cada medio en una llamada punto a punto. Es también cierto que un determinado terminal H.323 puede conseguir participar en más de una conferencia a un tiempo, lo que da lugar al uso de identificadores de TSAP adicionales. Todos los canales lógicos H.245 son unidireccionales, excepto los asociados con T.120, que son bidireccionales.

Cuadro 1/H.225.0 – ID de TSAP utilizados por H.225.0 por llamada unidifusión punto a punto

Utilización de ID de TSAP	Fiable o no fiable	Conocidos o dinámicos
Audio/RTP	No fiable	Dinámico
Audio/RTCP	No fiable	Dinámico
Vídeo/RTP	No fiable	Dinámico
Vídeo/RTCP	No fiable	Dinámico
Señalización de llamada	Fiable	Conocido o dinámico
H.245	Fiable	Dinámico
Datos (T.120)	Fiable	Conocido o dinámico
RAS	No fiable	Conocido o dinámico
NOTA – Si se utilizan identificadores de TSAP conocidos, puede haber sólo un único punto extremo por dirección de red. Además, en el modelo de llamada directa, el llamante requiere un identificador de TSAP conocido para que el canal de señalización de llamada inicie la llamada.		

Aunque la dirección de transporte para, por ejemplo, audio y vídeo, puede compartir la misma dirección de la red de paquetes y diferir sólo en el identificador de TSAP, algunos fabricantes pueden decidir utilizar diferentes direcciones de la red de paquetes para audio y vídeo. El único requisito es que se siga el convenio de los anexos A y B en la numeración de identificadores TSAP en la sesión RTP[7].

El cuadro 1 describe el caso básico de operaciones unidifusión punto a punto entre dos terminales. Para facilitar la construcción de pasarelas, MCU, y controladores de acceso, se pueden utilizar los ID de TSAP dinámicos en vez de los ID de TSAP conocidos. Los cuadros 2 y 3, ilustran un ejemplo de la utilización de los ID de TSAP en el caso de pasarela/MCU y en el caso de controladores de acceso.

[7] Adviértase que puede utilizarse cualquier ID de TSAP para la sesión RTP inicial; la razón principal de seguir el convenio RTP es para una posible interoperabilidad IETF RTP.

Cuadro 2/H.225.0 – ID de TSAP utilizados en una MCU/un puerto de pasarela (ejemplo unidifusión)

Utilización de ID de TSAP	Fiable o no fiable	Conocidos o dinámicos
Audio/RTP	No fiable	Dinámico
Audio/RTCP	No fiable	Dinámico
Vídeo/RTP	No fiable	Dinámico
Vídeo/RTCP	No fiable	Dinámico
Señalización de llamada	Fiable	Dinámico (nota)
H.245	Fiable	Dinámico
Datos (T.120)	Fiable	Dinámico
RAS	No fiable	Dinámico (nota)
NOTA – Véase la nota 1 al cuadro 3.		

Cuadro 3/H.225.0 – Ejemplo de la utilización de ID de TSAP por un controlador de acceso H.225.0 por punto extremo que soporte el modelo de llamada por mediación de un controlador de acceso de la figura 28/H.323 para una llamada punto a punto

Utilización de ID de TSAP	Fiable o no fiable	Conocidos o dinámicos	Número de canales
Señalización de llamada	Fiable	Dinámico o conocido (Nota 1)	2 por llamada (Nota 2)
H.245	Fiable	Dinámico	2 por llamada (Nota 2)
RAS	No fiable	Conocido	1
NOTA 1 – Si se utiliza el ID de TSAP conocido, el controlador de acceso puede limitarse a un único punto extremo por dispositivo; por tanto, deben utilizarse ID de TSAP dinámicos. NOTA 2 – 0 para modelo de llamada directa; 2 para modelo de llamada por mediación de un controlador de acceso.			

Adviértase que se utiliza una dirección de transporte fiable conocida para el establecimiento de la comunicación en el caso de terminal a terminal, y también para el caso de mediación de un controlador de acceso. La conexión de señalización de llamada fiable se mantendrá activa hasta que se reciba un mensaje de liberación completa para todas las llamadas activas señalizadas en un canal de señalización de llamada.

Adviértase que puede haber abierto en un determinado momento más de un canal H.245, es decir, un punto extremo puede estar en más de una llamada/conferencia al mismo tiempo. Adviértase también que dentro de una determinada llamada, un terminal puede tener abierto más de un canal del mismo tipo, por ejemplo, dos canales de audio para audio estéreo. La única limitación es que habrá exclusivamente un canal de control H.245 en cada sentido por llamada punto a punto.

La señalización de canal lógico H.245 se utiliza para comenzar y detener la utilización de protocolos de vídeo, audio y datos. Este proceso exige el cierre del canal abierto, y la posterior reapertura con un nuevo modo de operación. Como parte del proceso de apertura del canal, antes de enviar el acuse de canal lógico abierto, el punto extremo utiliza la frecuencia ARQ/ACF o BRQ/BCF para asegurar que hay disponible suficiente anchura de banda para el nuevo canal (a menos que haya disponible suficiente anchura de banda de una secuencia ARQ/ACF o BRQ/BCF anterior). En algunos casos, la pasarela puede encontrar que el cambio de modo en el lado RCC se produce mucho más rápidamente que el cambio de modo en el lado red de paquetes, lo que

introduce la posibilidad de pérdida de información de audio. La pasarela podría adoptar varios procedimientos a discreción del fabricante:

a) la pasarela puede transcodificar audio, ocultando así los cambios de modo en el lado RCC;

b) la pasarela puede simplemente desechar la información de audio; o

c) la pasarela puede funcionar como una MCU H.231, obteniendo así control sobre todos los cambios de modo en el lado RCC.

No existe una regla general para saber si los procedimientos H.245 o RTP (véanse los anexos A, B y C) tienen precedencia; cada conflicto y su resolución se menciona específicamente en esta Recomendación.

Obsérvese también que no hay ninguna asociación fija entre los SSRC y los canales lógicos. La Rec. UIT-T H.245 proporciona esta asociación que puede utilizar para la sincronización de audio/vídeo.

En general, son posibles dos tipos de modos de operación conferencia en el lado red de paquetes: distribuido y centralizado. Es también posible que puedan hacerse elecciones diferentes para diferentes medios, por ejemplo, audio/vídeo distribuido y datos centralizados. Los procedimientos para determinar qué clase de conferencia por establecer figuran en la Rec. UIT-T H.323; los mensajes de esta Recomendación se destinan a soportar todas las combinaciones permitidas, señalándose que el control y datos distribuidos quedan en estudio aunque son soportados por la señalización de capacidades H.245.

6.2 Utilización de RTP/RTCP

El punto extremo H.225.0 deberá poder utilizar los ID de TSAP distintos para audio y vídeo y los canales RTCP asociados descritos en los anexos A y B. Opcionalmente, los puntos extremos pueden decidir utilizar diferentes direcciones de la red de paquetes para audio y vídeo, pero para cada dirección de la red de paquetes se debe seguir el convenio de los anexos A y B en el uso de ID de TSAP. Utilizando señalización H.245 pueden establecerse canales de audio y de vídeo adicionales si el terminal soporta esta capacidad.

Sigue en estudio una capacidad opcional para utilizar una sola dirección de transporte para audio y vídeo.

A menos que se mencione específicamente aquí una excepción, las implementaciones seguirán las del RTP contenidas en el anexo A, a menos que sean modificadas por texto en esta Recomendación. Las implementaciones seguirán el perfil RTP (véase el anexo B) únicamente, como se menciona específicamente en esta Recomendación.

Los traductores y mezcladores de RTP no son elementos del sistema H.323, y toda información sobre ellos que figure en los anexos A y B deberá considerarse informativa. Se señala que tanto las pasarelas como las MCU tienen algunos aspectos de los mezcladores y de los traductores, y la información de los anexos A y B puede ser de utilidad en la implementación de pasarelas y MCU. Sin embargo, las MCU no son mezcladores, y los mezcladores no son MCU. Adviértase que las pasarelas, por ejemplo, en una llamada de red de paquetes a red de paquetes a través de la pasarela, pueden actuar como traductores.

Versión (V): Se utilizará la versión 2 del RTP.

Cuenta de CSRC (CC): El uso de la cuenta de CSRC en esta Recomendación es opcional. Cuando no se utiliza, el valor de CC será cero (0). El CSRC puede ser utilizado por las MCU para proporcionar información sobre contribuyentes a la suma de audio cuando se produce procesamiento de audio distribuido. Adviértase que no hay capacidades asociadas con la aptitud para entender la cuenta de CSRC, por lo que la MCU/MC no tiene ningún modo de conocer si y cómo el terminal de la conferencia hace uso de la información.

CNAME: En el caso más simple de una conexión punto a punto por la red de paquetes, el SSRC se utiliza para identificar una fuente de audio/vídeo desde un terminal, y los dos trenes están asociados por un CNAME suministrado por el mismo punto extremo que se especifica en el anexo A.

Cuando se utiliza RTCP, los paquetes RR o SR se enviarán periódicamente como se describe en el anexo A. Se utilizará el mensaje CNAME SDES. Otros mensajes SDES (véase el anexo A) son opcionales, pero no se utilizarán para control de conferencia o información de conferencia cuando se utilizan funciones de control H.245 y/o T.120. La información proporcionada por la Rec. UIT-T H.245 y/o la Rec. UIT-T T.120 se considerará la información correcta.

No se dependerá del mensaje RTCP BYE para la terminación de la sesión RTP. El terminal H.323 determina cuándo es desconectada una llamada mediante los procedimientos de la Rec. UIT-T H.323. La única utilización obligatoria del paquete RTCP BYE es para la resolución de colisiones de SSRC.

El terminal H.323, cuando interviene en cualquier conferencia, sea punto a punto o multipunto, restringirá la velocidad binaria del canal lógico promediada en un periodo definido en la Rec. UIT-T H.245 a la señalizada en las **instrucciones de control de flujo** H.245 **(FlowControlCommands** H.245), instrucciones de canal lógico H.245, y el mecanismo de control de flujo T.120.

Cuando el terminal H.323 está conectado a una pasarela H.323, la pasarela utilizará los medios de la Rec. UIT-T H.245 y la Rec. UIT-T T.120 para obligar al terminal H.323 a transmitir a una velocidad inferior o igual a las velocidades de medios del lado RCC y recibirá a una velocidad igual o superior a la velocidad RCC, con las siguientes excepciones:

- La anchura de banda de control en la red de paquetes no necesita concordar con la de la Rec. UIT-T H.221.
- La anchura de banda de audio en la red de paquetes puede concordar con la de la Rec. UIT-T H.221 en la RCC, pero con la transcodificación de pasarela, no se necesita concordancia.
- En el caso de que la pasarela esté utilizando un reductor de velocidad, el terminal H.323 del lado red de paquetes no rebasará la velocidad señalizada H.245, que probablemente será inferior a la velocidad que se envía por la RCC.

La criptación para los puntos extremos H.323 queda en estudio.

6.2.1 Audio

Antes de considerar cómo se paquetiza el audio utilizando el RTP, debemos considerar cómo se señaliza mediante H.245, y la relación de esta señalización con el RTP. En general, cuando se abre el canal de audio, se abre un canal lógico H.245. La señalización H.245 en la estructura **capacidad de audio (AudioCapability)** se expresa en forma de máximo número de tramas por paquete. El tamaño de trama para esta Recomendación varía con la codificación de audio en uso.

Todos los terminales H.323 que ofrecen comunicación de audio soportarán G.711. Para todos los códecs de audio orientados a las tramas, los receptores señalizarán el máximo número de tramas de audio que son capaces de aceptar en un único paquete de audio. Los transmisores pueden enviar cualquier número entero de tramas de audio en cada paquete, hasta el máximo especificado por el receptor. Los transmisores no dividirán las tramas de audio a lo largo de los paquetes, y enviarán números completos de octetos en cada paquete de audio.

Los códecs basados en muestras, tales como los códecs G.711 y G.722, se considerarán orientados a las tramas, con un tamaño de trama de ocho muestras. (Para más información sobre las directrices relativas a la codificación audio basada en muestras, véase el anexo B.) Con los algoritmos de audio tales como el G.723.1, que utilizan más de un tamaño de trama de audio, las fronteras de trama de audio dentro de cada paquete serán señalizadas dentro de banda al canal de audio.

Con los algoritmos de audio que utilizan un tamaño de trama fijo (véanse en las Recomendaciones UIT-T G.728 y G.729 el tamaño de trama utilizado por cada uno), los límites de trama de audio vendrán determinados por la relación tamaño de paquete/tamaño de trama de audio; en otras palabras, sólo se pondrán tramas de audio completas en el paquete RTP.

Tipo de cabida útil (PT): Sólo se utilizarán tipos de cabida útil UIT-T tales como (0)[PCMU], (8)[PCMA], (9)[G722], y (15)[G728] para los códecs de la UIT señalizados en la Rec. UIT-T H.245. Los tipos de cabida útil dinámica intercambiados mediante la señalización H.245 se utilizarán para cualesquiera tipos de cabida útil UIT-T no enumerados en el anexo B.

Se recomienda que si se observa una interrupción en los números de secuencia, el receptor puede repetir los sonidos recibidos más recientes de modo que la amplitud del sonido repetido caiga a silencio; pueden utilizarse otros procedimientos similares a discreción del fabricante.

Cada octeto G.711 estará alineado en un paquete RTP. El bit de signo de cada octeto G.711 corresponderá al bit más significativo del octeto en el paquete RTP (es decir, suponiendo que las muestras G.711 son tratadas como octetos en el computador central, el bit de signo será el bit más significativo del octeto definido por el formato del computador central).

Cuando se envía MIC a 48/56 kbit/s hacia la red de paquetes, la pasarela H.323 rellenará los 1 ó 2 bits extra de cada octeto de conformidad con la nota 2 del cuadro 1b/G.711, y utilizará los valores RTP para PCMA o PCMU(8 ó 0). En ley μ, el relleno consiste en un "1" en los séptimo y octavo bits. En ley A, el séptimo bit será 0 y el octavo bit 1. En sentido opuesto, la pasarela H.323 truncará 64 kbit/s G.711 en el lado red de paquetes para ajustarse a la velocidad G.711 utilizada en H.320. Así, en el lado red de paquetes sólo se utilizará 64 kbit/s G.711.

Cuando se envíe 48/56 kbit/s G.722 hacia la red de paquetes, la pasarela H.323 rellenará los 1 ó 2 bits extra de cada octeto, y utilizará tipos de cabida útil RTP dinámica señalizados por la Rec. UIT-T H.245 para diferenciar entre 64 kbit/s (que utiliza PT = 9) y los casos de velocidad reducida. En el sentido opuesto, la pasarela H.323 truncará 64 kbit/s G.722 en el lado red de paquetes para ajustarse a la velocidad G.711 utilizada en H.320. Así, en el lado red de paquetes sólo se utilizará 64 kbit/s G.722.

Si es posible, el terminal H.323 debe hacer uso de la característica de supresión de silencio del RTP, especialmente cuando la conferencia es multidifusión. El terminal H.323 podrá recibir trenes RTP comprimidos de silencio. Los codificadores pueden omitir el envío de señales de audio durante periodos de silencio después de enviar una sola trama de silencio, o pueden enviar tramas de relleno de fondo de silencio si estas técnicas son especificadas por la Recomendación sobre códecs de audio en uso.

6.2.2 Mensajes de vídeo

Tipo de cabida útil (PT, *payload type*): Sólo se utilizarán tipos de cabida útil UIT-T tales como el que se utiliza en la Rec. UIT-T H.261 o la Rec. UIT-T H.263 para los códecs de la UIT señalizados en la Rec. UIT-T H.245. Pueden utilizarse tipos de cabida útil dinámica en códecs que pueden ser señalizados por H.245 y para los cuales no se han definido formatos de paquetización.

Marcador (M, *marker*): El bit marcador se debe fijar según los procedimientos descritos en el anexo A, salvo en los casos en que aumente el retardo de extremo a extremo.

A fin de recuperarse de la pérdida de paquetes de vídeo, se utilizarán H.245 **VideoFastUpdatePicture**, **VideoFastUpdateMB** y **VideoFastUpdateGOB**. La utilización de los paquetes de control RTCP petición de trama completa (FIR, *full intra request*) [envíeme una trama completa] y acuse de recibo negativo (NACK, *negative acknowledgment*) [envíeme ciertos paquetes] es facultativa y se señaliza en las capacidades H.245.

En RFC 2032 [39] sección 5 el método de recuperación tras error 3) puede no ser práctico si NACK no llega dentro de un periodo de trama.

H.261 está paquetizada en el lado red de paquetes como en el anexo C. Mientras se disponga de paquetes RTP suficientemente grandes, no se requiere fragmentación en las fronteras de MB por el transmisor. Sin embargo, si el terminal H.323 fragmenta paquetes H.261 en el nivel RTP, esta fragmentación ocurrirá en las fronteras MB. Todos los terminales H.323 podrán recibir paquetes fragmentados MB así como paquetes fragmentados GOB, o paquetes con una combinación de MB y GOB. Adviértase que de no conseguir soportar la fragmentación de MB en el transmisor puede dar lugar a la pérdida de un GOB completo, y puede también rebajar la velocidad de paquetes. Los paquetes RTP utilizados no deberán rebasar el tamaño de la máxima de unidad de transferencia (MTU, *maximun transfer unit*) en una determinada red de paquetes para maximizar la solidez de la operación, pero si el elemento más pequeño del esquema de codificación codificado independientemente (por ejemplo, un macrobloque) es mayor que el tamaño de la MTU, no es necesario fragmentar el paquete en unidades MTU. Los MB no se separarán a lo largo de los paquetes; todos los paquetes terminarán en una frontera de GOB o de MB. El transmisor H.323 puede decidir rellenar un paquete que contenga un pequeño GOB con MB adicionales, pero esto no es necesario.

Para excluir la posibilidad de corrupción en múltiples imágenes causadas por la pérdida de un paquete RTP, el paquetizador RTP en un punto extremo H.323 no incluirá vídeo de más de una imagen en un paquete RTP.

SBIT es el número de bits más significativos que serán ignorados en el primer octeto de datos y EBIT es el número de bits menos significativos que serán ignorados en el último octeto de datos.

El paquetizador RTP no alineará vídeo en octetos intencionalmente al principio de los paquetes RTP. En otras palabras, si EBIT = n en un paquete RTP, SBIT en el siguiente paquete RTP será igual 8 – n, $0 < n < 8$, y si EBIT = 0 en un paquete RTP, SBIT en el siguiente paquete RTP será igual a 0. Este requisito evita posible retardo adicional de extremo a extremo causado por el desplazamiento de bits. Este requisito se aplicará a través de las fronteras de imagen.

El anexo D especifica una extensión H.323 del encabezamiento de paquete de vídeo que contiene una cuenta de octetos. La utilización de esta extensión facultativa se describe en el anexo D.

Véase en el apéndice IV asesoramiento específico para la red de paquetes sobre la paquetización de vídeo.

6.2.3 Mensajes de datos

No hay mensajes ni formatos de datos especiales; T.120 se utiliza en la red de paquetes como en la Rec. UIT-T T.123. La comparación entre la conferencia de datos centralizada y distribuida por la red de paquetes se describe en la Rec. UIT-T H.323, y se negocia mediante H.245.

El control de flujo T.120 en la red de paquetes es gestionado utilizando protocolos de red de paquetes cuando son solicitados por **FlowControlCommands (Instrucciones de control de flujo)** y tienen límites **maxBitRate (velocidad binaria máxima)**.

Véase en la Rec. UIT-T H.323 los procedimientos utilizados para conectar una conferencia T.120 en curso con una conferencia H.323, o para añadir una llamada H.323 a una conferencia T.120.

El protocolo a utilizar por H.224 en la red de paquetes queda en estudio.

7 Definición de mensajes H.225.0

En esta cláusula se trata la definición de los mensajes para el establecimiento de la comunicación, control de llamada y las comunicaciones entre terminales, pasarelas, controladores de acceso y MCU.

Las definiciones ASN.1 para todos los mensajes H.225.0 figuran en el anexo H.

7.1 Utilización de mensajes Q.931

Las implementaciones seguirán la Rec. UIT-T Q.931 como se especifica en esta Recomendación. Los terminales pueden también soportar APDU H.450 opcionales en el elemento de información (IE) usuario-usuario. Los mensajes contendrán todos los elementos de información obligatorios y pueden contener cualquiera de los elementos de información opcionales definidos en la Rec. UIT-T Q.931 que se describen en esta Recomendación. Adviértase que el punto extremo H.225.0 puede, según la Rec. UIT-T Q.931, ignorar todos los mensajes opcionales que no soportan sin dañar la interoperabilidad, pero responderá a un mensaje desconocido con un mensaje de estado.

Cada punto extremo H.225.0 será capaz de recibir e identificar un mensaje de señalización de llamada H.225.0 incluso si contiene una APDU H.450 en el elemento de información usuario-usuario. Será capaz de procesar los mensajes de señalización de llamada H.225.0 obligatorios; puede ser capaz de procesar los mensajes de señalización de llamada H.225.0 opcionales. En cualquier caso, cada punto extremo H.225.0 será capaz de ignorar mensajes que le resulten desconocidos sin perturbar el funcionamiento.

Cada punto extremo H.225.0 será capaz de interpretar y generar los elementos de información que sean de su mandato en lo sucesivo para los respectivos mensajes de señalización de llamada H.225.0 y APDU H.450 en el elemento de información usuario-usuario. Podría interpretar y generar también los elementos de información opcionales definidos a continuación. Puede también interpretar otros elementos de información de Q.931 y otros protocolos de la serie Q o protocolos H.450. Los puntos extremos serán capaces de ignorar los elementos de información desconocidos contenidos en un mensaje de señalización de llamada H.225.0 o una APDU H.450 sin perturbar el funcionamiento. Los procedimientos para recibir elementos de información "se requiere comprensión" no reconocidos se aplicarán conforme a 5.8.7.1/Q.931. Los puntos extremos H.225.0 no enviarán múltiples elementos de información del mismo tipo en el mismo mensaje; por ejemplo, no enviarán múltiples elementos de información número de parte llamante según se describe en el anexo A/Q.951.3.

Los elementos de información se codificarán de acuerdo con la Rec. UIT-T Q.931, salvo aquellas partes en que se apliquen las modificaciones de la presente Recomendación. Sin embargo, se seguirá siempre el orden apropiado de los elementos de información dentro de un mensaje prescrito en la Rec. UIT-T Q.931, sin atender al orden de los elementos indicados en la presente Recomendación.

Los sistemas intermedios (pasarelas y controladores de acceso) seguirán las reglas siguientes en relación con los mensajes opcionales y elementos de información de señalización de llamada H.225.0:

1) La pasarela debe remitir y el controlador de acceso remitirá todos los elementos de información (opcionales u obligatorios) después de la modificación apropiada asociados con mensajes de señalización de llamada H.225.0 obligatorios sea desde el terminal a la pasarela/terminal o en sentido opuesto. Esto incluye elementos de información tales como información usuario-usuario y la información de visualización.
2) Una pasarela debe remitir todos los mensajes de señalización de llamada H.225.0, incluso si contienen una APDU H.450, y elementos de información en ambos sentidos.
3) Un controlador de acceso remitirá todos los mensajes de señalización de llamada H.225.0, incluso si contienen APDU H.450, y elementos de información en ambos sentidos después de la modificación apropiada. Obsérvese que es posible que el controlador de acceso actúe como un elemento de señalización que puede proporcionar características (tales como las características de los servicios suplementarios) y, por lo tanto, modificar, terminar u originar mensajes de señalización de llamada H.225.0.

Las pasarelas H.323 pueden convertir servicios suplementarios de la serie H.450 y mensajes H.225.0 a los correspondiente servicios y mensajes de ISO/CEI 11582, parte usuario de la RDSI y

otras normas de señalización RCC. Los detalles están dentro del ámbito de la Rec. UIT-T H.246 y sus anexos.

Las pasarelas H.323 podrán hacer seguir mensajes de señalización de ISO/CEI 11582, la parte usuario de RDSI y otras normas de señalización, sin modificación, mediante la tunelización de señalización no H.323 en H.225.0. En el anexo M/H.323 M (véanse M.1/H.323. M.2/H.323, etc.) se presenta una información detallada.

En esta versión de esta Recomendación, todas las referencias corresponden a la versión 1998 de la Rec. UIT-T Q.931. Se siguen los procedimientos de 3.1/Q.931 para el establecimiento de conexión en modo circuito. Sin embargo, se recuerda al implementador que aunque el "portador" está siendo señalizado al efecto, no existen "canales B" efectivos del tipo RDSI en el lado red de paquetes. La "llamada" realizada con éxito da lugar a un canal fiable de extremo a extremo que soporta la mensajería H.245. Realmente, el establecimiento del "portador" se efectúa aplicando H.245. Sin embargo, la utilización de Q.931 en el lado red de paquetes permite el interfuncionamiento con Q.931 en el lado RCC así como el aprovisionamiento de un marco verificado para determinar las características generales de llamada orientadas a la conexión.

En general, se utilizan los procedimientos simétricos del anexo D/Q.931, lo cual implica que la máquina de estados Q.931 va seguida como se indica en el anexo D/Q.931 con la excepción de que el procedimiento de D.3/Q.931 (Colisión de llamadas) no se aplicará; la recuperación tras esta condición se deja a la capa de aplicación.

Los puntos extremos que no soporten juegos de códigos Q.931 con cambio a otros juegos ignorarán todos los mensajes Q.931 que utilicen dichos métodos.

El cuadro 4 muestra qué mensajes son obligatorios y opcionales para el establecimiento de la comunicación H.323 y H.225.0 utilizando Q.931 en la red de paquetes.

Cuadro 4/H.225.0 – Utilización de mensajes Q.931/Q.932 en H.225.0

	Transmisión (M, F, O, CM) (nota 1)	**Recepción y acción [M, F, O (nota 2), CM]**
Mensajes de establecimiento de la comunicación		
Aviso	M	M
Llamada en curso	O	CM (notas 3 y 6)
Conexión	M	M
Acuse de conexión	F	F
Progresión	O	CM (nota 6)
Establecimiento	M	M
Acuse de establecimiento	O	O
Mensajes de liberación de llamada		
Desconexión	F	F
Liberación	F	F
Liberación completa	M (nota 4)	M

Cuadro 4/H.225.0 – Utilización de mensajes Q.931/Q.932 en H.225.0

	Transmisión (M, F, O, CM) (nota 1)	**Recepción y acción [M, F, O (nota 2), CM]**
Mensajes de la fase de información de llamada		
Reanudación	F	F
Acuse de reanudación	F	F
Rechazo de reanudación	F	F
Suspensión	F	F
Acuse de suspensión	F	F
Rechazo de suspensión	F	F
Información de usuario	O	O
Mensajes varios		
Control de congestión	F	F
Información	O	CM (nota 6)
Notificación	O	O
Estado	M (nota 5)	M
Indagación de estado	O	M
Mensajes Q.932/H.450		
Facilidad	M	M
Retención	F	F
Acuse de retención	F	F
Rechazo de retención	F	F
Recuperación	F	F
Acuse de recuperación	F	F
Rechazo de recuperación	F	F

NOTA 1 – M: Obligatorio (*mandatory*), F: Prohibido (*forbidden*), O: Facultativo (u opcional), CM: Condicionalmente obligatorio *(conditionally mandatory*). Un mensaje es condicionalmente obligatorio si es obligatorio cuando es soportada una opción.

NOTA 2 – Obsérvese que no se enviará el mensaje Estado en respuesta a un mensaje indicado como "O" en el presente cuadro. El receptor simplemente pasará por alto el mensaje si no lo soporta.

NOTA 3 – Los terminales que han de utilizar pasarelas recibirán y actuarán al recibir Llamada en curso.

NOTA 4 – Liberación completa se necesita para cerrar el canal de señalización de llamada fiable H.225.0. No obstante, el canal de señalización de llamada se mantendrá abierto si otras llamadas que utilizan el mismo canal de señalización de llamada siguen en curso. Adicionalmente, el controlador de acceso puede fijar la bandera **maintainConnection** en VERDADERO para evitar el cierre del canal de señalización de llamada.

NOTA 5 – El punto extremo responderá a un mensaje desconocido con un mensaje Estado; es también obligatoria la respuesta a Indagación de estado. Sin embargo, un punto extremo no tiene que enviar Indagación de estado. Como un asunto práctico, el punto extremo debe ser capaz de comprender un mensaje Estado recibido en respuesta a un mensaje enviado que no es conocido para el receptor.

NOTA 6 – Los puntos extremos que soporten las características facultativas que utilizan estos mensajes (por ejemplo, la tunelización H.245, los servicios suplementarios H.450, la tunelización de los protocolos de señalización o las características que utilizan **genericData**) deberán procesar estos mensajes.

7.2 Elementos de información Q.931 comunes

7.2.1 Elementos de información de encabezamiento

Para todos los mensajes de señalización de llamada H.225.0, hay tres campos comunes que son obligatorios, además del tipo de mensaje, que se describe en esta cláusula.

7.2.1.1 Discriminador de protocolo

Se define en 4.2/Q.931.

Se pondrá a 08H – esto identifica el mensaje como mensaje usuario-red Q.931/I.451 (codificado según la figura 4-2/Q.931). Si un controlador de acceso está actuando como una red para suministrar servicios suplementarios, puede ser adecuado utilizar otro valor. Este asunto queda en estudio.

7.2.1.2 Referencia de llamada

Se define en 4.3/Q.931.

Se soportará una longitud de valor de referencia de llamada de dos octetos por cualquier punto extremo H.323.

El valor de referencia de llamada se elige en el lado que origina la llamada y tiene que ser localmente exclusivo. En una comunicación posterior, el lado llamante y el lado llamado utilizarán este valor de referencia de llamada en todos los mensajes pertenecientes a esta llamada determinada.

El valor se codifica según la figura 4-5/Q.931 para un valor de referencia de llamada de dos octetos. El octeto más significativo del valor de referencia se codifica siempre en el octeto N.º 2.

Obsérvese que el CRV es sólo exclusivo en una determinada parte de una llamada, por ejemplo, entre los terminales, o entre un terminal y un controlador de acceso. Si un determinado terminal tiene dos llamadas en la misma conferencia, cada uno tendrá el mismo ID de conferencia, pero diferentes CRV.

La bandera de referencia de llamada se fijará de acuerdo con los procedimientos descritos en la Rec. UIT-T Q.931.

Nótese que los valores CRV enviados en mensajes RAS se ajustarán a la estructura indicada en la Rec. UIT-T Q.931. Concretamente, la bandera de referencia de llamada se incluirá como el bit más significativo del valor de referencia de llamada. Esto limita el CRV real a la gama de 0 a 32 767, inclusive.

La referencia de llamada global, que se muestra en la figura 4-5/Q.931 y tiene 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.

7.2.1.3 Tipo de mensaje

El tipo de mensaje se codifica según la figura 4-6/Q.931 utilizando los valores especificados en el cuadro 4-2/Q.931. Quedan en estudio las extensiones específicas de H.225.0.

7.2.2 Elementos de información específicos del mensaje

Las reglas de codificación generales para los elementos de información siguientes se definen en 4.5.1/Q.931 y en el cuadro 4-3/Q.931. Se seguirán estas reglas. El mecanismo de escape (véase la figura 4-8/Q.931) es opcional.

7.2.2.1 Capacidad portadora

Este elemento de información se codifica de acuerdo con la figura 4-11/Q.931 y el cuadro 4-6/Q.931. Si este elemento de información se recibe en una llamada de red de paquetes a

red de paquetes puede ser ignorada por el receptor. Si este elemento de información aparece en un mensaje de establecimiento de la comunicación para una conexión de señalización independiente de la llamada, definida en la Rec. UIT-T H.450.1 la codificación se ajustará a 7.2.2.1.2. En todos los demás casos, la codificación deberá ajustarse a 7.2.2.1.1. Las referencias de números de octeto remiten a la figura 4-11/Q.931.

7.2.2.1.1 Codificación por defecto de la capacidad portadora

Las entidades H.323 codificarán los elementos de información de capacidad portadora como se indica a continuación, a menos que se señale otra cosa en las cláusulas subsiguientes.

Bit de extensión para el octeto N.º 3 (bit 8)

– Se pondrá a "1".

Norma de codificación (octeto N.º 3, bits 6-7)

– Se pondrá a "00" indicando "UIT-T".

Capacidad de transferencia de información (octeto N.º 3, bits 1-5)

– Para llamadas originadas en un punto extremo de RDSI se remitirá la información indicada a la pasarela.

  NOTA – Esto permite obtener alguna información adelantada sobre la naturaleza de la conexión que ha de remitirse al punto extremo H.323, por ejemplo, voz solamente *versus* datos *versus* vídeo; esto tendría repercusión en la anchura de banda requerida así como en la aptitud/voluntad de aceptar o no la llamada.

– Las llamadas que se originan en un punto extremo H.323 utilizarán este campo para indicar su deseo de efectuar una llamada audiovisual. Por tanto, el campo se pondrá a "información digital sin restricciones", es decir, "01000" o a "información digital restringida" es decir "01001". Si ha de efectuarse una llamada sólo vocal, el terminal H.323 pondrá la capacidad de transferencia de información a "conversación" (es decir "00000") o a "audio a 3,1 kHz" (es decir "10000").

Bit de extensión para el octeto N.º 4 (bit 8)

– Se pondrá a "0" si la velocidad de transferencia de información se pone a "multivelocidad"; se pondrá a "1" en otro caso.

Modo de transferencia (octeto N.º 4, bits 6-7)

– Especificará "modo circuito", valor "00".

Velocidad de transferencia de información (octeto N.º 4, bits 1-5)

– Se codificará siguiendo el cuadro 4-6/Q.931, salvo que el valor "00000" (para el modo paquete) no se permite a menos que la pasarela se conecte a una red de paquetes.

Multiplicador de velocidad (octeto N.º 4.1)

– Estará presente si la velocidad de transferencia de información se pone a "multivelocidad".

– El bit de extensión (bit 8) se pondrá a "1".

– Los bits 1 a 7 indicarán la anchura de banda necesaria para la llamada definida a continuación (nótese que, contrariamente a la Rec. UIT-T Q.931, se permite aquí un valor de "0000001").

– Para una llamada originada en un punto extremo de RDSI, la pasarela pasará simplemente la información que recibe de la RDSI.

– Para una llamada entrante procedente de un punto extremo H.324, la pasarela fijará el multiplicador de velocidad a 01H.

– Para una llamada entrante procedente de una RDSI-BA, es necesario efectuar cierta traducción de la Rec. UIT-T Q.2931 a la Rec. UIT-T Q.931. Este asunto queda en estudio.

– Para una llamada originada en un punto extremo H.323, éste se utilizará para indicar la anchura de banda a utilizar para esta llamada. Si el sistema llamado es otro punto extremo H.323, este valor puede reflejar la anchura de banda a utilizar en la red de paquetes, pero no es necesario que el terminal de recepción siga esta información. Si interviene una pasarela, este valor reflejará entonces el número de conexiones externas a establecer. La anchura de banda necesaria para la llamada es la anchura de banda requerida en el lado RCC y puede o no concordar con la anchura de banda permitida en la red de paquetes por los mensajes ACF/BCF.

Protocolo de capa 1 (octeto N.º 5)

– El bit de extensión (bit 8) se pondrá a "1".

– Los bits 6 y 7 indicarán el identificador de capa 1, es decir, "01".

– Los bits 1 a 5 indicarán el protocolo de capa 1.

– Los valores permitidos son G.711 (ley A "00011" y ley μ "00010") para indicar una llamada sólo voz y H.221 y H.242 ("00101") para indicar una llamada videotelefónica H.323.

Los octetos N.º 5a, 5b, 5c, 5d, 6 y 7 no estarán presentes.

7.2.2.1.2 Codificación de la capacidad portadora para conexiones de señalización H.450.1 independientes de la llamada

Las entidades H.323 codificarán el elemento de información capacidad portadora como se indica a continuación para las conexiones de señalización independientes de la llamada definidas en la Rec. UIT-T H.450.1.

Bit de extensión para el octeto N.º 3 (bit 8)

– Se pondrá a "1".

Norma de codificación (octeto N.º 3, bits 6-7)

– Se pondrá a "01" indicando "Otra norma internacional". Se señala que, cuando se indique esta norma de codificación, deberá aplicarse la codificación definida en la Rec. UIT-T Q.931 para los octetos 1 a 2 y el bit 8 de los octetos 3 a 4. La capacidad de transferencia de información, el modo de transferencia y la velocidad de transferencia de información se codificarán como se indica sin incluir ningún otro octeto.

Capacidad de transferencia información (octeto N.º 3, bits 1-5)

– Se pondrá a "01000", indicando "Información digital sin restricciones".

Bit de extensión para el octeto N.º 4 (bit 8)

– Se pondrá a "1".

Modo de transferencia (octeto N.º 4, bits 6-7)

– Se pondrá a "00", indicando "Conexión de señalización independiente de la llamada".

Velocidad de transferencia de información (octeto N.º 4, bits 1-5)

– Se pondrá a "00000", indicando "Capacidad de señalización independiente de la llamada".

No se incluirán los octetos 4.1 y superiores.

7.2.2.2 Identidad de la llamada

El posible uso del elemento de información identidad de llamada queda en estudio. En este estudio se debe considerar la marcación en múltiples etapas incluidas terminal-a-controlador-de-acceso-a-terminal, y terminal-a-pasarela-a-terminal y, encaminamiento de fuente flexible.

7.2.2.3 Estado de la llamada

Este elemento de información se codifica según la figura 4-13/Q.931.

Octeto N.º 3 norma de codificación (bits 8-7)

– Se pone a "00" para codificación normalizada indicando UIT-T.

Valor de estado de la llamada (octeto N.° 3, bits 1-6)

– Fijado como en el cuadro 4-8/Q.931, pero no se utilizan los valores globales de estado de la interfaz. Los valores se interpretan como estado de usuario tal como se usa en el anexo D/Q.931. Adviértase que la mayoría de los códigos enumerados no serán generados por un terminal H.323.

7.2.2.4 Número de la parte llamada

Este elemento de información se codifica según la figura 4-14/Q.931 y el cuadro 4-9/Q.931.

Octeto N.º 3 extensión (bit 8)

– Puesto a "1".

Tipo de número (octeto N.º 3, bits 5-7)

– Codificado según los valores y reglas del cuadro 4-9/Q.931.

Identificación del plan de numeración (octeto N.º 3, bits 1-4)

– Codificado según los valores y reglas del cuadro 4-9/Q.931. Un número en forma de una cadena de dígitos marcada debe codificarse como "0000" (desconocido). Si está puesto a "1001" (plan de numeración privado) en una llamada originada en una red de paquetes, esto indica que:

  1) la cadena de dígitos marcada no está presente en Establecimiento; y
  2) la llamada se encaminará mediante una dirección de alias en la información usuario-usuario.

Tipo de número (octeto N.º 3, bits 5-7)

– Codificado según los valores y reglas del cuadro 4-9/Q.931. Un número con la identificación de plan de numeración codificada como "0000" (desconocido) se codificará como "000" (desconocido). Un número con la identificación de plan de numeración codificada como "0001" (plan de numeración RDSI/telefonía, Rec. UIT-T E.164) con el tipo de número codificado como "000" (desconocido) puede utilizarse para compatibilidad hacia atrás.

"Dígitos" de número

– Cualquier número de caracteres IA5, según los formatos especificados en el plan de numeración/marcación apropiado.

NOTA – Un número E.164 estará formado solamente por los caracteres IA5 "0", "1", "2", "3", "4", "5", "6", "7", "8", "9" y "0".

7.2.2.5 Subdirección de la parte llamada

Se utiliza como en la Rec. UIT-T Q.931.

7.2.2.6 Número de la parte llamante

Este elemento de información se codifica según la figura 4-16/Q.931 y el cuadro 4-11/Q.931.

Tipo de número (octeto N.º 3, bits 5-7)

– Codificado según los valores y reglas del cuadro 4-11/Q.931. Un número con la identificación de plan de numeración codificada como "0000" (desconocido) se codificará como "000" (desconocido). Un número con la identificación de plan de numeración codificada como "0001" (plan de numeración RDSI/telefonía, Rec. UIT-T E.164) con el tipo de número codificado como "000" (desconocido) puede utilizarse para compatibilidad hacia atrás.

Identificación del plan de numeración (octeto N.º 3, bits 1-4)

– Codificada según los valores y reglas del cuadro 4-11/Q.931. Un número en forma de una cadena de dígitos marcada debe codificarse como "0000" (desconocido). Si está puesto a "1001" (plan de numeración privado) en una llamada originada en una red de paquetes, esto indica que:

  1) la cadena de dígitos marcada no está presente en Establecimiento; y

  2) la llamada se encaminará mediante una dirección de alias en la información usuario-usuario.

Octeto N.º 3a

– Codificado según los valores y reglas del cuadro 4-11/Q.931.

"Dígitos" de número

– Cualquier número de caracteres IA5, según los formatos especificados en el plan de numeración/marcación apropiado.

NOTA – Un número E.164 estará formado solamente por los caracteres IA5 "0", "1", "2", "3", "4", "5", "6", "7", "8", "9" y "0".

Los puntos extremos H.323 no enviarán múltiples elementos de información número de la parte llamante en el mismo mensaje. Las pasarelas pueden facilitar el interfuncionamiento con los mensajes ESTABLECIMIENTO Q.931 que contienen múltiples elementos de información número de la parte llamante. Las pasarelas que faciliten ese soporte deberán establecer la correspondencia entre el primer elemento de información número de la parte llamante Q.931 y el elemento información número de la parte llamante del mensaje Establecimiento H.225.0, así como las correspondencias subsiguientes entre los elementos de información número de la parte llamante Q.931 y el campo **additionalSourceAddresses** del mensaje Establecimiento H.225.0.

7.2.2.7 Subdirección de la parte llamante

Se utiliza como en la Rec. UIT-T Q.931.

7.2.2.8 Causa

Si se recibe, se aplican las reglas definidas en la Rec. UIT-T Q.850. Obsérvese que, o bien Causa o **ReleaseCompleteReason** es obligatorio para Liberación completa; el IE Causa es facultativo en cualquier otra parte. El IE Causa y el **ReleaseCompleteReason** (motivo de liberación completa) (una parte del mensaje Liberación completa) se excluyen mutuamente. Las pasarelas establecerán una correspondencia de **ReleaseCompleteReason** al IE Causa cuando se envíe un mensaje Liberación completa del lado red con conmutación de paquetes al lado red con conmutación de circuitos (véase el cuadro 5). (No se requiere la correspondencia inversa ya que las entidades de red de paquetes tienen que decodificar el IE Causa.)

Cuadro 5/H.225.0 – Correspondencia de ReleaseCompleteReason al IE Causa

Código ReleaseCompleteReason	Valor de causa Q.931/Q.850 correspondiente
noBandwidth	34 – No hay circuito/canal disponible
gatekeeperResources	47 – Recurso no disponible, no especificado
unreachableDestination	3 – No hay ruta hacia el destino
destinationRejection	16 – Liberación normal de la llamada
invalidRevision	88 – Destino incompatible
noPermission	127 – Interfuncionamiento, no especificado
unreachableGatekeeper	38 – Red fuera de servicio
gatewayResources	42 – Congestión en el equipo de conmutación
badFormatAddress	28 – Formato de número no válido (dirección incompleta)
adaptiveBusy	41 – Fallo temporal
inConf	17 – Usuario ocupado
undefinedReason	31 – Normal, no especificado
facilityCallDeflection	16 – Liberación normal de la llamada
securityDenied	31 – Normal, no especificado
securityWrongSyncTime	31 – Normal, no especificado
securityReplay	31 – Normal, no especificado
securityWrongGeneralID	31 – Normal, no especificado
securityWrongSendersID	31 – Normal, no especificado
securityMessageIntegrityFailed	31 – Normal, no especificado
securityWrongOID	31 – Normal, no especificado
securityDHmismatch	31 – Normal, no especificado
securityCertificateExpired	31 – Normal, no especificado
securityCertificateDateInvalid	31 – Normal, no especificado
securityCertificateRevoked	31 – Normal, no especificado
securityCertificateNotReadable	31 – Normal, no especificado
securityCertificateSignatureInvalid	31 – Normal, no especificado
securityCertificateMissing	31 – Normal, no especificado
securityCertificateIncomplete	31 – Normal, no especificado
securityUnsupportedCertificateAlgOID	31 – Normal, no especificado
securityUnknownCA	31 – Normal, no especificado
calledPartyNotRegistered	20 – Abonado ausente
callerNotRegistered	31 – Normal, no especificado
newConnectionNeeded	47 – Recurso no disponible, no especificado
nonStandardReason	127 – Interfuncionamiento, no especificado
replaceWithConferenceInvite	31 – Normal, no especificado
genericDataReason	31 – Normal, no especificado
neededFeatureNotSupported	31 – Normal, no especificado
tunnelledSignallingRejected	127 – Interfuncionamiento, no especificado

Cuadro 5/H.225.0 – Correspondencia de ReleaseCompleteReason al IE Causa

Código ReleaseCompleteReason	Valor de causa Q.931/Q.850 correspondiente
InvalidCID	3 – No hay ruta hacia el destino
hopCountExceeded	3 – No hay ruta hacia el destino

Asimismo, las pasarelas establecerán una correspondencia de **AdmissionRejectReason** y **LocationRejectReason** al IE Causa cuando se envíe un mensaje Liberación completa al lado red con conmutación de circuitos tras haber recibido un **AdmissionReject** o un **LocationReject** (cuadro 6).

Cuadro 6/H.225.0 – Correspondencia de AdmissionRejectReason/ LocationRejectReason al IE Causa

Código AdmissionRejectReason o LocationRejectReason	Valor de causa Q.931/Q.850 correspondiente
calledPartyNotRegistered	20 – Abonado ausente
invalidPermission	127 – Interfuncionamiento, no especificado
requestDenied	31 – Normal, no especificado
undefinedReason	31 – Normal, no especificado
callerNotRegistered	31 – Normal, no especificado
routeCallToGatekeeper	No aplicable
invalidEndpointIdentifier	127 – Interfuncionamiento, no especificado
resourceUnavailable	47 – Recurso no disponible, no especificado
securityDenial	31 – Normal, no especificado
qosControlNotSupported	63 – Servicio u opción no disponible, no especificado
incompleteAddress	28 – Formato de número no válido (dirección incompleta)
aliasesInconsistent	31 – Normal, no especificado
routeCallToSCN	3 – No hay ruta hacia el destino
exceedsCallCapacity	41 – Fallo temporal
collectDestination	31 – Normal, no especificado
collectPIN	31 – Normal, no especificado
genericDataReason	31 – Normal, no especificado
neededFeatureNotSupported	31 – Normal, no especificado
securityWrongSyncTime	31 – Normal, no especificado
securityReplay	31 – Normal, no especificado
securityWrongGeneralID	31 – Normal, no especificado
securityWrongSendersID	31 – Normal, no especificado
securityIntegrityFailed	31 – Normal, no especificado
securityWrongOID	31 – Normal, no especificado
secuirtyDHMismatch	31 – Normal, no especificado
noRouteToDestination	3 – No hay ruta hacia el destino
unallocatedNumber	1 – Número no atribuido (no asignado)

7.2.2.9 Identificación de canal

La utilización queda en estudio; puede utilizarse para proporcionar una reacción a múltiples intentos de llamada.

7.2.2.10 Número conectado

Codificado conforme a 4.1/Q.951.5.

7.2.2.11 Subdirección conectada

Codificada conforme a 4.2/Q.951.5.

7.2.2.12 Nivel de congestión

No se utilizará.

7.2.2.13 Fecha/hora

Codificado según la figura 4-21/Q.931.

7.2.2.14 Visualización

Codificado según la figura 4-22/Q.931. La longitud máxima del elemento de información completo es 82 octetos.

7.2.2.15 Elemento de información Facilidad ampliada

Cualquier IE Facilidad ampliada utilizado para indicar una semántica sin modificaciones, tal como se define en las Recomendaciones de la serie Q.95.x, se codificará de acuerdo con 8.2.4/Q.932. En este caso, las ADU de servicio se formarán de acuerdo con ROSE [utiliza la Rec. UIT-T X.680 (Especificación de la ASN.1) y la Rec. UIT-T X.690 (Especificación de las reglas de codificación básica de la ASN.1)] como se define en la Rec. UIT-T X.229.

7.2.2.16 Facilidad

Para señalizar la redirección de llamada específica de los procedimientos H.323 (reenvío de llamada, redireccionamiento de una llamada al MC, o reencaminamiento forzado de una llamada hacia el controlador de acceso) o, en el caso de servicios suplementarios, señalización según la Rec. UIT-T H.450, se utiliza el elemento de información usuario-usuario del mensaje facilidad. Este caso particular se indicará codificando un IE Facilidad de longitud cero; es decir, el elemento de información Facilidad constará exactamente de 2 octetos, como sigue:

- Octeto N.º 1 (identificador del elemento de información) se pondrá a "00011100" ("1C'H) para indicar el IE Facilidad.
- Octeto N.º 2 (longitud del elemento de información) se pondrá a "0" para indicar que no siguen más octetos pertenecientes a este elemento de información.

Para indicar el reenvío de llamada, el IE Facilidad estará vacío y en el **UUIE Facilidad** se indicará en **dirección alternativa (alternativeAddress)** o **dirección alias alternativa (alternativeAliasAddress)** el terminal al que será redirigida la llamada. En este caso, **motivo de la facilidad (facilityReason)** se fijará en **llamada reenviada (callForwarded)**.

Para ordenar a un punto extremo que llame a un punto extremo diferente porque el punto extremo llamante desea incorporarse a una conferencia y el punto extremo llamado no tiene el MC, el IE Facilidad se podría también dejar vacío. El **ID de conferencia** indicará la conferencia a la que se ha de incorporar y el motivo en el **UUIE Facilidad** será **encaminar llamada a MC**.

Además, para ordenar al punto extremo llamante que señalice al punto extremo llamado a través del controlador de acceso del punto extremo llamado, el IE Facilidad se deja vacío. El **ID de conferencia** en el **UUIE Facilidad** indicará la conferencia a la que se ha de incorporar y el motivo en el **UUIE Facilidad** será **encaminar llamada a controlador de acceso**.

Cualquier IE Facilidad ampliada utilizado para indicar una semántica sin modificaciones, tal como se define en las Recomendaciones de la serie Q.95.x, se codificará de acuerdo a 8.2.3/Q.932. En este caso, las ADU de servicio se formarán de acuerdo con ROSE [utiliza la Rec. UIT-T X.680 (Especificación de la ASN.1) y la Rec. UIT-T X.690 (Especificación de las reglas básicas de codificación de la ASN.1)] como se define en la Rec. UIT-T X.229.

7.2.2.17 Compatibilidad de capa alta

Queda en estudio.

7.2.2.18 Facilidad de tecladillo

Codificado según la figura 4-24/Q.931. El carácter signo de admiración de cierre "!" representa una indicación de señal de gancho conmutador. Los puntos extremos que no soporten la recepción de la indicación de señal de gancho conmutador pasarán por alto el carácter "!" recibido.

7.2.2.19 Compatibilidad de capa baja

Queda en estudio.

7.2.2.20 Más datos

No se utilizará.

7.2.2.21 Facilidades específicas de la red

No se utilizará.

7.2.2.22 Indicador de notificación

Codificado según 4.5.22/Q.931.

7.2.2.23 Indicador de progresión

Codificado según la figura 4-29/Q.931 y el cuadro 4-20/Q.931.

Este elemento de información sólo se requiere para hacer de interfaz desde un terminal H.323 a un terminal basado en la RDSI y el ATM cuando hay disponible información de llamada en curso detallada. En este caso, la pasarela remitirá esta información al terminal H.323. El sistema extremo H.323 no necesita interpretar este elemento de información.

Si este elemento de información es generado por un terminal H.323, se aplican las siguientes restricciones:

Norma de codificación (octeto N.º 3, bits 6, 7)

– Indicará "UIT-T" ("00").

Ubicación

– Según el cuadro 4-20/Q.931.
– Los valores "usuario" ("0000"), "red privada que sirve al usuario local" ("0001"), y "red privada que sirve al usuario distante" ("0101") están permitidos.

Descripción de progresión

– Según el cuadro 4-20/Q.931.

7.2.2.24 Número de redireccionamiento

Se codifica según 4.6.7/Q.931. Obsérvese que este elemento de información se proporciona con la exclusiva finalidad de facilitar el interfuncionamiento con la RCC, y no con la finalidad de proporcionar un mecanismo para servicios de desviación de llamada basados en H.323. Los servicios de desviación de llamada se definen en la Rec. UIT-T H.450.3.

7.2.2.25 Indicador de repetición

No se utilizará.

7.2.2.26 Indicador de rearranque

No se utilizará.

7.2.2.27 Mensaje segmentado

No se utilizará. Adviértase que ni en la Rec. UIT-T H.323 ni en la presente Rec. se impone un límite superior crítico al tamaño de mensaje.

7.2.2.28 Envío completo

Codificado según la figura 4-33/Q.931.

No se aplican restricciones.

7.2.2.29 Señal

Codificado según la figura 4-34/Q.931 y el cuadro 4-24/Q.931.

No se aplican restricciones.

7.2.2.30 Selección de la red de tránsito

No se utilizará.

7.2.2.31 Usuario-usuario

Codificado según la figura 4-36/Q.931 y el cuadro 4-26/Q.931, con las modificaciones introducidas en la presente Recomendación.

El elemento de información Usuario-usuario será utilizado por todas las entidades H.323 para transportar información relacionada con H.323. La información usuario-usuario efectiva a intercambiar solamente entre los terminales participantes está anidada en el campo **user-data** de la PDU **H323-UserInformation** (a la cual no se aplican restricciones).

Se aplican las siguientes restricciones:

Longitud de contenido de usuario-usuario

– Será 2 octetos en vez de 1 (como se indica en la figura 4-36/Q.931).

Discriminador de protocolo

– Indicará información de usuario codificada (ASN.1) ("00000101") de las Recomendaciones UIT-T X.680 y X.690.

  NOTA – Esto se ha tomado de la revisión 1998 de la Rec. UIT-T Q.931, que hace referencia a las anteriores revisiones de ASN.1. Las referencias correctas a ASN.1 son las Recomendaciones UIT-T X.680 (sintaxis) y X.691 (PER).

Información de usuario

– Contendrá una estructura ASN.1 **(H323-UserInformation)** que, además de la información pertinente H.323, incluya los datos de usuario efectivos, como sigue. La ASN.1 se codifica utilizando la variante alineada básica de las reglas de codificación compactada especificadas en la Rec. UIT-T X.691.

La estructura **H323-UserInformation** contiene los campos **h323-uu-pdu** y **user-data**.

El campo **h323-uu-pdu** de la estructura **H323-UserInformation** contiene los campos que se indican más adelante. Obsérvese que no todos los campos de **h323-uu-pdu** están permitidos en todos los mensajes. Para las restricciones, véase la descripción de cada uno de los mensajes.

– **h323-message-body (cuerpo de mensaje h323)** – Este campo contiene información específica de un determinado mensaje de señalización de llamada H.225.0, descrito en 7.3 y 7.4. Un emisor puede seleccionar una opción **empty (vacío)** si no hay necesidad de enviar el campo UUIE **(Facility-UUIE**, etc.**)** en un mensaje dado, como en el caso en que se usa un mensaje Facilidad para transportar información no asociada a la llamada. Obsérvese que, a partir de la versión 4 de esta Recomendación, si un mensaje está asociado a una determinada llamada, el emisor incluirá el campo UUIE. Esto es necesario para proporcionar el campo **callIdentifier**.

– **nonStandardData (datos no normalizados)** – Este campo transporta información no definida en esta Recomendación (por ejemplos datos de particulares).

– **h4501SupplementaryService (servicio suplementario h4501)** – Este campo transporta una secuencia de APDUs H4501SupplementaryService definida en el cuadro 3/H.450.1.

– **h245Tunnelling (tunelización h245)** – Este elemento se fija a VERDADERO si la tunelización de mensajes H.245 está habilitada. Los sistemas conformes con H.225.0 versión 4 o más alta fijarán este elemento a VERDADERO si se utiliza el procedimiento de conexión rápida para establecer la comunicación.

– **h245Control (control h245)** – Este campo transporta una secuencia de PDU H.245 tunelizadas. Cada cadena de octetos contiene exactamente una PDU H.245.

– **nonStandardControl (control no normalizado)** – Este campo contiene información de control no definida en esta Recomendación (por ejemplo, información de control de particulares).

– **callLinkage (vinculación de llamada)** – El contenido de este campo es controlado por lo general por un servicio de vinculación de llamada. Para los procedimientos y semántica de este campo, véase la Rec. UIT-T H.323.

– **tunnelledSignallingMessage (mensaje de señalización tunelizado)** – Es un mensaje de señalización completo tunelizado, en su formato nativo, para el soporte de señalización de control de llamada de extremo a extremo adicional. El campo **tunnelledProtocolID** identifica el protocolo que está siendo tunelizado. El campo **messageContent (contenido de mensaje)** es una secuencia de mensajes completos reales en su formato binario nativo; esto permite la agregación de mensajes tunelizados en un solo mensaje H.225.0. Si el campo **tunnellingRequired (tunelización requerida)** está presente, la llamada proseguirá solamente si se soporta tunelización.

– **provisionalRespToH245Tunnelling (respuesta provisional a tunelización H245)** – Esta bandera se utiliza para señalar que la entidad llamada todavía no ha decidido si la tunelización es aplicable a esta llamada. Si está presente, la entidad receptora no tendrá en cuenta la bandera **h245Tunnelling**.

– **stimulusControl (control de estímulo)** – Este campo se reserva para su utilización futura por el UIT-T en un protocolo basado en el estímulo.

– **genericData (datos genéricos)** – Este campo es una lista de elementos genéricos relacionados con características que están definidas fuera de la especificación H.225.0 de base. Estos parámetros pueden utilizarse, por ejemplo, para tunelizar información transparentemente a través de H.225.0.

El campo **user-data (datos de usuarios)** de la estructura **H323-UserInformation** contiene los campos siguientes:

– **protocol-discriminator (discriminador de protocolo)** – Para codificar este campo se debe aplicar el cuadro 4-26/Q.931.

– **user-information (información de usuario)** – Para codificar este campo se se debe aplicar 4.5.30/Q.931.

7.3 Detalles de un mensaje de señalización de llamada H.225.0 basado en Q.931

Obsérvese que las longitudes de los elementos de información especificados en los cuadros que siguen no se refieren a mensajes que son generados únicamente por terminales H.323. Se tiene entendido que el tamaño mostrado del elemento de información usuario-usuario es el tamaño de la estructura **user-data** en **H323-UserInformation** y no incluye **h323-UU-PDU**. El tamaño total de **H323-UserInformation** está limitado a 65 536 octetos. Independientemente de los tamaños especificados, los mensajes reenviados desde el lado RCC pueden tener diferentes tamaños (mayores).

Obsérvese también que un elemento de información especificado más abajo como obligatorio, facultativo o prohibido, sólo indica si los terminales H.323 pueden o no originar dicho elemento de información.

7.3.1 Aviso

Este mensaje puede ser enviado por el usuario llamado para indicar que se ha iniciado el aviso del usuario llamado. En lenguaje corriente, "el teléfono está sonando".

Debe aplicarse el cuadro 3-2/Q.931 (versión 1998) con las modificaciones del cuadro 7.

Cuadro 7/H.225.0 – Aviso

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Capacidad portadora	O	5-6
Facilidad ampliada	O	8-*
Identificación de canal	En estudio	No aplicable
Facilidad	O	8-*
Indicador de progresión	O	2-4
Indicador de notificación	O	2-*
Visualización	O	2-82
Señal	O	2-3
Compatibilidad de capa alta	En estudio	No aplicable
Usuario-usuario	M	2-131

El elemento de información usuario-usuario contiene el UUIE Aviso definido en la sintaxis de mensaje H.225.0. **UUIE Aviso** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

destinationInfo (información de destino) – Contiene un **EndpointType** (**tipo de punto extremo**) para permitir al llamante determinar si en la llamada interviene o no una pasarela.

h245Address (dirección h245) – Es una dirección de transporte específica en la cual el punto extremo llamado o el controlador de acceso que trata la llamada desearía establecer señalización H.245. Esta dirección se enviará en los mensajes Llamada en curso, Progresión o Conexión.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

h245SecurityMode (modo de seguridad h245) – Una entidad H.323 que recibe un mensaje Establecimiento con el conjunto **h245SecurityCapability (capacidad de seguridad h245)** responderá con el correspondiente **h245SecurityMode** aceptable en un mensaje Llamada en curso, Aviso, Progresión o Conexión.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

fastStart (arranque rápido) – Utilizado únicamente en el procedimiento de conexión rápida, **fastStart** soporta la señalización necesaria para abrir un canal lógico. Utiliza la estructura **canal lógico abierto (OpenLogicalChannel)** definida en la Rec. UIT-T H.245, pero el emisor indica los modos en que prefiere recibir y transmitir, y las direcciones de transporte en las que espera recibir trenes de medios.

multipleCalls (múltiples llamadas) – Si es VERDADERO indica que el emisor del mensaje puede señalizar múltiples llamadas a través de una sola conexión de señalización de llamadas.

maintainConnection (mantener la conexión) – Si es VERDADERO indica que el emisor del mensaje puede soportar una conexión de señalización cuando ninguna llamada está actualmente señalizada en la conexión.

alertingAddress (dirección de aviso) – Contiene las direcciones de alias para la parte que avisa.

presentationIndicator (indicador de presentación) – Indica si se debe permitir o restringir la presentación de la **alertingAddress**.

screeningIndicator (indicador de cribado) – Indica si el punto extremo o la red (controlador de acceso) suministró la **alertingAddress**, y si ésta fue verificada por un controlador de acceso.

fastConnectRefused (conexión rápida rechazada) – Cuando un punto extremo establece una comunicación, debe retornar este elemento en cualquier mensaje, hasta el mensaje de conexión inclusive, para indicar que rechaza el procedimiento de conexión rápida.

serviceControl (control de servicio) – Contiene datos específicos de servicio, o referencia a los mismos, que pueden ser utilizados como parte del procedimiento de establecimiento por el punto extremo llamante (por ejemplo, un menú de opciones para desviación de llamada) como se describe, por ejemplo, en el anexo K/H.323.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor en un instante dado, suponiendo que este mensaje Aviso representa una llamada activa. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity (capacidad de la llamada actual)**.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

7.3.2 Llamada en curso

Este mensaje puede ser enviado por el usuario llamado para indicar que se ha iniciado el establecimiento de la comunicación solicitado y que no se aceptará más ninguna información de establecimiento de la comunicación. Véase el cuadro 8.

Cuadro 8/H.225.0 – Llamada en curso

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Capacidad portadora	O	5-6
Facilidad ampliada	O	8-*
Identificación de canal	En estudio	No aplicable
Facilidad	O	8-*
Indicador de progresión	O	2-4
Indicador de notificación	O	2-*
Visualización	O	2-82
Compatibilidad de capa alta	En estudio	No aplicable
Usuario-usuario	M	2-131

El elemento de información usuario-usuario contiene el **UUIE Llamada en curso** definido en la sintaxis de mensaje H.225.0. **UUIE Llamada en curso** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

destinationInfo (información de destino) – Contiene un **EndpointType** para permitir al llamante determinar si en la llamada interviene o no una pasarela.

h245Address (dirección h245) – Es una dirección de transporte específica en la cual el punto extremo llamado o el controlador de acceso que trata la llamada desearía establecer señalización H.245.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada, utilizada en esta Recomendación.

h245SecurityMode (modo de seguridad h245) – Una entidad H.323 que recibe un mensaje Establecimiento con el conjunto **h245SecurityCapability** responderá con el correspondiente **h245SecurityMode** aceptable en un mensaje Llamada en curso, Aviso, Progresión o Conexión.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

fastStart (arranque rápido) – Utilizado únicamente en el procedimiento de conexión rápida, **fastStart** soporta la señalización necesaria para abrir un canal lógico. Utiliza la estructura **OpenLogicalChannel** definida en la Rec. UIT-T H.245, pero el emisor indica los modos en que prefiere recibir y transmitir, y las direcciones de transporte en las que espera recibir trenes de medios.

multipleCalls (múltiples llamadas) – Si es VERDADERO indica que el emisor del mensaje puede señalizar múltiples llamadas a través de una sola conexión de señalización de llamadas.

maintainConnection (mantener la conexión) – Si es VERDADERO indica que el emisor del mensaje puede soportar una conexión de señalización cuando actualmente no está señalizada ninguna llamada en la conexión.

fastConnectRefused (conexión rápida rechazada) – Cuando un punto extremo establece una comunicación, debe retornar este elemento en cualquier mensaje, hasta el mensaje de conexión inclusive, para indicar que rechaza el procedimiento de conexión rápida.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

7.3.3 Conexión

Este mensaje será enviado por la entidad llamada a la entidad llamante (controlador de acceso, pasarela o terminal llamante) para indicar aceptación de la llamada por la entidad llamada. Se debe aplicar el cuadro 3-4/Q.931 con las modificaciones del cuadro 9.

Cuadro 9/H.225.0 – Conexión

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Capacidad portadora	O	5-6
Facilidad ampliada	O	8-*
Identificación de canal	En estudio	No aplicable
Facilidad	O	8-*
Indicador de progresión	O	2-4
Indicador de notificación	O	2-*
Visualización	O	2-82
Fecha/hora	O	8
Número conectado	O	2-*
Subdirección conectada	O	2-23
Compatibilidad de capa baja	En estudio	No aplicable
Compatibilidad de capa alta	En estudio	No aplicable
Usuario-usuario	M	2-131

El elemento de información usuario-usuario contiene el **UUIE Conexión** definido en la sintaxis de mensaje H.225.0. **UUIE Conexión** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

h245Address (dirección h245) – Es una dirección de transporte específica en la cual el punto extremo llamado o el controlador de acceso que trata la llamada desearía establecer señalización H.245. Esta dirección se enviará si se envió antes en un mensaje Aviso, Progresión, o Llamada en curso.

destinationInfo (información de destino) – Contiene un **EndpointType** para permitir al llamante determinar si en la llamada interviene o no una pasarela.

conferenceID (ID de conferencia) – Contendrá un número exclusivo para permitir a la conferencia identificarse inequívocamente de las otras recibidas en el mensaje Establecimiento.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada, utilizada en esta Recomendación.

h245SecurityMode (modo de seguridad h245) – Una entidad H.323 que recibe un mensaje Establecimiento con el conjunto **h245SecurityCapability** responderá con el correspondiente **h245SecurityMode** aceptable en un mensaje Llamada en curso, Aviso, Progresión o Conexión.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

fastStart (arranque rápido) – Utilizado únicamente en el procedimiento de conexión rápida, **fastStart** soporta la señalización necesaria para abrir un canal lógico. Utiliza la estructura **OpenLogicalChannel** definida en la Rec. UIT-T H.245, pero el emisor indica los modos en que prefiere recibir y transmitir, y las direcciones de transporte en las que espera recibir trenes de medios.

multipleCalls (múltiples llamadas) – Si es VERDADERO indica que el emisor del mensaje puede señalizar múltiples llamadas a través de una sola conexión de señalización de llamadas.

maintainConnection (mantener la conexión) – Si es VERDADERO indica que el emisor del mensaje puede soportar una conexión de señalización cuando no hay llamadas actualmente señalizadas en la conexión.

language (idioma) – Indica el o los idiomas en que el usuario prefiere recibir anuncios y avisos. El campo contiene uno o más rótulos de lenguaje que satisfacen la norma RFC 1766.

connectedAddress (dirección conectada) – Contiene las direcciones de alias para la parte conectada (que responde); la cadena de dígitos marcada de la parte conectada está en el elemento de información Número conectado.

presentationIndicator (indicador de presentación) – Indica si se debe permitir o restringir la presentación de la **connectedAddress**. Si tanto el **presentationIndicator** como el indicador de presentación del IE número conectado están en conflicto, se utilizará el indicador de presentación del IE número conectado.

screeningIndicator (indicador de cribado) – Indica si el punto extremo o la red (controlador de acceso) suministró la **connectedAddress**, y si esta dirección fue verificada por un controlador de acceso. Si tanto el **screeningIndicator** como el indicador de cribado del IE número conectado están presentes y en conflicto, se utilizará el indicador de cribado del IE número conectado.

fastConnectRefused (conexión rápida rechazada) – Cuando un punto extremo establece una comunicación, debe retornar este elemento en cualquier mensaje, hasta el mensaje de conexión inclusive, para indicar que rechaza el procedimiento de conexión rápida.

serviceControl (control de servicio) – Contiene datos específicos de servicio, o referencia a los mismos, que podrán ser utilizados por un punto extremo o pasarela (por ejemplo, para la presentación visual de un menú de opciones a un usuario llamante) como se describe, por ejemplo, en el anexo K/H.323.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor en un instante dado, suponiendo que este mensaje Conexión representa una llamada activa. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity**.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

7.3.4 Acuse de conexión

Este mensaje no será enviado.

7.3.5 Desconexión

Este mensaje no será enviado por una entidad H.323.

El contenido y la semántica de un mensaje Desconexión recibido de la red se definen en el cuadro 3-6/Q.931 y en 10.5 de ISO/CEI 11582.

7.3.6 Información

Este mensaje puede enviarse para proporcionar información adicional. Puede utilizarse para proporcionar información para el establecimiento de la comunicación (por ejemplo, envío con superposición) o informaciones diversas relacionadas con la llamada. Puede utilizarse para entregar características privadas.

Este mensaje puede enviarlo una entidad H.323.

Este mensaje satisface el cuadro 3-7/Q.931 con las modificaciones que se muestran en el cuadro 10.

Cuadro 10/H.225.0 – Contenido del mensaje Información

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Envío completo	O	1
Visualización	O	2-82
Facilidad de tecladillo	O	2-34
Señal	O	2-3
Número de la parte llamada	O (nota)	2-35
Usuario-usuario	M	2-131
NOTA – Se utilizará el IE Número de la parte llamada para transportar números de un plan de numeración privado cuando se realice un envío superpuesto conforme con 8.1.12/H.323.		

El elemento de información usuario-usuario contiene el **Information-UUIE** definido en la sintaxis de mensaje H.225.0. El **Information-UUIE** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 utilizada en la presente Recomendación.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

fastStart (arranque rápido) – Este campo no será incluido, y será ignorado en recepción.

fastConnectRefused (conexión rápida rechazada) – Este campo no será incluido, y será ignorado en recepción.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos RCC utilizados en la llamada.

7.3.7 Progresión

Este mensaje puede ser enviado por una pasarela H.323 para indicar la progresión de una llamada en caso de interfuncionamiento con RCC. También puede ser enviado por un punto extremo H.323 antes del mensaje Conexión, lo que dependerá de la interacción del servicio suplementario.

Se debe aplicar el cuadro 3-9/Q.931 y 10.10 de ISO/CEI 11502 con las siguientes modificaciones, en el cuadro 11.

Cuadro 11/H.225.0 – Progresión

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Capacidad portadora	O	5-6
Causa	O	2-32
Facilidad ampliada	O	8-*
Identificación de canal	En estudio	No aplicable
Facilidad	O	8-*
Indicador de progresión	M	2-4
Indicador de notificación	O	2-*
Visualización	O	2-82
Compatibilidad de capa alta	En estudio	No aplicable
Usuario-usuario	M	2-131

El elemento de información usuario-usuario contiene el **UUIE Progresión** definido en la sintaxis de mensaje H.225.0. El **UUIE Progresión** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

destinationInfo (información de destino) – Contiene un **EndpointType** para permitir al llamante determinar si en la llamada interviene o no una pasarela.

h245Address (dirección h245) – Es una dirección de transporte específica en la cual el punto extremo llamado o el controlador de acceso que trata la llamada desearía establecer señalización H.245. Esta dirección se enviará si se envió antes en los mensajes Llamada en curso, Aviso o Conexión.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

h245SecurityMode (modo de seguridad h245) – Una entidad H.323 que recibe un mensaje Establecimiento con el conjunto **h245SecurityCapability** responderá con el correspondiente **h245SecurityMode** aceptable en un mensaje Llamada en curso, Aviso, Progresión o Conexión.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

fastStart (arranque rápido) – Utilizado únicamente en el procedimiento de conexión rápida, **fastStart** soporta la señalización necesaria para abrir un canal lógico. Utiliza la estructura **OpenLogicalChannel** definida en la Rec. UIT-T H.245, pero el emisor indica los modos en que prefiere recibir y transmitir, y las direcciones de transporte en las que espera recibir trenes de medios.

multipleCalls (múltiples llamadas) – Si es VERDADERO indica que el emisor del mensaje puede señalizar múltiples llamadas a través de una sola conexión de señalización de llamadas.

maintainConnection (mantener la conexión) – Si es VERDADERA indica que el emisor del mensaje puede soportar una conexión de señalización cuando no hay llamadas actualmente señalizadas en la conexión.

fastConnectRefused (conexión rápida rechazada) – Cuando un punto extremo establece una comunicación, debe retornar este elemento en cualquier mensaje, hasta el mensaje de conexión inclusive, para indicar que rechaza el procedimiento de conexión rápida.

7.3.8 Liberación

Este mensaje no será enviado por una entidad H.323.

El contenido y la semántica de un mensaje Liberación recibido de la red se definen en el cuadro 3-10/Q.931 y en 10.5 de ISO/CEI 11582.

7.3.9 Liberación completa

Este mensaje será enviado por un terminal para indicar liberación de la llamada. Después, el valor de referencia de llamada (CRV, *call reference value*) está disponible para su reutilización.

La secuencia desconexión/liberación/liberación completa no se utiliza, ya que su objetivo principal es indicar la conclusión de la liberación de los recursos de red con conmutación de circuitos. Como esto no se aplica al entorno de la red de paquetes, se utiliza el método del paso único de enviar sólo liberación completa.

Se debe aplicar el cuadro 3-11/Q.931 con las modificaciones del cuadro 12.

Cuadro 12/H.225.0 – Liberación completa

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Causa	CM (nota)	2-32
Facilidad	O	8-*
Indicador de notificación	O	2-*
Visualización	O	2-82
Señal	O	2-3
Usuario-usuario	M	2-131
NOTA – Estará presente el IE Causa o la **ReleaseCompleteReason**.		

Si este mensaje se envía en respuesta a un mensaje Facilidad con un IE Facilidad vacío, la **ReleaseCompleteReason** se fijará a **facilityCallDeflection**.

Si este mensaje lo reenvía una pasarela desde una RCC, el valor de causa se fijará como se especifica en la Rec. UIT-T Q.931.

El elemento de información usuario-usuario contiene el **UUIE Liberación completa** definido en la sintaxis de mensaje H.225.0. El **UUIE Liberación completa** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

reason (motivo) – Más información sobre la razón (o motivo) por el cual se liberó la llamada. El motivo **genericDataReason** indica que la llamada se liberó como resultado de un elemento o de una característica genéricos; en este caso se puede especificar información adicional en el campo **genericData** de la **h323-uu-pdu** de este mensaje. El motivo **neededFeatureNotSupported** indica que una característica requerida por una entidad no está soportada por otra. El motivo **tunnelledSignallingRejected** se envía cuando la llamada se libera porque el emisor no permite la tunelización de señalización que no sea H.323 y se requiere tunelización para el establecimiento exitoso de la comunicación. El motivo **hopCountExceeded** indica el rechazo de la llamada porque el valor **hopCount** ha llegado a 0 y, por consiguiente, la llamada no puede seguir adelante.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada, utilizada en esta Recomendación.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

busyAddress (dirección ocupada) – Contiene las direcciones de alias para la parte ocupada.

presentationIndicator – Indica si se debe permitir o restringir la presentación de la **busyAddress**.

screeningIndicator (indicador de cribado) – Indica si el punto extremo o la red (controlador de acceso) suministró la **busyAddress**, y si ésta fue cribada por un controlador de acceso.

capacity (capacidad) – Indica la capacidad de llamada disponible del punto extremo emisor después de que la llamada referenciada en este mensaje de Liberación completa ha sido liberada. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity**.

serviceControl (control de servicio) – Contiene datos específicos de servicio, o referencia a los mismos, para servicios posteriores a la llamada (por ejemplo, un mensaje de error o un anuncio) como se describe, por ejemplo, en el anexo K/H.323.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

7.3.10 Establecimiento

Este mensaje será enviado por una entidad H.323 llamante para indicar su deseo de establecer una conexión a la entidad llamada.

Se debe aplicar el cuadro 3-15/Q.931 con las modificaciones del cuadro 13.

Cuadro 13/H.225.0 – Establecimiento

Elemento de información	Estado H.225.0 (M/F/O/CM)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M (nota 2)	3
Tipo de mensaje	M	1
Envío completo	O	1
Indicador de repetición	F	No aplicable
Capacidad portadora	M	5-6
Facilidad ampliada	O	8-*
Identificación de canal	En estudio	No aplicable

Cuadro 13/H.225.0 – Establecimiento

Elemento de información	Estado H.225.0 (M/F/O/CM)	Longitud en H.225.0
Facilidad	O	8-*
Indicador de progresión	O	2-4
Facilidades específicas de la red	F	No aplicable
Indicador de notificación	O	2-*
Visualización	O	2-82
Facilidad de tecladillo	O	2-34
Señal	O	2-3
Número de la parte llamante	O	2-131
Subdirección de la parte llamante	CM (nota 1)	No aplicable
Número de la parte llamada	O	2-131
Subdirección de la parte llamada	CM (nota 1)	No aplicable
Número de redireccionamiento	O	2-*
Selección de red de tránsito	F	No aplicable
Compatibilidad de capa baja	En estudio	No aplicable
Compatibilidad de capa alta	En estudio	No aplicable
Usuario-usuario	M	2-131
NOTA 1 – Las subdirecciones se necesitan para algunos casos de escenarios de llamadas RCC; no deben utilizarse para llamadas del lado red de paquetes, solamente. NOTA 2 – Si se envió previamente un ARQ, el CRV utilizado aquí será el mismo.		

El elemento de información usuario-usuario contiene el **UUIE Establecimiento** definido en la sintaxis de mensaje H.225.0. El **UUIE Establecimiento** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

h245Address (dirección h245) – Es una dirección de transporte específica en la cual el punto extremo llamante o controlador de acceso que trata la llamada desearían establecer la señalización H.245. Sólo debe ser proporcionada por el emisor si es capaz de tratar los procedimientos H.245 antes de recibir un mensaje Conexión por el canal de señalización de llamada.

sourceAddress (dirección de origen) – Contiene las direcciones de alias del origen. La dirección primaria será la primera. Se señala que el número E.164 del origen, si existe, estará contenido en el IE número de la parte llamante.

sourceInfo (información de origen) – Contiene un **EndpointType** para que la parte llamada pueda determinar si la llamada comprende o no una pasarela.

destinationAddress (dirección de destino) – Es la dirección a la que el punto extremo desea conectarse. La dirección primaria será la primera. Cuando se llama a un punto extremo utilizando solamente una cadena de dígitos marcada, esta dirección se colocará en el IE número de la parte llamada en el mensaje de señalización de llamada H.225.0. La **dirección de destino**, si está disponible, será incluida en el mensaje Establecimiento por los terminales conformes con la versión 2 o con una versión ulterior de esta Recomendación.

destCallSignalAddress (dirección de señalización de llamada de destino) – Es necesario para informar al controlador de acceso de la dirección de transporte de señalización de llamada del

terminal de destino; es redundante en el caso de terminal a terminal, directo. En todos los casos en que la información esté a disposición del emisor del mensaje Establecimiento, se rellenará este campo.

destExtraCallInfo (información de llamada suplementaria de destino) – Necesario para efectuar posibles llamadas por canal adicional, es decir, para una llamada 2×64 kbit/s en el lado RCC. Sólo contendrá cadenas de dígitos marcadas, números E.l64 o números privados, y no contendrá el número del canal inicial (véase la nota).

destExtraCRV (CRV suplementario de destino) – CRV para las llamadas RCC adicionales especificados por **destExtraCallInfo**. Su uso queda en estudio. Estos valores pueden emplearse para asociar señalización RAS con la señalización Q.931 utilizada en esta Recomendación.

activeMC (MC activo) – Indica que el punto extremo llamante está bajo la influencia de un MC activo.

conferenceID (ID de conferencia) – Identificador de conferencia único.

conferenceGoal (objetivo de la conferencia):

- **create (crear)** – Comenzar una nueva conferencia;
- **invite (invitar)** – Invitar a una parte a una conferencia existente;
- **join (incorporar)** – Incorporarse a una conferencia existente;
- **capability-negotiation (negociación de capacidad)** – Negociar capacidades para una ulterior conferencia con acoplamiento menos estricto.
- **callIndependentSupplementaryService (servicios suplementarios independientes de la llamada)** – Transporte de las APDU de servicios suplementarios de una manera no relacionada con la llamada.

callServices (servicios de llamada) – Proporciona información sobre el soporte de protocolos facultativos de la serie Q para el controlador de acceso y el terminal llamado.

callType (tipo de llamada) – Mediante este valor, el controlador de acceso de la parte llamada puede tratar de determinar la utilización de anchura de banda "real". El valor por defecto es **pointToPoint** para todas las llamadas; se debe reconocer que el tipo de llamada puede cambiar dinámicamente durante la llamada, y que el tipo de llamada final puede no ser conocido cuando se envía el mensaje Establecimiento.

sourceCallSignalAddress (dirección de señalización de llamada de origen) – Contiene la dirección de transporte para la llamada de origen; este valor será utilizado en el mensaje ARQ por el receptor del mensaje Establecimiento. En todos los casos en que la información esté a disposición del emisor del mensaje Establecimiento, se rellenará este campo. El valor de **sourceCallSignalAddress** será igual al valor que fue utilizado en la ARQ por el emisor del mensaje Establecimiento, y será transmitido en eco por el punto extremo que recibe el mensaje Establecimiento en su ARQ.

remoteExtensionAddress (dirección de extensión distante) – Contiene la dirección de alias de un punto extremo llamado en los casos en que esta información es necesaria para atravesar múltiples pasarelas. En todos los casos en que la información esté a disposición del emisor del mensaje Establecimiento, se rellenará este campo.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada, utilizada en esta Recomendación.

h245SecurityCapability (capacidad de seguridad h245) – Conjunto de capacidades que puede utilizar el emisor para asegurar el canal H.245.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

fastStart (arranque rápido) – Utilizado únicamente en el procedimiento de conexión rápida, **fastStart** soporta la señalización necesaria para abrir un canal lógico. Utiliza la estructura **OpenLogicalChannel** definida en la Rec. UIT-T H.245, pero el emisor indica los modos en que prefiere recibir y transmitir, y las direcciones de transporte en las que espera recibir trenes de medios.

mediaWaitForConnect (medios esperan conexión) – Si es VERDADERO, indica que el recibiente del mensaje Establecimiento no transmitirá medios hasta que se haya enviado el mensaje Conexión.

canOverlapSend (puede enviar con superposición) – Si es VERDADERO, indica que el emisor del mensaje Establecimiento soporta el envío con superposición.

endpointIdentifier (identificador de punto extremo) – Es un identificador de punto extremo que fue asignado al terminal en el mensaje RCF. Este campo se presentará cuando se envía Establecimiento al controlador de acceso en el que está registrado el punto extremo, y no estará presente cuando el mensaje Establecimiento se envía a otra entidad.

multipleCalls (múltiples llamadas) – Si es VERDADERO, indica que el emisor del mensaje puede señalizar múltiples llamadas a través de una sola conexión de señalización de llamadas.

maintainConnection (mantener conexión) – Si es VERDADERO, indica que el emisor del mensaje puede soportar una conexión de señalización cuando no hay llamadas actualmente señalizadas en la conexión.

ConnectionParameters (parámetros de conexión) – Permite la especificación de parámetros que son requeridos por pasarelas que proporcionan múltiples tipos de conexión y/o agregación (por ejemplo, una pasarela H.323/H.320):

- **scnConnectionType (tipo de conexión rcc)** – Proporciona información a una pasarela sobre el tipo de conexión particular utilizada para producir la llamada RCC completa. Los puntos extremos o controladores de acceso rellenarán este campo si tienen a su disposición la información pertinente. Si se indica la opción "multivelocidad", el octeto de velocidad de transferencia de información en la capacidad portadora también deberá indicar "multivelocidad" y el octeto multiplicador de velocidad indicará el número de conexiones. En todos los otros casos, si el campo **scnConnectionType** está presente, prevalece sobre cualquier indicación referente al tipo de conexión individual contenida en la velocidad de transferencia (octeto #4) y en el multiplicador de velocidad (octeto #4.1) del IE capacidad portadora.
- **numberOfSCNConnections (número de conexiones RCC)** – Indica el número de conexiones del tipo **scnConnectionType** que son agregadas conjuntamente para producir la llamada RCC. Este campo, cuando se multiplica por la anchura de banda de la conexión particular especificada en **scnConnectionType**, da la anchura de banda para toda la llamada en la RCC. Los puntos extremos o controladores de acceso rellenarán este campo si disponen de la información pertinente. Se debe señalar que si el campo **scnConnectionType** está fijado a desconocido, se supone una unidad de anchura de banda de 64 kbit/s. Si tanto este campo como los campos **scnConnectionType** están presentes, la anchura de banda total indicada estará en conformidad con la anchura de banda RCC total indicada por la velocidad de transferencia (octeto #4) y el multiplicador de velocidad (octeto #4.1) del IE capacidad portadora.
- **scnConnectionAggregation (agregación de conexión rcc)** – Indica cómo las conexiones particulares son agregadas conjuntamente para producir la llamada RCC completa. Los

puntos extremos o controladores de acceso rellenarán este campo si disponen de la información pertinente. La opción por defecto que se utilizará cuando el mecanismo real de agregación es desconocido, es "auto". Cuando se sabe que se utiliza ligamiento, pero se desconoce el modo preciso de ligamiento, se utilizará la opción "modo de ligamiento 1".

language (idioma) – Indica el o los idiomas en que el usuario prefiere recibir anuncios y avisos. El campo contiene uno o más rótulos de idioma que satisfacen la norma RFC 1766.

presentationIndicator (indicador de presentación) – Indica si se permite o restringe la presentación del campo **sourceAddress**. Si el **presentationIndicator** y el indicador de presentación del IE número de parte llamante están presentes y en conflicto, se utilizará el indicador de presentación del IE número de parte llamante.

screeningIndicator (indicador de cribado) – Indica si el punto extremo o red (controlador de acceso) proporciona el campo **sourceAddress**, y si este campo fue cribado por un controlador de acceso. Si tanto el **screeningIndicator** como el indicador de cribado del IE número de parte llamante están presentes y en conflicto, se utilizará el indicador de cribado del IE número de parte llamante.

serviceControl (control de servicio) – Contiene datos específicos de servicio, o referencia a los mismos, que pueden ser utilizados como parte del procedimiento de establecimiento en el punto extremo llamante (por ejemplo, por ejemplo una imagen o icono para visualización en un aviso) como se describe, por ejemplo, en el anexo K/H.323.

symmetricOperationRequired (operación simétrica requerida) – Si está presente, indica que el punto extremo llamado tiene que seleccionar capacidades de audio idénticas en transmisión y recepción. Este elemento no se incluirá a menos que también se haya incluido el elemento **fastStart**.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor en un instante dado, suponiendo que este mensaje Establecimiento representa una llamada activa. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity**.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos RCC utilizados en la llamada.

desiredProtocols (protocolos deseados) – Identifica el tipo de protocolos, por orden de preferencia, que el punto extremo desea para su llamada (por ejemplo voz y fax). Una entidad de resolución puede utilizar este campo para localizar un punto extremo que también soporta el protocolo, teniendo en cuenta el orden de preferencia.

neededFeatures (características requeridas) – Este campo especifica una lista de características genéricas requeridas para que la llamada tenga éxito.

desiredFeatures (características deseadas) – Este campo especifica una lista de características genéricas que son preferidas para la llamada, pero que no son indispensables para que la llamada tenga éxito.

supportedFeatures (características soportadas) – Este campo especifica una lista de características genéricas que el emisor soporta y ha optado por declarar.

parallelH245Control (control H245 paralelo) – Este campo transporta una secuencia de PDU tunelizadas del conjunto de capacidades de terminal H.245 y, facultativamente, las PDU de determinación de director/subordinado. Cada cadena de octetos contendrá exactamente una PDU H.245.

additionalSourceAddresses (direcciones de origen adicionales) – Este campo lleva una secuencia de direcciones de alias que corresponde al segundo elemento de información y elementos de información subsiguientes número de la parte llamante en una red no H.323. Por ejemplo, en la RDSI, pueden estar presentes múltiples números de la parte llamante para soportar la "Opción de

entrega de dos elementos de información número de la parte llamante" definida en el anexo A/Q.951.

hopCount (recuento de saltos) – Este campo especifica un valor entero para indicar el número de saltos que puede alcanzar la señalización de llamada.

NOTA – Si está presente **destExtraCallInfo (información de llamada suplementaria de destino)**, se puede suministrar un CRV para cada llamada, en **destExtraCRV**. Estos CRV se utilizarán para identificar cualquier respuesta a cada llamada iniciada. Estos procedimientos quedan en estudio. Si el campo **destExtraCRV** no está presente, una pasarela agregará toda la información de llamada en una única respuesta, de manera que, si una llamada fracasa en el lado RCC, la llamada completa es tratada como una llamada fracasada.

7.3.11 Acuse de establecimiento

Este mensaje puede ser enviado por una entidad H.323. Sin embargo, puede ser reenviado desde la red a través de una pasarela. Su procesamiento en recepción es facultativo, pero una entidad que indique **canOverlapSend** en el mensaje Establecimiento deberá soportar Acuse de establecimiento.

El contenido y la semántica de un mensaje de Acuse de establecimiento recibido de la red se definen en el cuadro 3-16/Q.931, con las modificaciones que aparecen en el cuadro 14.

Cuadro 14/H.225.0 – Acuse de establecimiento

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Identificación de canal	En estudio	No aplicable
Visualización	O	2-82
Usuario-usuario	M	2-131

Con miras a la retrocompatibilidad con sistemas anteriores a la versión 4 de H.225.0, el emisor de este mensaje no incluirá el campo **h4501SupplementaryService** ni el campo **h245Control** en el campo **h323-message-body** del elemento de información usuario-usuario.

El elemento de información usuario-usuario contiene el **SetupAcknowledge-UUIE** definido en la sintaxis de mensajes H.225.0. El **SetupAcknowledge-UUIE** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

7.3.12 Estado

El mensaje Estado se utilizará para responder a un mensaje de señalización de llamada desconocido o a un mensaje indagación de estado.

Se debe aplicar el cuadro 3-17/Q.931 tal como está modificado por el cuadro 15.

Cuadro 15/H.225.0 – Situación

Elemento de información	Estado (status) H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada (nota)	M	3
Tipo de mensaje	M	1
Causa	M	4-32
Estado de la llamada	M	3
Visualización	O	2-82
Usuario-usuario	M	2-131
NOTA – Este mensaje puede transportar la referencia de llamada global si se aplica a todas las llamadas en una conexión que transporta múltiples llamadas.		

Con miras a la retrocompatibilidad con sistemas anteriores a la versión 4 de H.225.0, el emisor de este mensaje no incluirá el campo **h4501SupplementaryService** ni el campo **h245Control** en el campo **h323-message-body** del elemento de información usuario-usuario.

El elemento de información usuario-usuario contiene el **Status-UUIE** definido en la sintaxis de mensajes H.225.0. El **Status-UUIE** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada, utilizada en esta Recomendación.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – Testigos criptados.

7.3.13 Indagación de estado

El mensaje Indagación de estado puede utilizarse para solicitar el estado de la llamada como se describe en 8.4.2/H.323.

Se debe aplicar el cuadro 3-18/Q.931 con las modificaciones en el cuadro 16.

Cuadro 16/H.225.0 – Indagación de estado

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada (nota)	M	3
Tipo de mensaje	M	1
Visualización	O	2-82
Usuario-usuario	M	2-131
NOTA – Este mensaje puede transportar la referencia de llamada global si se aplica a todas las llamadas en una conexión que transporta múltiples llamadas.		

Con miras a la retrocompatibilidad con sistemas anteriores a la versión 4 de H.225.0, el emisor de este mensaje no incluirá el campo **h4501SupplementaryService** ni el campo **h245Control** en el campo **h323-message-body** del elemento de información usuario-usuario.

El elemento de información usuario-usuario contiene el **StatusInquiry-UUIE** definido en la sintaxis de mensajes H.225.0. El **StatusInquiry-UUIE** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado a la versión de H.225.0 soportada.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen y que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

7.4 Detalles de un mensaje de señalización de llamada H.225.0 basado en Q.932

Los mensajes definidos a continuación se derivan de la Rec. UIT-T Q.932 y la Rec. UIT-T H.450. Para más detalles véanse las citadas Recomendaciones.

7.4.1 Facilidad

El mensaje facilidad se utilizará para proporcionar información sobre adónde direccionar una llamada **(FacilityReason = routeCallToMC)**, o para que un punto extremo indique que la llamada entrante debe pasar por un controlador de acceso **(FacilityReason = routeCallToGatekeeper)**.

Para señalizar redireccionamiento de la llamada específico de los procedimientos H.323, se utiliza el elemento de información usuario-usuario del mensaje Facilidad. Este caso particular se indicará codificando un IE Facilidad de longitud cero. En este caso, el elemento de información facilidad constará exactamente de 2 octetos. Una entidad H.323 tratará adecuadamente el IE Facilidad vacío (específico de H.323) y será capaz de hacer caso omiso de los IE Facilidad que no comprenda.

El mensaje Facilidad puede utilizarse para pedir o acusar recibo de un servicio suplementario de conformidad con las Recomendaciones de la serie H.450.x. Por ese motivo, una o más APDU del servicio suplementario H.450 serán transportadas dentro del elemento de información usuario-usuario del mensaje Facilidad. Las APDU del servicio suplementario H.450 se codificarán según la cláusula 8/H.450.1. El elemento de información facilidad se contendrá con longitud cero. Obsérvese que un mensaje Facilidad de H.225.0 versión 2 o versión 3 que lleve únicamente las APDU del servicio suplementario H.450 podría optar por no incluir el UUIE Facilidad, pero sí en cambio utilizar la opción **cuerpo de mensaje h323 (h323-message-body) "vacío"**. En este caso, un mensaje Facilidad no contendría un campo **callIdentifier**. En H.225.0 versión 4 y posteriores, un emisor incluirá un UUIE Facilidad que lleve un campo **callIdentifier** en cada mensaje Facilidad asociado a una llamada, y fijará el campo **reason** en **transportedInformation**.

Si está presente un IE Facilidad que lleva la semántica de la Rec. UIT-T Q.932 y está codificado tal como se define en la Rec. UIT-T Q.932 y la Rec. UIT-T Q.95.x, constará por lo menos de 8 octetos tal como se indica en el cuadro 7-2/Q.932. La utilización de los IE Facilidad de ese tipo queda en estudio.

El mensaje Facilidad puede ser utilizado por un punto extremo o un controlador de acceso para pedir al recibiente que establezca un canal H.245 entre las dos entidades **(FacilityReason = startH245)**.

El mensaje Facilidad puede ser utilizado por un punto extremo o controlador de acceso para enviar un nuevo conjunto de testigos en el campo **tokens** y/o **cryptoTokens** del mensaje Facilidad **(FacilityReason = newTokens)**. Esto puede ser útil, por ejemplo, en aplicaciones en las que se utilizan testigos para permitir que se ejecuten algunas acciones durante un periodo de tiempo limitado.

Se debe seguir 7.1.1/Q.932 y 10.8 de ISO/CEI 11582, con las modificaciones del cuadro 17.

Cuadro 17/H.225.0 – Facilidad

Elemento de información	Estado H.225.0 (M/F/O)	Longitud H.225.0
Discriminador de protocolo	M	1
Referencia de llamada (nota 1)	M	3
Tipo de mensaje	M	1
Facilidad ampliada	O (nota 2)	8-*
Facilidad	O (nota 2)	2 u 8-*
Indicador de notificación	O	2-*
Visualización	O	2-82
Número de la parte llamante	F	No aplicable
Número de la parte llamada	F	No aplicable
Usuario-usuario	M	2-131
NOTA 1 – Este mensaje puede transportar la referencia de llamada global si se aplica a todas las llamadas en una conexión que transporta múltiples llamadas. NOTA 2 – Si se utiliza el mensaje Facilidad para llevar la señalización del servicio suplementario Q.95.x, se necesita el elemento de información Facilidad o bien el elemento de información Facilidad ampliada. Si se utiliza el mensaje Facilidad para el control del servicio suplementario de conformidad con las Recomendaciones de la serie H.450.x, o si se utiliza el mensaje Facilidad para el reencaminamiento hacia las funciones MC/GK, se requiere el elemento de información Facilidad de longitud cero.		

Codificación del elemento de información tipo de mensaje

El elemento de información tipo de mensaje del mensaje Facilidad se codificará "0110 0010".

El elemento de información usuario-usuario contiene el UUIE Facilidad definido en la sintaxis de mensaje H.225.0. El UUIE Facilidad incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado según la versión de H.225 soportada.

alternativeAddress (dirección alternativa) – Es una dirección de transporte específica a la cual la parte llamante debe dirigir la llamada; si está presente no se necesita **dirección alias alternativa**.

alternativeAliasAddress (dirección alias alternativa) – Contiene los alias que se pueden utilizar para redireccionar la llamada; si se proporciona un alias no se necesita **dirección alternativa**.

conferenceID (ID de conferencia) – Identificador de conferencia único; no es necesario si se utiliza el campo **conferencias**.

reason (motivo) – Más información sobre el mensaje Facilidad. Un **reason** de **featureSetUpDate** indica que el mensaje tiene por finalidad actualizar la información **featureSet** anteriormente enviada. Un **reason** de **forwardedElements** indica que el mensaje tiene por finalidad reenviar elementos de otro mensaje cuando no pueda enviarse el mensaje, como ocurriría cuando un controlador de acceso recibe un mensaje Llamada en curso después de haber enviado Llamada en curso. Un **reason** de **transportedInformation** indica que el objetivo del mensaje es transportar información de capa superior, por ejemplo en el campo **h4501SupplementaryService**; en este caso, el **Facility-UUIE** se incluye sólo para proporcionar el **callIdentifier**.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

destExtraCallInfo (información de llamada suplementaria de destino) – Necesario para efectuar posibles llamadas de canal adicional, es decir, para una llamada 2 × 64 kbit/s en el lado RCC. Sólo contendrá cadenas de dígitos marcados, números E.l64 o números privados, y no contendrá el número del canal inicial.

remoteExtensionAddress (dirección de extensión distante) – Contiene la dirección de alias de un punto extremo llamado en los casos en que es necesaria esta información para atravesar múltiples pasarelas.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

conferences (conferencias) – Una o más conferencias a las que es posible incorporarse.

h245Address (dirección h245) – Dirección de transporte específica en la que el punto extremo o el controlador de acceso que envía esta Facilidad desearía que el recibiente estableciera la señalización H.245. Obsérvese que este campo puede estar presente cuando una entidad de señalización intermedia transporta el campo **h245Address** de un mensaje Llamada en curso. Se ordena a la entidad receptora que inicie procedimientos H.245 solamente cuando **reason** es **startH245**.

fastStart (arranque rápido) – Utilizado únicamente en el procedimiento de conexión rápida, **fastStart** soporta la señalización necesaria para abrir un canal lógico. Utiliza la estructura **OpenLogicalChannel** definida en la Rec. UIT-T H.245, pero el emisor de la misma indica los modos en que prefiere recibir y transmitir, y las direcciones de transporte en las que espera recibir trenes de medios. Este campo está presente en un mensaje Facilidad cuando un controlador de acceso lo recibió en un mensaje Llamada en curso del usuario llamado y está reenviando esta información al usuario llamante. Un punto extremo no incluirá este campo.

multipleCalls (múltiples llamadas) – Si es VERDADERO, indica que el emisor del mensaje puede señalizar múltiples llamadas a través de una sola conexión de señalización de llamadas.

maintainConnection (mantener conexión) – Si es VERDADERO, indica que el emisor del mensaje puede soportar una conexión de señalización cuando no hay llamadas actualmente señalizadas a través de la conexión.

fastConnectRefused (arranque rápido rechazado) – Cuando un punto extremo establece una comunicación, debe retornar este elemento en cualquier mensaje, hasta el mensaje de conexión inclusive, para indicar que rechaza el procedimiento de conexión rápida. Este campo está presente en un mensaje Facilidad cuando un controlador de acceso lo recibió en un mensaje Llamada en curso del usuario llamado y está reenviando esta información al usuario llamante.

serviceControl (control de servicio) – Contiene datos específicos de servicio, o referencia a los mismos, que podrían ser utilizados por un punto extremo o pasarela (por ejemplo, para la presentación visual de un menú de opciones a un participante en la llamada) como se describe, por ejemplo, en el anexo K/H.323.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o circuitos RCC utilizados en la llamada.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

destinationInfo (información de destino) – Contiene un **EndpointType** para permitir al llamante determinar si en la llamada interviene o no una pasarela. Este campo está presente en un mensaje Facilidad cuando un controlador de acceso lo recibió en un mensaje Llamada en curso del usuario llamado y está reenviando esta información al usuario llamante. Este campo no existía en el mensaje Facilidad antes de la versión 4 de H.225.0.

h245SecurityMode (modo de seguridad h245) – Una entidad H.323 que recibe un mensaje Establecimiento con el conjunto **h245SecurityCapability** responderá con el correspondiente **h245SecurityMode** aceptable en mensaje Llamada en curso, Aviso, Progresión o Conexión. Este campo está presente en un mensaje Facilidad cuando un controlador de acceso lo recibió en un mensaje Llamada en curso del usuario llamado y está reenviando esta información al usuario llamante. Este campo no existía en el mensaje Facilidad antes de la versión 4 de H.225.0.

7.4.2 Notificación

Este mensaje puede ser enviado por una entidad H.323. El procesamiento en recepción es opcional.

Se debe seguir el cuadro 3-8/Q.931 con las modificaciones en el cuadro 18.

Cuadro 18/H.225.0 – Notificación

Elemento de información	Estado H.225.0 (M/F/O)	Longitud en H.225.0
Discriminador de protocolo	M	1
Referencia de llamada	M	3
Tipo de mensaje	M	1
Capacidad portadora	O (nota)	5-6
Indicador de notificación	M	3
Visualización	O	2-82
Usuario-usuario	M	2-131
NOTA – Incluido para indicar un cambio de la capacidad portadora.		

Con miras a la retrocompatibilidad con sistemas anteriores a la versión 4 de H.225.0, el emisor de este mensaje no incluirá el campo **h4501SupplementaryService** ni el campo **h245Control** en el campo **h323-message-body** del elemento de información usuario-usuario.

El elemento de información usuario-usuario contiene el **Notify-UUIE** definido en la sintaxis de mensajes H.225.0. El **Notify-UUIE** incluye lo siguiente:

protocolIdentifier (identificador de protocolo) – Fijado según la versión de H.225.0 soportada.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada utilizada en esta Recomendación.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

7.4.3 Otros mensajes

Los mensajes de control de llamada que pueden llevar los elementos de información facultativos Facilidad, Facilidad ampliada o Indicador de notificación se especifican en 8.3.

7.5 Valores de temporizadores de señalización de llamada H.225.0

Se soportarán los siguientes temporizadores Q.931:

- El "temporizador de establecimiento" T303 (véanse los cuadros 9-1/Q.931 y 9-2/Q.931), que define cuánto tiempo esperará el punto extremo llamante un mensaje Aviso, Llamada en curso, Conexión, Conexión completa u otro mensaje de la entidad llamada después de que ha enviado un mensaje Establecimiento. Este valor de temporización será de por lo

menos 4 segundos. Cabe señalar que pueden aparecer algunas aplicaciones en redes que tienen de por sí retardos más amplios (por ejemplo, compárese Internet con una red de empresa local o intranet).

- El "temporizador de establecimiento" T301 (véanse los cuadros 9-1/Q.931 y 9-2/Q.931), que define después de cuánto tiempo el punto extremo llamado responda. Este temporizador arranca cuando se recibe el mensaje Aviso y termina normalmente en Conexión o cuando el llamante termina el intento de llamada y envía Liberación completa. Este valor de temporización será 180 segundos (3 minutos) o superior.
- El "temporizador de envío solapado" T302 (véanse los cuadros 9-1/Q.931 y 9-2/Q.931), que define después de cuánto tiempo el punto extremo llamado dejará de esperar los dígitos marcados desde el punto extremo llamante durante el envío solapado. Este temporizador arranca cuando se envía el ACUSE DE ESTABLECIMIENTO o se recibe el mensaje INFORMACIÓN, y normalmente para recibir la indicación de envío completo. Este valor de temporización será 10-15 segundos.
- El "temporizador de recepción solapada" T304 (véanse los cuadros 9-1/Q.931 y 9-2/Q.931) que define después de cuánto tiempo el punto extremo llamante dejará de esperar los dígitos marcados desde el punto extremo llamado durante la recepción solapada. Este temporizador arranca cuando se recibe el ACUSE DE ESTABLECIMIENTO, rearranca cuando se envía el mensaje INFORMACIÓN, y normalmente para cuando se recibe LLAMADA EN CURSO, AVISO o CONEXIÓN. Este valor de temporización será 20 segundos o superior.
- El "temporizador de llamada entrante en curso" T310 (véanse los cuadros 9-1/Q.931 y 9-2/Q.931) que define después de cuánto tiempo el punto extremo llamado dejará de esperar los dígitos marcados desde el punto extremo llamante durante el envío solapado. Este temporizador arranca cuando se recibe LLAMADA EN CURSO, y normalmente para cuando se recibe AVISO, CONEXIÓN, o cuando el punto extremo llamante termina el intento de llamada y envía el mensaje Liberación completa. Este valor de temporización será 10 segundos o superior.
- El "temporizador de estado" T322 (véanse los cuadros 9-1/Q.931 y 9-2/Q.931) que define después de cuánto tiempo el punto extremo llamado dejará de esperar el mensaje ESTADO en respuesta al mensaje INDAGACIÓN DE ESTADO enviado. Este temporizador arranca cuando se envía INDAGACIÓN DE ESTADO, y normalmente para cuando se recibe el mensaje ESTADO. Este valor de temporización será 4 segundos o superior.

Adviértase que los valores del lado red de paquetes de estos temporizadores son los mismos que se utilizaron en la RCC.

Pueden soportarse otros temporizadores como parte de las Recomendaciones de la serie H.450.x sobre servicios suplementarios opcionales.

7.6 Elementos comunes de mensajes H.225.0

Esta cláusula describe estructuras ASN.1 que se utilizan en más de un mensaje registro, admisión y situación (RAS, *registration, admission and status*). Algunas pueden utilizarse en la parte usuario-usuario de los mensajes de señalización de llamada.

requestSeqNum (número secuencial de petición) en los mensajes se utiliza para seguir la pista a las múltiples peticiones pendientes. Junto con los mensajes de respuesta asociados (éxito o fracaso) devolverá el **requestSeqNum**. Los mensajes retransmitidos tendrán el mismo **requestSeqNum**. **RequestSeqNum** se incrementa en 1 módulo 65536.

El **protocolIdentifier (identificador de protocolo)** se incluye como parte del mensaje de descubrimiento, registro y establecimiento/conexión para permitir a las partes que intervienen determinar la antigüedad de las implementaciones que intervienen.

nonStandardParameter (parámetro no normalizado): Este parámetro es opcional en las secuencias de descubrimiento, registro y establecimiento/conexión para permitir a las partes que intervienen determinar la situación no normalizada de los puntos extremos que intervienen. Un controlador de acceso o una pasarela no está obligado a pasar **nonStandardData** que no soporta ni entiende, ya que éstos podrían interferir con las operaciones.

La estructura **TransportAddress (dirección de transporte)** se destina a captar los diversos formatos de transporte e incluye cualquier esquema específico de transporte, además de la referencia posiblemente local a un identificador de TSAP.

Las direcciones IPv4 e IPv6 se codificarán con el octeto más significativo de la dirección que es el primer octeto en la CADENA DE OCTETOS respectiva, por ejemplo, la clase dirección B IPv4 130.1.2.97 tendrá el "130" codificado en el primer octeto de la CADENA DE OCTETOS, seguido de "1" y así sucesivamente.

La dirección IPv6 a148:2:3:4:a:b:c:d tendrá "a1" codificado en el primer octeto "48" en el segundo octeto, "00" en el tercero, "02" en el cuarto y así sucesivamente.

Una estructura **TransportAddress** del tipo **ipSourceRoute** en la cual la SECUENCIA **route** no tiene entrada se interpretará como representando la misma dirección que la del tipo **ipAddress** que contiene los mismos valores para **ip** y **port**.

Las direcciones IPX, **node**, **netnum** y **port** se codificarán con el octeto más significativo de cada campo como el primer octeto en la respectiva CADENA DE OCTETOS.

Adviértase que esta estructura no utiliza el lenguaje dirección de transporte = "dirección de red de paquetes más identificador TSAP" de la Rec. UIT-T H.323. En su lugar, se utilizan los términos comunes en cada dominio de transporte.

La estructura **EndpointType** transmite información sobre la entidad H.323 en el extremo del enlace de señalización. La entidad H.323 podría completar uno o más elementos de mensaje **controlador de acceso**, **pasarela**, **mcu** o **terminal**. Si la entidad H.323 tiene un MC, la variable booleana **mc** podría ser entonces VERDADERA. En la cláusula 6.3/H.323 se describe la representación de una MCU cuando está situada con una pasarela; en este caso, el dispositivo H.323 puede incluir tanto la **gateway (pasarela)** como los elementos **mcu** dentro de su definición de **EndpointType**. La presencia del componente **set** indica que la entidad es un dispositivo del tipo punto extremo simple (SET, *simple endpoint type*) como se define por ejemplo en el anexo F/H.323. Las posiciones de bit en el componente **set** indican el tipo de dispositivo SET; su significado se define en el anexo F/H.323 y en otras Recomendaciones que especifican el los tipos de dispositivos SET. El campo **supportedTunnelledProtocols (protocolos tunelizados soportados)** suministra una lista prioritaria (por orden descendente del nivel de prioridad) de los protocolos tunelizados soportados.

La estructura **TunnelledProtocol (protocolo tunelizado)** identifica un protocolo de señalización tunelizado tal como se describe, por ejemplo, en los anexos M.1 y M.2/H.323. El campo **tunnelledProtocolObjectID (identificador de objeto de protocolo tunelizado)** es un **OBJECT IDENTIFIER** que identifica el protocolo que se tuneliza. El **tunnelledProtocolAlternateID (identificador alternativo de protocolo tunelizado)** proporciona un formato de identifiador alternativo. El campo **subIdentifier (subidentificador)** permite especificar una versión particular de un protocolo normalizado.

La estructura **TunnelledProtocolAlternateIdentifier (identificador alternativo de protocolo tunelizado)** proporciona un formato de identificador basado en cadenas para un protocolo tunelizado. El **protocolType (tipo de protocolo)** proporciona el tipo general de protocolo, por ejemplo PU-RDSI. El campo **protocolVariant (variante de protocolo)** proporciona una variación específica de esa norma, por ejemplo la ANSI.

En los cuadros VI.1 y VI.2 se muestran los protocolos tunelizados que se definen como propios de esta Recomendación. Se señala que la tunelización no se limita a los protocolos indicados en esos cuadros.

La estructura **GatewayInfo (información de pasarela)** contiene un elemento **protocol**, que permite a la pasarela indicar los protocolos que soporta.

La estructura **SupportedProtocols (protocolos soportados)** indica una elección de protocolos con los que una entidad H.323 tiene la capacidad de interfuncionar. Por ejemplo, la elección de la opción **h310** indica que la entidad proporciona interfuncionamiento con H.310.

En cada estructura de capacidad de protocolo soportada **(H310Caps**, **H320Caps**, etc.**)**, el elemento **dataRatesSupported (velocidades de datos soportadas)** indica las velocidades de datos que para cada protocolo soporta el dispositivo. El elemento **supportedPrefixes (prefijos soportados)** indica los prefijos asociados con un protocolo soportado y también, en algunos casos, con las velocidades de datos.

La estructura **McuInfo (información de unidad de control multipunto)** contiene un elemento **protocol** (**protocolo**), que permite a la MCU indicar los protocolos que soporte.

La estructura **CapacityReportingCapability (capacidad de informes de capacidades)** indica la aptitud de un punto extremo para comunicar información de capacidad de llamada.

La estructura **CapacityReportingSpecification (especificación de informes de capacidades)** indica la información de capacidad de llamada que un punto extremo debe comunicar. **callStart** indica una petición de información de capacidad al comienzo de la llamada (es decir, en ARQ o Establecimiento). **callEnd** indica una petición de información de capacidad al final de la llamada (es decir, en DRQ o Liberación completa). Una secuencia **when** vacía indica que el punto extremo no comunica información de capacidad.

La estructura **CallCapacityInfo (capacidad de llamada)** permite a un punto extremo indicar su capacidad de aceptación de llamada para cada tipo de llamada soportado por el punto extremo. Por tanto, representa la situación de reposo actual del punto extremo. Por ejemplo, en una pasarela vocal, **CallCapacityInfo** representaría el número de circuitos en reposo.

La estructura **CallCapacity (capacidad de llamada)** permite a un punto extremo indicar su capacidad máxima para cada tipo de llamada y su capacidad disponible en cada momento para cada tipo de llamada que soporte.

La estructura **CallsAvailable (llamadas disponibles)** representa un subconjunto de la capacidad total de llamadas de un punto extremo. El campo **group** permite identificar el subconjunto mediante una etiqueta de grupo. El **group** puede ser el mismo informado en el **CircuitIdentifier (identificador de circuito)**.

La estructura **DataRate (velocidad de datos)** proporciona información sobre la velocidad del protocolo de pasarela. **channelRate (velocidad de canal)** es la velocidad de canal básica en cientos de bits. **channelMultiplier (multiplicador de canales)** indica el número de canales a la channelRate. Por ejemplo, si una pasarela soporta una llamada 3B, **channelMultiplier** = 3 y **channelRate** = 640 para un canal de 64 kbit/s.

La estructura **VendorIdentifier (identificador de vendedor)** permite a un vendedor identificar un producto. El elemento **vendedor (vendor)** permite la identificación en términos de indicativo de país, extensión y código del fabricante. **productId (identificador de producto)** y **versionId (identificador de versión)** son cadenas de textos que pueden dar información sobre el producto. El campo **enterpriseNumber (número de empresa)** identifica al fabricante y viene dado por la Autoridad de asignación de números Internet (IANA, *Internet assigned numbers authority*),

La estructura **H221NonStandard** permite la definición de un campo no normalizado. El elemento **t35CountryCode** identificará el país, como se describe en el anexo A/T.35. El elemento

t35Extension contendrá una ampliación del indicativo de país que se asigna en el plano nacional, a menos que **t35CountryCode** sea "1111 1111" binario, en cuyo caso este campo contendrá el indicativo de país que figura en el anexo B/T.35. El **manufacturerCode** se asignará en el plano nacional e identifica un fabricante de equipo.

La estructura **AliasAddress (dirección de alias)** está destinada a captar los diversos formatos de dirección externos que hacen referencia a una determinada ubicación de transporte en la red de paquetes. Cuando se registra una dirección constituida por dígitos marcados con un controlador de acceso, un punto extremo utilizará el campo **dialledDigits** y utilizará solamente los dígitos 0-9. Cuando se registra una dirección E.164 con un controlador de acceso, un punto extremo utilizará el campo **e164Number** y utilizará solamente los dígitos 0-9. Cuando se registra, o de otro modo, se representa un prefijo, un punto extremo utilizará el campo **dialledDigits** y utilizará solamente los dígitos 0-9 y "#" y "*". El campo **mobileUIM** es un módulo de identificación para sistemas compatibles con redes inalámbricas de la segunda y tercera generación, y permite el interfuncionamiento con redes móviles públicas terrestres como se describe, por ejemplo, en el anexo E/H.246.

La estructura **AddressPattern (esquema de dirección)** permite la especificación de una **AliasAddress** expandida por comodín o una gama de **PartyNumbers**. El campo **wildcard (comodín)** representa la posible expansión de la estructura **AliasAddress**. Para dígitos marcados o números E.164, esta expansión es posible al final del número. Para direcciones de correo electrónico, la expansión es posible al principio. Por ejemplo, si el comodín es "+1 303", el esquema podría representar cualquier número en el indicativo de zona de Denver (Estados Unidos). El campo **range (gama)** de la estructura **AddressPattern** representa una gama de direcciones incluidos el principio y fin indicados de la gama.

El mecanismo que utiliza un punto extremo para determinar el tipo de dirección es una cuestión de implementación. La representación de los diversos tipos de números en el mensaje se muestra en el cuadro 19. Obsérvese que si un punto extremo no conoce el tipo o el alcance de una dirección, debe representarlo como un número privado desconocido cuando se codifica en mensajes de señalización de llamada H.225.0, y como una **dirección de alias de dígitos marcados (dialledDigits AliasAddress)** cuando se codifica en mensajes RAS.

Cuadro 19/H.225.0 – Correspondencia de representaciones de tipos de números

Tipo de número	Representación Q.931	Representación de elemento de información H.225.0	Representación H.225.0 UUIE
Desconocido (valor por defecto y modo interoperabilidad versión 1)	Plan de numeración privado, Tipo de número = Desconocido ("000") (Nota 1)	Plan de numeración privado, Tipo de número = Desconocido "000"	**dialledDigits AliasAddress** (Nota 2)
Número privado desconocido	Plan de numeración privado, Tipo de número = Desconocido ("000") (Nota 1)	Plan de numeración privado, Tipo de número = Desconocido ("000") (Nota 1)	**dialledDigits AliasAddress** (Nota 2)

Cuadro 19/H.225.0 – Correspondencia de representaciones de tipos de números

Tipo de número	Representación Q.931	Representación de elemento de información H.225.0	Representación H.225.0 UUIE
Número regional privado, de nivel 2	Plan de numeración privado, Tipo de número = Número regional de nivel 2 ("001")	Plan de numeración privado, Tipo de número = Desconocido ("000") (Nota 1)	**privateNumber** de **PartyNumber AliasAddress**, **TypeOfNumber** = **level2RegionalNumber**
Número regional privado, de nivel 1	Plan de numeración privado, Tipo de número = Número regional de nivel 1 ("010")	Plan de numeración privado, Tipo de número = Desconocido ("000") (Nota 1)	**privateNumber** de **PartyNumber AliasAddress**, **TypeOfNumber** = **level1RegionalNumber**
Número privado, específico de RPSI	Plan de numeración privado, Tipo de número = Número privado específico de RPSI ("011")	Plan de numeración privado, Tipo de número = Desconocido ("000") (Nota 1)	**privateNumber** de **PartyNumber AliasAddress**, **TypeOfNumber** = **pISNSpecificNumber**
Número regional privado, de nivel 0 (local)	Plan de numeración privado, Tipo de número = Número regional de nivel 0 ("100")	Plan de numeración privado, Tipo de número = Desconocido ("000") (Nota 1)	**privateNumber** de **PartyNumber AliasAddress**, **TypeOfNumber** = **localNumber**
Número público E.164, desconocido	Plan de numeración RDSI/telefonía, Tipo de número = Desconocido ("000")	Plan de numeración RDSI/telefonía, Tipo de número = Desconocido ("000")	**e164Number** de **PartyNumber AliasAddress**, **TypeOfNumber** = **Unknown**
Número público E.164, número internacional	Plan de numeración RDSI/telefonía, Tipo de número = Número internacional ("001")	Plan de numeración RDSI/telefonía, Tipo de número = Número internacional ("001")	**e164Number** de **PartyNumber AliasAddress**, **TypeOfNumber** = **internationalNumber**
Número público E.164, número nacional	Plan de numeración RDSI/telefonía, Tipo de número = Número nacional ("010")	Plan de numeración RDSI/telefonía, Tipo de número = Número nacional ("010")	**e164Number** de **PartyNumber AliasAddress**, **TypeOfNumber** = **nationalNumber**

Cuadro 19/H.225.0 – Correspondencia de representaciones de tipos de números

Tipo de número	Representación Q.931	Representación de elemento de información H.225.0	Representación H.225.0 UUIE
Número público E.164, número específico de red	Plan de numeración RDSI/telefonía, Tipo de número = Número específico de red ("011")	Plan de numeración RDSI/telefonía, Tipo de número = Número específico de red ("011")	**e164Number** de **PartyNumber AliasAddress**, **TypeOfNumber** = **networkSpecific Number**
Número público E.164, número de abonado	Plan de numeración RDSI/telefonía, Tipo de número = Número de abonado ("100")	Plan de numeración RDSI/telefonía, Tipo de número = Número de abonado ("100")	**e164Number** de **PartyNumber AliasAddress**, **TypeOfNumber** = **subscriberNumber**
Número público E.164, número abreviado	Plan de numeración RDSI/telefonía, Tipo de número = Número abreviado ("110")	Plan de numeración RDSI/telefonía, Tipo de número = Número abreviado ("110")	**e164Number** de **PartyNumber AliasAddress**, **TypeOfNumber** = **abbreviatedNumber**
NOTA 1 – Cuando la identificación de plan de numeración = Private (privado), los dígitos de número privado se codifican en **privateNumber** de **PartyNumber**, que incluye el tipo de número. El campo tipo de número del elemento de información no se tendrá en cuenta en recepción, y se codificará según este cuadro en transmisión. NOTA 2 – Un **privateTypeOfNumber = Unknown PartyNumber AliasAddress** se tratará de la misma manera que un **dialledDigits AliasAddress**.			

La estructura **MobileUIM** representa un módulo identificación para sistemas compatibles con redes inalámbricas de la segunda y tercera generación. Las opciones son:

- **ansi-41-uim** – Para redes inalámbricas definidas por normas de Estados Unidos de América.
- **gsm-uim** – Para redes inalámbricas definidas por normas europeas.

La estructura **ANSI-41-UIM** identifica un módulo de identificación para sistemas conformes con normas de Estados Unidos de América para redes inalámbricas. Las opciones son:

- **imsi** – Para números de identificación de estación móvil internacional (*international mobile station identification*).
- **min** – Para números de identificación de móviles (*mobile identification number*).
- **mdn** – Para números de directorio móviles (*mobile directory number*).
- **msisdn** – Para números RDSI de estación móvil (*mobile station ISDN number*).
- **esn** – Para números de serie electrónicos (*electronic serial number*).
- **mscid** – Para números de centro de conmutación móvil más números de identificación de mercado o de identificación sistema (*mobile switching center number plus market identification or system identification number*).
- **sid** – Para números de identificación de sistema (*system identification number*).

- **mid** – Para números de identificación de mercado (*market identification number*).
- **systemMyTypeCode** – Para números de identificación de vendedor.
- **systemAccessType** – Para tipo de sistema de acceso.
- **qualificationInformationCode** – Para código de información de calificación.
- **sesn** – Para números de serie electrónicos SIM (*SIM electronic serial number*).
- **soc** – Para códigos de operador de sistema (*system operator code*).

La estructura **GSM-UIM** identifica un módulo de identificación para sistemas conformes con normas europeas para redes inalámbricas. Las opciones son:

- **imsi** – Para identificación de estación móvil internacional (*international mobile station identification*).
- **tmsi** – Para identificación temporal de estación móvil (*temporary mobile station identification*).
- **msisdn** – Para números RDSI de estación móvil (*mobile station ISDN*).
- **imei** – Para números de identificación de equipo móvil internacional (*international mobile equipment identification*).
- **hplmn** – Para números de red móvil terrestre pública propia (*home public land mobile network*).
- **vplmn** – Para números de red móvil terrestre pública de visita (*visiting public land mobile network*).

La estructura **ExtendedAliasAddress (dirección de alias extendida)** proporciona una manera de asociar información común con direcciones de alias. El **presentationIndicator (indicador de presentación)** indica si deberá permitirse o restringirse la presentación de la **address** (**dirección**). El **screeningIndicator (indicador de cribado)** indica si la **address** fue proporcionada por el punto extremo o por la red y si ha sido cribada por la red.

La estructura **Endpoint (punto extremo)** se utiliza para indicar la información de reserva, redundante o alternativa sobre un punto extremo:

- **nonStandardData (datos no normalizados) –** Lleva información no definida en esta Recomendación (por ejemplo, datos privados).
- **aliasAddress (dirección de alias) –** Es una lista de direcciones de alias por las que otros puntos extremos pueden identificar este punto extremo.
- **callSignalAddress (dirección de señalización de llamada) –** Es la dirección de transporte de señalización de llamada para este punto extremo.
- **rasAddress (dirección ras) –** Es la dirección de transporte de registro y situación para este punto extremo.
- **endpointType (tipo de punto extremo) –** Especifica el tipo del punto extremo.
- **tokens (testigos) –** Testigos asociados en este punto extremo (esto es, el punto extremo descrito en la estructura **Endpoint**).
- **cryptoTokens (testigos criptados) – Testigos criptados** asociados con este punto extremo (esto es, el punto extremo descrito en la estructura **Endpoint**).
- **priority (prioridad) –** Se utiliza cuando se presenta una SECUENCIA de **puntos extremos**. Se prefieren los puntos extremos con números de prioridad inferior a los puntos extremos con números de prioridad superior. Los puntos extremos sin números de prioridad son equivalentes a los que tienen una prioridad de 0 (la prioridad más alta).

- **remoteExtensionAddress (dirección de extensión distante) –** Contiene la dirección de alias de un punto extremo en los casos en que es necesaria esta información para atravesar múltiples pasarelas.
- **destExtraCallInfo (información de llamada suplementaria de destino) –** Contiene direcciones externas para múltiples llamadas.
- **alternateTransportAddresses –** Indica el soporte de transportes diferentes de TCP.

La estructura **alternateTransportAddresses** transporta direcciones de señalización de llamada para transportes diferentes de TCP.

La estructura **UseSpecifiedTransport** define una opción de protocolos de transporte de señalización. Un valor de **tcp** indica el protocolo TCP; un valor de **annexE** indica el protocolo definido en el anexo E/H.323, y un valor **sctp** indica la utilización del protocolo de transmisión de control de trenes (SCTP, *stream control transmission protocol*).

La estructura **AlternateGK (controlador de acceso alternativo)** se utiliza para indicar una lista de controladores de acceso alternativos o de reserva:

- **rasAddress (dirección ras) –** Dirección de transporte utilizada para la señalización RAS.
- **gatekeeperIdentifier (identificador de controlador de acceso) –** Se incluye opcionalmente para identificar el controlador de acceso de reserva o alternativo. Si se suministra, deberá incluirse en futuros mensajes RAS enviados al controlador de acceso de reserva.
- **needToRegister (necesidad de registro) –** Fijado a VERDADERO para indicar que el punto extremo se debe registrar con el controlador de acceso alternativo antes de enviar otras peticiones RAS.
- **priority (prioridad) –** Indica la prioridad del controlador de acceso de reserva o alternativo. Un número bajo implica una prioridad alta.

La estructura **AltGKInfo (información de controlador de acceso alternativo)** se utiliza para dar información sobre controladores de acceso alternativos:

- **alternateGatekeeper (controlador de acceso alternativo) –** Secuencia de controladores de acceso alternativos prioritarios.
- **altGKisPermanent (el controlador de acceso alternativo es permanente) –** VERDADERO para indicar que todas las futuras señales RAS deben ser redireccionadas a un controlador de acceso indicado en el campo **alternateGatekeeper**, y FALSO para indicar que sólo debe redireccionarse el mensaje que provocó el rechazo. Esta bandera se debe fijar a VERDADERO si una bandera **needToRegister** se fija a VERDADERO en el campo **alternateGatekeeper**.

La estructura **QseriesOptions (opciones de la serie Q)** suministra información al controlador de acceso o a otros puntos extremos relativa al soporte por un terminal de protocolos opcionales de la serie Q. Se utiliza en los mensajes ARQ, Establecimiento y GRQ. La utilización de la estructura QSeriesOptions no está definida y queda en estudio.

GloballyUniqueID (identificador único a nivel mundial) y **ConferenceIdentifier (identificador de conferencia)** son considerados identificadores únicos a nivel mundial; su utilización se describe en la Rec. UIT-T H.323. Un **GloballyUniqueID** se codifica primero con el octeto cero. Un **GloballyUniqueID** está formado según el cuadro 20.

Cuadro 20/H.225.0 – Formación de identificador único a nivel mundial

Campo	Tipo de datos	Número de octetos	Nota
time_low	Entero de 32 bits sin signo	0-3	El campo bajo de la indicación de tiempo
time_mid	Entero de 16 bits sin signo	4-5	El campo medio de la indicación de tiempo
time_hi_and_version	Entero de 16 bits sin signo	6-7	El campo alto de la indicación de tiempo multiplexado con el número de versión
clock_seq_hi_and_reserved	Entero de 8 bits sin signo	8	El campo alto de la secuencia de reloj multiplexado con la variante
clock_seq_low	Entero de 8 bits sin signo	9	El campo bajo de la secuencia de reloj
node	Entero de 48 bits sin signo	10-15	El identificador de nodo único a nivel espacial

El **GloballyUniqueID** está formado por un registro de 16 octetos y no podrá contener relleno entre campos. El tamaño total es de 128 bits.

Para que sea menos confusa la asignación de bits dentro de los octetos, el registro del **GloballyUniqueID** se define únicamente en términos de campos que son números enteros de octetos. El número de versión es multiplexado con la indicación de tiempo (*time_high*), y el campo de la variante es multiplexado con la secuencia de reloj (*clock_seq_high*).

La indicación de tiempo es un valor de 60 bits representado por el tiempo universal coordinado (UTC, *coordinated universal time*) como un cómputo de intervalos de 100 nanosegundos a partir de las 00:00:00.00 del 15 de octubre de 1582 (fecha de la reforma gregoriana del calendario cristiano).

El número de versión es multiplexado en los 4 bits más significativos del campo *time_hi_and_version*, y se fija a 1 ("0001" binario).

El campo variable determina la disposición del **GloballyUniqueID**. La estructura de un **GloballyUniqueID** de DCE se fija en las distintas versiones. Es posible que otras variantes de **GloballyUniqueID** no puedan interfuncionar con un **GloballyUniqueID** de DCE. El interfuncionamiento de los **GloballyUniqueID** se define como la aplicabilidad de operaciones tales como conversión de cadena, comparación y ordenamiento del léxico en los distintos sistemas. El campo *variante* está formado por un número variable de los bits más significativos (MSB) del campo *clock_seq_hi_and_reserved* (véase el cuadro 21).

Cuadro 21/H.225.0 – Contenido del campo variante DCE

msb1	msb2	msb3	Descripción
0	–	–	Reservado, compatibilidad hacia atrás NCS
1	0	–	Variante DCE
1	1	0	Reservado, Microsoft Corporation GUID
1	1	1	Reservado para futura definición

La secuencia de reloj es necesaria para detectar las posibles pérdidas de monotonía del reloj. La secuencia de reloj se codifica en los 6 bits menos significativos del campo *clock_seq_hi_and_reserved* y en el campo *clock_seq_low*.

El campo *node* está formado por la dirección IEEE, generalmente la dirección central. Para sistemas con múltiples nodos IEEE 802, puede utilizarse cualquier dirección de nodo disponible. El octeto

direccionado más bajo (octeto número 10) contiene el bit mundial/local y el bit unidifusión/multidifusión, y es el primer octeto de la dirección transmitida por una red de paquetes 802.3.

El valor de la secuencia de reloj se cambiará cuando:

- El generador del **GloballyUniqueID** detecte que el valor local del UTC ha retrocedido; esto puede deberse al funcionamiento normal del servicio de tiempo del DCE.
- El generador del **GloballyUniqueID** haya perdido su estado del último valor de UTC utilizado, lo que indica que el tiempo ha retrocedido; esto suele ocurrir en el rearranque.

Aunque un nodo esté operativo, el generador del **GloballyUniqueID** conserva siempre el último UTC utilizado para crear un **GloballyUniqueID**. Cada vez que se crea un nuevo **GloballyUniqueID**, el *UTC* actual se compara con el valor conservado y si el valor actual es menor (caso del reloj no monótono) o si se ha perdido el valor conservado, la *secuencia de reloj* se incrementa en módulo 16 384, evitando así la duplicación del **GloballyUniqueID**.

La *secuencia de reloj* deberá inicializarse en un número aleatorio para reducir al mínimo la correlación entre sistemas.

Un **GloballyUniqueID** se genera aplicando el siguiente algoritmo:

1) Determinar los valores de la indicación de tiempo basada en UTC y la secuencia de reloj que se ha de utilizar en el **GloballyUniqueID**.
2) Fijar el campo *time_low* igual a los 32 bits menos significativos (bits numerados de 0 a 31 inclusive) de la indicación de tiempo en el mismo orden de importancia.
3) Fijar el campo *time_mid* igual a los bits numerados de 32 a 47 inclusive de la indicación de tiempo en el mismo orden de importancia.
4) Fijar los 12 bits menos significativos (bits numerados de 0 a 11 inclusive) del campo *time_hi_and_version* igual a los bits numerados de 48 a 59 inclusive de la indicación de tiempo en el mismo orden de importancia.
5) Fijar los 4 bits más significativos (bits numerados de 12 a 15 inclusive) del campo *time_hi_and_version* en el número de versión de 4 bits correspondientes a la versión del **GloballyUniqueID** que se crea, tal como se indicó en el cuadro 21.
6) Fijar el campo *clock_seq_low* en los 8 bits menos significativos (bits numerados de 0 a 7 inclusive) de la *secuencia de reloj* en el mismo orden de importancia.
7) Fijar los 6 bits menos significativos (bits numerados de 0 a 5 inclusive) del campo *clock_seq_hi_and_reserved* en los 6 bits más significativos (bits numerados de 8 a 13 inclusive) de la *secuencia de reloj* en el mismo orden de importancia.
8) Fijar los 2 bits más significativos (bits numerados de 6 a 7) del campo *clock_seq_hi_and_reserved* a 0 y 1, respectivamente.
9) Fijar el campo *node* en la dirección IEEE de 48 bits en el mismo orden de importancia que la dirección.

Si un sistema desea generar un **GloballyUniqueID** pero no tiene una tarjeta de red conforme a IEEE 802 u otra fuente de direcciones IEEE 802, se utilizará un método alternativo para generar un valor de sustitución de la dirección. La solución ideal es obtener un número aleatorio de calidad criptográfica de 47 bits, y utilizarlo como los 47 bits más significativos del ID de nodo, con el bit menos significativo del primer octeto del ID de nodo fijado a 1. Este es el bit unidifusión/multidifusión, que no se fijará nunca en las direcciones IEEE 802 obtenidas a partir de las tarjetas de red; por lo tanto, nunca puede surgir un conflicto entre **GloballyUniqueID** generados por máquinas que dispongan o no de tarjetas de red.

Aunque algunos sistemas no tengan una primitiva con la que generar números aleatorios de calidad criptográfica, en muchos de ellos se dispone por lo general de un número relativamente importante

de fuentes de aleatoriedad a partir de las cuales puede generarse uno de esos números. Esas fuentes son específicas del sistema pero suelen incluir el porcentaje de memoria utilizada, la capacidad de memoria principal en octetos, la capacidad de memoria principal libre en octetos, el tamaño del fichero de desplazamiento por páginas en octetos, los octetos libres del fichero de desplazamiento por páginas, el tamaño total del espacio de la dirección virtual de usuario en octetos, los octetos totales disponibles del espacio de la dirección de usuario, el tamaño de la unidad del disco de carga en octetos, el espacio libre del disco en la unidad de carga en octetos, el tiempo actual, el tiempo transcurrido desde la carga inicial del sistema, las dimensiones de cada fichero en los diversos directorios del sistema, etc.

Para ser utilizada en un texto legible por el hombre, la representación en cadena de un **GloballyUniqueID** se especifica como una secuencia de campos, algunos de los cuales se separan con guiones.

Cada campo es tratado como un entero y su valor se imprime como una cadena de dígitos hexadecimales rellena de ceros, cuyo primer dígito es el dígito más significativo. Los valores hexadecimales de a a f inclusive se representan con caracteres en minúscula en la salida, en la entrada, son independientes del tamaño de los caracteres que los represente. La secuencia es la misma que el tipo construido de **GloballyUniqueID**.

La definición formal de la representación en cadena del **GloballyUniqueID** viene dada por la siguiente forma Backus Naur (BNF) ampliada:

```
UUID                    = <time_low> <hyphen> <time_mid> <hyphen>
                          <time_high_and_version> <hyphen>
                          <clock_seq_and_reserved>
                          <clock_seq_low> <hyphen> <node>
time_low                = <hexOctet> <hexOctet> <hexOctet> <hexOctet>
time_mid                = <hexOctet> <hexOctet>
time_high_and_version   = <hexOctet> <hexOctet>
clock_seq_and_reserved  = <hexOctet>
clock_seq_low           = <hexOctet>
node                    = <hexOctet><hexOctet><hexOctet>
                          <hexOctet><hexOctet><hexOctet>
hexOctet                = <hexDigit> <hexDigit>p
hexDigit                = <digit> | <a> | <b> | <c> | <d> | <e> | <f>
digit                   = "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" |
                          "8" | "9"
hyphen                  = "-"
a                       = "a" | "A"
b                       = "b" | "B"
c                       = "c" | "C"
d                       = "d" | "D"
e                       = "e" | "E"
f                       = "f" | "F"
```

A continuación se indica un ejemplo de la representación en cadena de un **GloballyUniqueID**:

f81d4fae-7dec-11d0-a765-00a0c91e6bf6

timeToLive (tiempo de vida) es el número de segundos durante los cuales se considera válido un registro.

La estructura **H248PackagesDescriptor (descriptor de lotes H248)** es una cadena de octetos que contiene **PackagesDescriptor** H.248, codificado con las reglas de codificación compactada (PER *packed encoding rules*) de ASN.1

La estructura **H248SignalsDescriptor (descriptor de señales H248)** es una cadena de octetos que contiene **SignalsDescriptor** H.248 codificado con PER de ASN.1.

La estructura **FeatureDescriptor (descriptor de característica)** es un elemento **GenericData** que se utiliza para la identificación general de una característica.

La estructura **CircuitInfo (información de circuito)** proporciona información sobre el circuito o los circuitos RCC utilizados para la llamada. El campo **sourceCircuitID (identificador de circuito de origen)** proporciona información sobre el circuito de origen cuando la llamada se origina en la RCC, y podría ser utilizado por una pasarela de ingreso para notificar el identificador de circuito de origen al controlador de acceso. El **destinationCircuitID** (**identificador de circuito de destino**) proporciona información sobre el circuito de destino cuando la llamada termina en la RCC, y podría ser utilizado por un controlador de acceso para seleccionar un circuito de destino en una pasarela de egreso.

La estructura **CircuitIdentifier (identificador de circuito)** designa una facilidad a los efectos de informes por una pasarela o de selección por un controlador de acceso. La estructura **CircuitIdentifier** soporta una diversidad de interfaces.

La estructura **CicInfo** designa canales portadores SS7. El campo **cic** es el código de identificador de circuito definido en la Rec. UIT-T Q.763 y se codifica con los bits menos significativos en el primer octeto y los bits más significativos en el último octeto. El campo **pointCode** contiene el código de punto definido en la Rec. UIT-T Q.763. El primer octeto del **pointCode** identifica la red (código indicador de red) y los octetos restantes identifican el valor de código de punto SS7. Los campos **cic** y **pointCode** son de longitud variable para hacer posibles opciones nacionales diferentes.

La estructura **GroupID (identificador de grupo)** identifica un **group** físico o lógico y un **member (miembro)** (o conjunto de **members**) de ese grupo. Por ejemplo, **group** podría identificar una interfaz física, en tanto que **member** podría identificar un determinado DS0 en esa interfaz. Si se omite el campo **member**, cabe esperar que la pasarela seleccione una facilidad disponible en el **group** especificado.

La estructura **CarrierInfo (información de portadora)** contiene información sobre la Selección de portadora. El **carrierIdentificationCode (código de identificación de portadora)** identifica la portadora [al igual que el código de identificación de portadora en un mensaje de dirección inicial (IAM, *initial address message*) de la parte usuario de la RDSI] elegida por el abonado o determinada por las aplicaciones de encaminamiento, como una cadena binaria de dígitos. El campo **carrierName (nombre de portadora)** es otro medio de identificar la portadora como una cadena ASCII.

carrier (portadora) – Código de identificación/selección de portadora para el encaminamiento de llamada, determinado por las aplicaciones de encaminamiento o elegido por el abonado.

La estructura **ServiceControlDescriptor (descriptor de control de servicio)** contiene datos específicos de servicio, o referencias a éstos, destinados a la presentación de usuario u otras comunicaciones de control de servicio descritas, por ejemplo, en el anexo K/H.323. Son posibles las siguientes opciones:

- **url** – Esta selección contiene un protocolo o recurso referenciado por URL.
- **signal** – Esta selección contiene un **SignalsDescriptor** definido en la Rec. UIT-T H.248, en formato binario. Los elementos facultativos **streamID** y **notifyCompletion** no se incluirán en la secuencia **Signal** del **SignalsDescriptor**.
- **nonStandard** – Esta selección contiene información no definida en esta Recomendación (por ejemplo, datos privados).
- **callCreditServiceControl** – Esta selección contiene información relacionada con el control de la duración de una llamada y suministra al usuario información sobre el saldo de su cuenta.

La estructura **ServiceControlSession (sesión de control de servicio)** contiene una descripción de una sesión de control de servicio descrita, por ejemplo, en el anexo K/H.323. Contiene los siguientes campos:

- **sessionId (identificador de sesión)** – Número entero que identifica la sesión en cuestión y que es exclusivo del cliente. Obsérvese que los identificadores recibidos por trayectos de señalización diferentes (por ejemplo, RAS y señalización de llamada) son ortogonales y pueden superponerse.
- **contents (contenido)** – Estructura **ServiceControl** con el contenido o mecanismo de comunicación pertinentes.
- **reason (motivo, o razón)** – Indica si se trata de una nueva sesión **(open)** o de una modificación de una sesión existente **(refresh)**, o que la sesión es terminada por el proveedor **(close)** y se debe cerrar los recursos existentes tales como GUI, etc.

La estructura **RasUsageInfoTypes (tipos de información de utilización de RAS)** indica los tipos de información de utilización que pueden ser comunicados por un punto extremo a un controlador de acceso. El punto extremo utiliza esta estructura para indicar sus capacidades con respecto a la toma y la comunicación de información de utilización, y el controlador de acceso utiliza esta estructura para solicitar información de utilización de determinados tipos. El campo **nonStandardUsageTypes** permite a un vendedor hacer referencia a tipos de información de utilización privada. Los campos **startTime** y **endTime** indican, respectivamente, los instantes en que una llamada comienza y termina. El parámetro **terminationCause** indica el motivo por el cual terminó la llamada.

La estructura **RasUsageSpecification (especificación de utilización de RAS)** es una plantilla que permite a un controlador de acceso solicitar determinados tipos de información de utilización en puntos específicos de una llamada. El campo **when** indica el punto o puntos de la llamada en el cual o en los cuales el punto extremo debe comunicar la información que se le ha solicitado; **start** hace referencia al comienzo de la llamada, **end** hace referencia al final de la llamada, e **inIrr** hace referencia a mensajes IRR no solicitados. El campo **callStartingPoint** define el punto o puntos de la llamada que deberán considerarse el comienzo de la llamada a los efectos de comunicar información de utilización; un valor de **connect** hace referencia a la transmisión o recepción del mensaje Conexión, y un valor de **alerting** hace referencia a la transmisión o recepción del mensaje Aviso. El campo **required** indica los tipos de información de utilización que el punto extremo debe comunicar. Una estructura **RasUsageSpecification** en la que no se selecciona nada en el campo **when** ni en el campo **required** indica una petición de que se inhabilite la comunicación de información de utilización.

La estructura **RasUsageInformation (información de utilización de RAS)** es una colección de datos de utilización relativos a una determinada llamada. El campo **nonStandardUsageFields** permite a un vendedor indicar información de utilización de tipos privados. El campo **alertingTime** indica el instante en que se envió o recibió el mensaje Aviso. El campo **connectTime** indica el instante en que se envió o recibió el mensaje Conexión. El campo **endTime** indica el instante en que se envió o recibió el mensaje Liberación completa.

La estructura **CallTerminationCause (causa de terminación de la llamada)** indica el motivo por el cual termina la llamada. El campo **releaseCompleteReason** indica la **reason** que se especificó en el mensaje Liberación completa. El campo **releaseCompleteCauseIE** proporciona el elemento de información causa del mensaje Liberación completa.

La estructura **BandwidthDetails (detalles de anchura de banda)** define información adicional de utilización de anchura de banda que no está disponible en la estructura **BandWidth**. El campo **sender** se fija a VERDADERO si el mensaje lo envía el emisor del tren, o a FALSO si lo envía el receptor. El campo **multicast** se fija a VERDADERO si el tren es multidifusión, o a FALSO si no lo es. El campo **bandwidth** indica la anchura de banda utilizada para el tren en unidades de cien bits por segundo. El campo **rtcpAddresses** indica las direcciones RTCP utilizadas para el tren de medios.

La estructura **CallCreditCapability (capacidad de crédito de llamada)** indica ciertas capacidades de un punto extremo relacionadas con la facturación de una llamada. Por defecto, se supone que un punto extremo no tiene estas capacidades facultativas. Si un campo de esta estructura no está incluido, ello indica que la situación de la capacidad representada por ese campo no ha cambiado desde la última vez en que se notificó. El campo **canDisplayAmountString** indica si el punto extremo puede visualizar una cadena de texto que da la cantidad de dinero en la cuenta de un usuario. El campo **canEnforceDurationLimit** indica si un punto extremo está facultado para desligar una llamada cuando se ha rebasado un límite de duración de la llamada indicado por el controlador de acceso.

La estructura CallCreditServiceControl (control de servicio de crédito de llamada) permite a un controlador de acceso proporcionar a un punto extremo cierta información y control relacionados con la facturación. Contiene los siguientes campos:

- **amountString (cadena de cantidad)** – Este campo indica la cantidad de dinero en la cuenta de un usuario, por ejemplo, "$10.00". La cadena contendrá el símbolo de moneda adecuado. Adviértase que las abreviaturas normalizadas para tipos de moneda, como "USD" para dólares de Estados Unidos, se definen en ISO 4217. El campo **amountString** se codificará en Basic ISO/CEI 10646-1 (Unicode).
- **billingMode (modo de facturación)** – Este campo indica el modo de facturación para esta llamada. Un modo de **debit** indica que las tasas correspondientes a la llamada se deducirán de la cantidad de dinero disponible en la cuenta del usuario. Un modo de **credit** indica que las tasas correspondientes a la llamada deberán pagarse después. Un punto extremo podría utilizar esta información para, por ejemplo, determinar el tipo de anuncio verbal o visual que habrá de presentarse.
- **callDurationLimit (límite de duración de llamada)** – Este campo indica la cantidad de tiempo restante autorizada para una determinada llamada.
- **enforceCallDurationLimit (cumplimiento del límite de duración de la llamada)** – Este campo indica si se pide al punto extremo que corte la llamada después de rebasado el límite de tiempo indicado por **callDurationLimit**. Si este campo no está incluido, el punto extremo interpretará esa ausencia en el sentido de que la directiva no ha cambiado desde su estado previo.
- **callStartingPoint (punto de comienzo de llamada)** – Este campo indica el punto de la llamada en que debe comenzar la temporización si el punto extremo se encarga del cumplimiento del límite de duración de la llamada.

La estructura **GenericData (datos genéricos)** consta de un campo **id** para identificar los datos, y un campo **parameters** para transportar los parámetros efectivos.

La estructura **GenericIdentifier (identificador genérico)** permite identificar un objeto de diversas maneras.

La estructura **EnumeratedParameter (parámetro enumerado)** proporciona un parámetro genérico. Consta de un campo **id** para identificar el parámetro, y de un campo **content** para transportar cualquier dato asociado.

La estructura **Content (contenido)** soporta diversos tipos de datos, incluidos **raw**, **text**, **unicode**, **bool**, **number8**, **number16**, **number32**, **id**, **alias**, **transport**, **compound**, y **nested**. Esto permite una definición flexible de un parámetro genérico. El tipo **raw** proporciona un parámetro o conjunto de parámetros cuya estructura de datos real está definida en otro lugar; por ejemplo, podría consistir en ASN.1 codificada en PER, o datos en forma de tipo-longitud-valor, o podría ser un mensaje encapsulado de otro protocolo de señalización.

La estructura **FeatureSet (conjunto de características)** permite a una entidad especificar información de característica genérica. La entidad especifica el conjunto de características que

necesita para la compleción exitosa de la llamada, utilizando el campo **neededFeatures (características que se necesitan)**; especifica el conjunto de características que prefiere pero que no necesita utilizando el campo **desiredFeatures (características deseadas)**; y especifica el conjunto de características que soporta utilizando el campo **supportedFeatures (características soportadas)**. El BOOLEANO **replacementFeatureSet (conjunto de características sustitutivas)** se fija a VERDADERO para indicar que este conjunto de características sustituye a cualquier conjunto de características antes enviado, o a FALSO en otro caso.

La estructura **TransportChannelInfo (información de canal de transporte)** proporciona información sobre un canal de transporte de medios. El campo **sendAddress (dirección de envío)** es la dirección de transporte del emisor, y el campo **recvAddress (dirección de recepción)** es la dirección de transporte del receptor.

La estructura **RTPSession (sesión RTP)** proporciona la descripción de una sesión RTP. Contiene los siguientes campos:

- **rtpAddress (dirección rtp)** – Este campo proporciona las direcciones de emisión y de recepción del tren RTP.
- **rtcpAddress (dirección rtcp)** – Este campo proporciona la dirección de emisión y de recepción de los mensajes RTCP.
- **cname (nombre canónico)** – Este campo proporciona el CNAME especificado en la cláusula 6 y en el anexo A.
- **ssrc (fuente de sincronización)** – Este campo se utiliza para identificar la fuente de un tren RTP, como se describe en la cláusula 6 y en el anexo A.
- **sessionId (identificador de sesión)** – Este campo proporciona el identificador de esta sesión RTP, como se describe en la Rec. UIT-T H.245.
- **associatedSessionIds (identificadores de sesiones asociadas)** – Este campo proporciona los identificadores de las sesiones RTP asociadas, como se describe en la Rec. UIT-T H.245.
- **multicast (multidifusión)** – Este campo indica si se trata de una sesión de multidifusión.
- **bandwidth (anchura de banda)** – Este campo indica la anchura de banda utilizada para el tren en centenas de bits por segundo.

7.7 Soporte necesario de los mensajes RAS

El cuadro 22 muestra los mensajes RAS que son soportados por diferentes tipos de puntos extremos.

Cuadro 22/H.225.0 – Estado de los mensajes RAS

Mensajes RAS	Punto extremo (Tx)	Punto extremo (Rx)	Controlador de acceso (Tx)	Controlador de acceso (Rx)
RAS Message	**Endpoint (Tx)**	**Endpoint (Rx)**	**Gatekeeper (Tx)**	**Gatekeeper (Rx)**
GRQ	O			M
GCF		O	M	
GRJ		O	M	
RRQ	M			M
RCF		M	M	
RRJ		M	M	

Cuadro 22/H.225.0 – Estado de los mensajes RAS

Mensajes RAS	Punto extremo (Tx)	Punto extremo (Rx)	Controlador de acceso (Tx)	Controlador de acceso (Rx)
RAS Message	**Endpoint (Tx)**	**Endpoint (Rx)**	**Gatekeeper (Tx)**	**Gatekeeper (Rx)**
URQ	O	M	O	M
UCF	M	O	M	O
URJ	O	O	M	O
ARQ	M			M
ACF		M	M	
ARJ		M	M	
BRQ	M	M	O	M
BCF	M (nota 1)	M	M	O
BRJ	M	M	M	O
IRQ		M	M	
IRR	M			M
IACK		O	CM	
INAK		O	CM	
DRQ	M	M	O	M
DCF	M	M	M	M
DRJ	M (nota 2)	M	M	M
LRQ	O		O	M
LCF		O	M	O
LRJ		O	M	O
NSM	O	O	O	O
XRS	M	M	M	M
RIP	CM	M	CM	M
RAI	O			M
RAC		O	M	
SCI	O	O	O	O
SCR	O	O	O	O

M: Obligatorio (*mandatory*), O: Facultativo (*optional*), F: Prohibido (*forbidden*), CM: condicionalmente obligatorio (*conditionally mandatory*), en blanco: "No aplicable".

NOTA 1 – Si un controlador de acceso envía un mensaje BRQ por el que se solicita una velocidad más baja, el punto extremo responde con BCF si la velocidad más baja está soportada, y en los demás casos responde con BRJ. Si un controlador de acceso envía una BRQ por el que se solicita una velocidad más alta, el punto extremo puede responder con BCF o BRJ.

NOTA 2 – El terminal no enviará DRJ en respuesta a una DRQ válida recibida de su controlador de acceso.

7.8 Mensajes de descubrimiento de terminal y de pasarela

El mensaje GRQ pide que cualquier controlador de acceso que lo reciba responda con un GCF que le conceda permiso para registrar. El GRJ es un rechazo de esta petición que indica que el punto extremo solicitante debe buscar otro controlador de acceso.

7.8.1 Petición de controlador de acceso (GRQ, *gatekeeperRequest*)

Se señala que se envía a una GRQ por punto extremo lógico; así, una MCU o una pasarela podría mandar muchos.

El mensaje GRQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

protocolIdentifier (identificador de protocolo) – Identifica la antigüedad del envío del punto extremo según H.225.0.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

rasAddress (dirección ras) – Es la dirección de transporte que este punto extremo utiliza para mensajes de registro y de situación. El controlador de acceso enviará mensajes RAS a esta dirección y no a la dirección que envío el mensaje, a menos que no pueda descodificar **rasAddress**.

endpointType (tipo de punto extremo) – Especifica el tipo o tipos del punto extremo que está registrando (el bit MC no será fijado por él mismo).

gatekeeperIdentifier (identificador de controlador de acceso) – Cadena para identificar el controlador de acceso desde el que el terminal desearía recibir permiso para registrarse. Un **gatekeeperIdentifier** faltante o de cadena nula indica que el terminal está interesado en cualquier controlador de acceso disponible.

callServices (servicios de llamada) – Proporciona información sobre el soporte de protocolos opcionales de la serie Q para el controlador de acceso y el terminal llamado.

endpointAlias (alias de punto extremo) – Lista de direcciones de alias por la cual otros terminales pueden identificar este terminal.

alternateEndpoints (puntos extremos alternativos) – Secuencia de alternativas de puntos extremos prioritarios para **rasAddress**, **endpointType** o **endpointAlias**.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

authenticationCapability (capacidad de autenticación) – Indica los mecanismos de autenticación soportados por el punto extremo.

algorithmOIDs – Indica el conjunto completo de algoritmos de criptación soportados por el punto extremo.

integrity (integridad) – Indica al recibiente el mecanismo de integridad que se debe aplicar en los mensajes RAS.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación de mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta a todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor

coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

supportsAltGK (soporta controlador de acceso alternativo) – Indica si el punto extremo soporta el mecanismo de controlador de acceso alternativo.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características definidas fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para la tunelización de información de forma transparente mediante RAS.

7.8.2 Confirmación de controlador de acceso (GCF, *gatekeeperConfirm*)

El mensaje GCF incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Será el mismo valor que fue pasado en la GRQ.

protocolIdentifier (identificador de protocolo) – Identifica la antigüedad del controlador de acceso aceptador.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

gatekeeperIdentifier (identificador de controlador de acceso) – Cadena para identificar el controlador de acceso que está enviando la GCF.

rasAddress (dirección ras) – Dirección de transporte que el controlador de acceso utiliza para los mensajes de registro y situación.

alternateGatekeeper (controlador de acceso alternativo) – Secuencia de alternativas prioritarias para gatekeeperIdentifier y rasAddress.

authenticationMode (modo de autenticación) – Indica el mecanismo de autenticación que se ha de utilizar. El controlador de acceso elegirá el **authenticationMode** tomándolo de la **authenticationCapability** proporcionada por el punto extremo en GRQ.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

algorithmOID – Indica el algoritmo de criptación requerido por el controlador de acceso.

integrity (integridad) – Indica al recibiente el mecanismo de integridad que se debe aplicar en los mensajes RAS.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta a todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características definidas fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para la tunelización de información de forma transparente mediante RAS.

7.8.3 Rechazo de controlador de acceso (GRJ, *gatekeeperReject*)

El mensaje GRJ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Será el mismo valor que fue pasado en la GRQ.

protocolIdentifier (identificador de protocolo) – Identifica la antigüedad del controlador de acceso rechazante.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

gatekeeperIdentifier (identificador de controlador de acceso) – Cadena para identificar el controlador de acceso que está enviando el GRJ.

rejectReason (motivo del rechazo) – Codifica el motivo por el cual la GRQ fue rechazado por este controlador de acceso. Un motivo del tipo **genericDataReason (motivo datos genéricos)** indica que la petición fue rechazada como resultado de una característica o un elemento genéricos; en este caso, se pude especificar información adicional en el campo **genericData (datos genéricos)**.

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación de mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta a todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características definidas fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para la tunelización de información de forma transparente mediante RAS.

7.9 Mensajes de registro de terminal y de pasarela

El RRQ es una petición de registrar de un terminal a un controlador de acceso. Si éste responde con un RCF, el terminal utilizará el controlador de acceso respondedor para futuras llamadas. Si el controlador de acceso responde con un RRJ, el terminal debe buscar otro controlador de acceso en el que registrarse.

7.9.1 Petición de registro (RRQ, *registrationRequest*)

El mensaje RRQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

protocolIdentifier (identificador de protocolo) – Identifica la antigüedad del punto extremo emisor según H.225.0

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

discoveryComplete (descubrimiento completo) – Se pone a VERDADERO si el punto extremo solicitante ha precedido este mensaje con el procedimiento de descubrimiento de controlador de acceso; se pone a FALSO si se trata del registro solamente. Obsérvese que el registro puede envejecer y el punto extremo obtendrá un fallo en una RRQ o ARQ con un código de motivos de **discoveryRequired** o **notRegistered** respectivamente. Esto indica que el punto extremo debe efectuar el procedimiento de descubrimiento (dinámico o estático) antes de emitir RRQ con **discoveryComplete** puesto a VERDADERO.

callSignalAddress (dirección de señalización de llamada) – Es la dirección de transporte de señalización de llamada para este punto extremo. Si se soportan múltiples transportes, serán registrados inmediatamente.

rasAddress (dirección ras) – Es la dirección de transporte de registro y de situación para este punto extremo. El controlador de acceso enviará mensajes RAS a esta dirección y no a la dirección que envió el mensaje, a menos que no pueda descodificar **rasAddress**.

terminalType (tipo de terminal) – Especifica el tipo (o tipos) del punto extremo que se está(n) registrando; adviértase que el bit **mc** no será fijado por sí mismo; se fijará también el bit **terminal**, **mcu**, **gateway** o **gatekeeper**. Si se proporciona información **vendor**, ésta será idéntica a la proporcionada en **endpointVendor**. Si el **terminalType** es **gateway** o **mcu**, el valor **supportedPrefixes** facultativo es una lista de direcciones de prefijos por las cuales otros puntos extremos pueden identificar los protocolos RCC y las velocidades de datos que soporta esta entidad. Este campo puede utilizarse además de **terminalAlias** y **terminalAliasPattern** o como una alternativa a los mismos. Todos los prefijos soportados del punto extremo se incluirán en cada RRQ, a menos que se haya especificado la opción **additiveRegistration**, en cuyo caso los prefijos soportados en una RRQ se añadirán a la lista de prefijos registrados actualmente para el punto extremo. Con la RRQ aditivo, se considerará que los prefijos soportados ya registrados en este punto extremo están registrados todavía. Se señala que los prefijos no forman parte de un **PartyNumber (número de parte)** (E.164 u otros). Para registrar un **PartyNumber** (o una gama o esquema de los mismos), el punto extremo deberá utilizar los campos **terminalAlias (alias de terminal)** y **terminalAliasPattern (esquema de alias de terminal)** que se describen más adelante.

terminalAlias (alias de terminal) – Este valor opcional es una lista de direcciones de alias mediante las cuales otros terminales pueden identificar este terminal. Este campo puede utilizarse además de los campos **terminalAliasPattern** y **supportedPrefixes** o como una alternativa a los mismos. Si **terminalAlias** es nulo, el controlador de acceso puede asignar una dirección **terminalAlias** e incluirla en la RCF. Si un **identificador de correo electrónico** está disponible para el punto extremo, deberá registrarse. Adviértase que múltiples direcciones de alias pueden hacer referencia a las mismas direcciones de transporte. Todos los alias del punto extremo que éste desea registrar se incluirán en esta lista, a menos que se haya especificado la opción **additiveRegistration**, en cuyo caso los alias de punto extremo en una RRQ se añadirán a la lista de alias actualmente registrados para el punto extremo.

gatekeeperIdentifier (identificador de controlador de acceso) – Cadena para identificar el controlador de acceso en el que el terminal desea registrarse.

endpointVendor (vendedor de punto extremo) – Información sobre el vendedor de punto extremo.

alternateEndpoints (puntos extremos alternativos) – Secuencia de alternativas de puntos extremos prioritarios para **callSignalAddress**, **rasAddress**, **terminalType** o **terminalAlias**.

timeToLive (tiempo de vida) – Duración de la validez del registro, en segundos, transcurrida la cual el controlador de acceso puede considerar que el registro ha caducado.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

keepAlive (mantener vivo) – Si está fijado a VERDADERO, indica que el punto extremo ha enviado esta RRQ como un mensaje de "mantener vivo". Un punto extremo puede enviar una RRQ ligero que conste únicamente de **rasAddress**, **keepAlive**, **endpointIdentifier**, **gatekeeperIdentifier**, **tokens** y **timeToLive**. Cuando un controlador de acceso reciba una RRQ con un campo **keepAlive** fijado a VERDADERO ignorará los campos que no sean **endpointIdentifier**, **gatekeeperIdentifier**, **tokens** y **timeToLive**. El campo **rasAddress** en un mensaje RRQ será únicamente utilizado por un controlador de acceso como el destino para un RRJ cuando el punto extremo no se registra.

endpointIdentifier (identificador de punto extremo) – **Identificador de punto extremo** proporcionado por el controlador de acceso durante la RCF original.

willSupplyUUIEs (proporcionará UUIE) – Si está fijado a VERDADERO, indica que el punto extremo suministrará información sobre el mensaje de señalización de llamada H.225.0 en mensajes IRR, si lo solicita el controlador de acceso.

maintainConnection (mantener conexión) – Si es VERDADERO, indica que el emisor del mensaje puede soportar una conexión de señalización cuando ninguna llamada no se selecciona actualmente a través de la conexión.

alternateTransportAddresses (direcciones de transporte alternativas) – Este campo lleva direcciones de señalización de llamada diferentes de TCP. La inclusión de una dirección indica el soporte del transporte correspondiente.

additiveRegistration (registro aditivo) – Si está presente, este campo indica que este mensaje es una RRQ "aditiva", lo que significa que el punto extremo ha enviado esta RRQ como una adición de información a un registro existente. Un punto extremo puede enviar una RRQ aditiva constituida únicamente por **callSignalAddress**, **rasAddress**, **terminalType**, **terminalAlias**, **terminalAliasPattern**, **alternateEndpoints**, **endpointIdentifier**, **gatekeeperIdentifier** y **tokens**. Un controlador de acceso que recibe una RRQ con el campo **additiveRegistration** presente pasará por alto los campos que sean diferentes de éste. Un controlador de acceso utilizará la **rasAddress** en una RRQ aditiva como el destino para el RRJ siguiente si el punto extremo no está registrado o si el **terminalAlias** y/o **terminalAliasPattern** no se ajusta a la política de registro del controlador de acceso.

terminalAliasPattern (esquema de alias de terminal) – Este valor facultativo es una lista de esquemas de dirección que especifican alias y direcciones mediante las cuales otros puntos extremos pueden identificar este punto extremo. Este campo puede utilizarse como una adición o alternativa a los campos **terminalAlias** y **supportedPrefixes**. Todos los alias y direcciones del punto extremo se incluirán en cada RRQ a menos que la opción **additiveRegistration** sea VERDADERO, en cuyo caso los alias y direcciones de punto extremo en la RRQ se añadirán a la lista de alias actualmente registrados para el punto extremo.

supportsAltGK (soporta controlador de acceso alternativo) – Indica si el punto extremo soporta el mecanismo de controlador de acceso alternativo.

usageReportingCapability (capacidad de comunicar información de utilización) – Este campo puede ser incluido por el punto extremo para dar a conocer su aptitud para tomar y comunicar diversos tipos de información de utilización.

multipleCalls (múltiples llamadas) – Si es VERDADERO, indica que el emisor del mensaje puede señalizar múltiples llamadas a través de una sola conexión de señalización de llamadas.

supportedH248Packages (lotes H248 soportados) – Este campo indica una lista de lotes H.248 soportados por este punto extremo.

callCreditCapability (capacidad de crédito de llamada) – Este campo describe ciertas capacidades de este punto extremo relacionadas con la facturación.

capacityReportingCapability (capacidad de informes de capacidades) – Este campo indica la aptitud de un punto extremo para comunicar información de capacidad de llamada.

capacity (capacidad) – Este campo indica la capacidad máxima y la capacidad actual de llamada del punto extremo. Cuando envíe este campo, el punto extremo deberá incluir los elementos **maximumCallCapacity (capacidad de llamada máxima)** y **currentCallCapacity (capacidad de llamada actual)**.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

restart (reinicio) – Si está activado, este campo indica que es el primer mensaje RRQ enviado por un punto extremo después del rearranque o de un evento anormal que ha originado la pérdida de sus llamadas. Esto permite al controlador de acceso realizar cualquier limpieza o función que sea necesaria.

supportsACFSequences (soporta secuencias ACF) – Si está activado, este campo indica que el punto extremo es capaz de recibir y procesar una secuencia de mensajes ACF en respuesta a un único mensaje ARQ.

7.9.2 Confirmación de registro (RCF, *registrationConfirm*)

El mensaje RCF incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la RRQ.

protocolIdentifier (identificador de protocolo) – Identifica la antigüedad del controlador de acceso aceptador.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

callSignalAddress (dirección de señalización de llamada) – Es una formación de direcciones de transporte para mensajes de señalización de llamada H.225.0; una para cada transporte al que responderá el controlador de acceso. Esta dirección incluye el identificador de TSAP.

terminalAlias (alias de terminal) – Este valor facultativo es una lista de direcciones de alias mediante las cuales otros terminales pueden identificar este terminal. Este campo puede utilizarse además de los campos **terminalAliasPattern** y **supportedPrefixes** o como una alternativa a los mismos. Especifica las direcciones de alias que han sido aceptadas entre las propuestas en el mensaje RRQ asociado. Si no se propuso ninguna en la RRQ, la lista da los alias asignados por el controlador de acceso. Si este campo no está incluido, y en el mensaje RRQ se propusieron direcciones de alias, indica que el controlador de acceso ha aceptado todas las direcciones de alias

propuestas. Si este campo está incluido y especifica un subconjunto de direcciones de alias propuestas en la RRQ, indica que el controlador de acceso ha aceptado únicamente estas direcciones.

gatekeeperIdentifier (identificador de controlador de acceso) – Cadena para identificar el controlador de acceso que ha aceptado el registro del terminal.

endpointIdentifier (identificador de punto extremo) – Cadena de identidad de terminal asignada por un controlador de acceso; se devolverá en eco en mensajes RAS subsiguientes.

alternateGatekeeper (controlador de acceso alternativo) – Secuencia de alternativas prioritarias para **gatekeeperIdentifier** y **rasAddress**.

timeToLive (tiempo de vida) – Duración de la validez del registro, en segundos, transcurrida la cual el controlador de acceso puede considerar que el registro ha caducado.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

willRespondToIRR (responderá a IRR) – Es verdadero si el controlador de acceso envía un mensaje IACK o INAK en respuesta a un mensaje IRR no solicitado con su campo **needsResponse** fijado a VERDADERO.

preGrantedARQ (ARQ concedido previamente) – Indica eventos cuya admisión ha concedido previamente el controlador de acceso. Esto permite tiempos de establecimiento de la comunicación más breves en entornos en los que la admisión está garantizada por medios distintos del intercambio ARQ/ACF. Obsérvese que incluso si estos campos están fijados en VERDADERO, un punto extremo puede todavía enviar una ARQ al controlador de acceso por razones tales como la traducción de dirección, o porque el punto extremo no soporta este modo de señalización modificado. Si la secuencia de **preGrantedARQ** no está presente, la señalización ARQ se utilizará en todos los casos. Los campos son:

- **makeCall (efectuar llamada)** – Si la bandera **makeCall** es VERDADERO, el controlador de acceso ha concedido permiso previamente al punto extremo para iniciar llamadas sin enviar primero una ARQ. Si la bandera **makeCall** es FALSO, el punto extremo deberá enviar siempre una ARQ a fin de obtener permiso para efectuar una llamada.
- **useGKCallSignalAddressToMakeCall (utilizar dirección de señalización de llamada GK para efectuar llamada)** – Si las banderas **makeCall** y **useGKCallSignalAddressToMakeCall** están fijadas ambas en VERDADERO, y el punto extremo no envía entonces una ARQ al controlador de acceso para efectuar una llamada, dicho punto deberá enviar la señalización de todas las llamadas H.225.0 al canal de señalización de llamada del controlador de acceso.
- **answerCall (responder a llamada)** – Si la bandera **answerCall** es VERDADERO, el controlador de acceso ha concedido permiso previamente al punto extremo para responder a llamadas sin enviar primero una ARQ. Si la bandera **answerCall** es FALSO, el punto extremo deberá enviar siempre una ARQ a fin de obtener permiso para responder a una llamada.

- **useGKCallSignalAddressToAnswer (utilizar dirección de señalización de llamada GK para responder)** – Si las banderas **answerCall** y **useGKCallSignalAddressToAnswer** están fijadas ambas en VERDADERO y un punto extremo no envía entonces una ARQ al controlador de acceso para responder a una llamada, dicho punto velará por que la señalización de todas las llamadas H.225.0 provenga del controlador de acceso. Si se ha ordenado a un punto extremo que utilice el controlador de acceso cuando responda a una llamada, pero no sabe si una llamada entrante proviene del controlador de acceso (lo que quizás implique observar la dirección de transporte), el punto extremo emitirá un ARQ independientemente del estado en que esté la bandera **useGKCallSignalAddressToAnswer**.
- **irrFrequencyInCall (frecuencia del irr en la llamada)** – Este campo indica la frecuencia, en segundos, de los mensajes IRR enviados al controlador de acceso cuando el punto extremo está en una o más llamadas. Si no está presente, el controlador de acceso no desea mensajes IRR no solicitados. Cuando el punto extremo envía esos mensajes IRR, el valor de referencia de llamada será único para el terminal, como hubiera sido generado en una petición de admisión. Sin embargo, éste no es CRV "normal" y no se puede reutilizar para nueva comunicación (DRQ, IRQ o BRQ). El identificador de llamada será el mismo que el utilizado en los mensajes del canal de señalización de llamada para la llamada pertinente.
- **totalBandwidthRestriction (restricción de anchura de banda total)** – Este campo limita la utilización total de la anchura de banda para el punto extremo cuando se encuentra en llamada. Si no está presente, no hay una restricción de anchura de banda constante.
- **alternateTransportAddresses (direcciones de transporte alternativo)** – Este campo lleva direcciones de señalización de llamada para transportes diferentes de TCP. La inclusión de una dirección indica el soporte del transporte correspondiente.
- **useSpecifiedTransport (usar transporte especificado)** – Este campo permite al controlador de acceso ordenar al punto extremo que utilice un determinado protocolo de transporte de señalización para marcar llamadas. Si se incluye este campo y el transporte especificado no es **tcp**, las **alternateTransportAddresses** se incluirán también en este mensaje.

maintainConnection (mantener conexión) – Si es VERDADERO, indica que el controlador de acceso (en el caso de encaminamiento de control de acceso) puede soportar una conexión de señalización cuando ninguna llamada está señalizada actualmente en la conexión.

serviceControl (control de servicio) – Contiene datos específicos de servicio o información de direccionamiento que el punto extremo puede utilizar para comunicación de control de servicio no relacionada con la llamada, como se describe, por ejemplo, en el anexo K/H.323.

supportsAdditiveRegistration (soporta registro aditivo) – Si está presente, este campo indica que el controlador de acceso soporta capacidades de registro aditivo. Si no está presente, el controlador de acceso no soporta registro aditivo.

terminalAliasPattern (esquema de alias de terminal) – Este valor facultativo es una lista de esquemas de dirección que especifican alias y direcciones mediante las cuales otros puntos extremos pueden identificar este punto extremo. Este campo puede utilizarse como una adición o alternativa a los campos **terminalAlias** y **supportedPrefixes**. Especifica los alias y direcciones que han sido aceptados entre los propuestos en el mensaje RRQ asociado. Si no se propuso ninguno en la RRQ, la lista indica alias y direcciones asignados por el controlador de acceso. Si este campo no está incluido y en el mensaje RRQ se propusieron direcciones de alias, indica que el controlador de acceso ha aceptado todos los esquemas propuestos. Si este campo está incluido y especifica un subconjunto de esquemas de dirección propuestos en la RRQ, indica que el controlador de acceso ha aceptado únicamente estos esquemas.

supportedPrefixes (prefijos soportados) – Este valor facultativo es una lista de prefijos mediante los cuales otros puntos extremos pueden identificar este punto extremo. Este campo puede utilizarse como una adición o alternativa a los campos **terminalAlias** y **terminalAliasPattern**. Especifica los prefijos de dirección que han sido aceptados entre los propuestos en el mensaje RRQ asociado. Si no se propuso ninguno en la RRQ, la lista indica prefijos asignados por el controlador de acceso. Si este campo no está incluido y en el mensaje RRQ se propusieron prefijos de dirección, indica que el controlador de acceso ha aceptado todos los prefijos propuestos. Si este campo está incluido y especifica un subconjunto de prefijos de dirección propuestos en la RRQ, indica que el controlador de acceso ha aceptado únicamente estos prefijos.

usageSpec (especificación de utilización) – Este campo puede incluirlo el controlador de acceso para pedir al punto extremo que tome y comunique la información de utilización de llamada indicada en los instantes especificados.

featureServerAlias (alias de servidor de características) – Este campo se reserva para su futura utilización por el UIT-T en un protocolo basado en estímulo.

capacityReportingSpec (especificación de informes de capacidad) – Este campo indica el tipo de información de capacidad de llamada que un punto extremo debe comunicar.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.9.3 Rechazo de registro (RRJ, *registrationReject*)

El mensaje RRJ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la RRQ.

protocolIdentifier **(identificador de protocolo)** – Identifica la antigüedad del controlador de acceso rechazante.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

rejectReason (motivo del rechazo) – Motivo del rechazo del registro. Este campo puede contener un valor **invalidTerminalAliases**, en cuyo caso contiene una lista de alias, direcciones y prefijos soportados que, en el mensaje RRQ asociado, se determinó que no eran válidos. En cualquier caso, todos los alias, direcciones y prefijos soportados del mensaje RRQ asociado son rechazados junto con los especificados en el campo **invalidTerminalAliases**. Un motivo del tipo **genericDataReason (motivo datos genéricos)** indica que la petición fue rechazada como resultado de una característica o un elemento genéricos; en este caso, se puede especificar información adicional en el campo **genericData (datos genéricos)**.

gatekeeperIdentifier (identificador de controlador de acceso) – Cadena para identificar el controlador de acceso que ha rechazado el registro del terminal.

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.10 Mensajes de desregistro de terminal/controlador de acceso

7.10.1 Petición de desregistro (URQ, *unregistrationRequest*)

La URQ solicita que se interrumpa la asociación entre un terminal y un controlador de acceso. Adviértase que ese registro es bidireccional; es decir, un controlador de acceso puede pedir a un terminal que se considere a sí mismo desregistrado, y un terminal puede informar a un controlador de acceso que está revocando un registro anterior.

El mensaje URQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

callSignalAddress (dirección de señalización de llamada) – Una o más de las direcciones de señalización de llamada de transporte para este punto extremo que han de ser desregistradas.

endpointAlias (alias de punto extremo) – Este valor facultativo es una lista de direcciones de alias, mediante las cuales otros terminales pueden identificar este terminal. Este campo puede ser utilizado como una adición o alternativa a los campos **endpointAliasPattern** y **supportedPrefixes**. Si este campo, el campo **endpointAliasPattern** y el campo **supportedPrefixes** no están presentes, todos los alias son desregistrados en un solo mensaje. Si el valor **dialledDigits** ha sido asignado, debe estar presente. Sólo se desregistran los valores aquí indicados; esto permite, por ejemplo, desregistrar un **h323-ID** mientras y dejar registrado el valor **dialledDigits**.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

endpointIdentifier (identificador de punto extremo) – Confirmación de identidad; no es enviado por el controlador de acceso.

alternateEndpoints (puntos extremos alternativos) – Secuencia de alternativas de puntos extremos prioritarios para **callSignalAddress** o **endpointAlias**.

gatekeeperIdentifier (identificador de controlador de acceso) – Un **gatekeeperIdentifier** que el punto extremo recibió en la lista de **alternateGatekeeper** en un mensaje RCF proveniente del controlador de acceso cuando se registró, o en un mensaje URJ anterior.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de

integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

reason (motivo) – Se utiliza cuando el controlador de acceso envía el mensaje URQ para indicar por qué considera desregistrado el punto extremo. Un **reason** de **maintenance** indica que el controlador de acceso o punto extremo se desactiva para mantenimiento.

endpointAliasPattern (esquema de alias de punto extremo) – Este valor facultativo es una lista de esquemas de dirección que especifican alias y direcciones mediante los cuales otros puntos extremos pueden identificar este punto extremo. Este campo puede utilizarse como una adición o alternativa a los campos **endpointAlias** y **supportedPrefixes**. Si este campo, el campo **endpointAlias** y el campo **supportedPrefixes** no están presentes, todos los alias y direcciones son desregistrados en un solo mensaje. En otro caso, sólo los valores aquí indicados son desregistrados.

supportedPrefixes (prefijos soportados) – Este valor facultativo es una lista de prefijos mediante los cuales otros puntos extremos pueden identificar este punto extremo. Este campo puede utilizarse como una adición o alternativa a los campos **terminalAlias** y **terminalAliasPattern**. Si este campo, el campo **endpointAlias** y el campo **endpointAliasPattern** no están presentes, todos los alias y direcciones son desregistrados en un solo mensaje. En otro caso, sólo los valores aquí indicados son desregistrados.

alternateGatekeeper (controlador de acceso alternativo) – Secuencia de alternativas prioritarias para **gatekeeperIdentifier** y **rasAddress**.

genericData (**datos genéricos**) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.10.2 Confirmación de desregistro (UCF, *unregistrationConfirm*)

El mensaje UCF incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la URQ.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.10.3 Rechazo de desregistro (URJ, *unregistrationReject*)

El mensaje URJ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la URQ.

rejectReason (motivo del rechazo) – Motivo del rechazo del registro.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.11 Mensajes de admisión de terminal a controlador de acceso

El mensaje ARQ solicita que a un punto extremo le sea permitido el acceso a la red de paquetes por el controlador de acceso, que concede la petición con una ACF o la deniega con un ARJ.

7.11.1 Petición de admisión (ARQ, *admissionRequest*)

El mensaje ARQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

callType (tipo de llamada) – Utilizando este valor, el controlador de acceso puede intentar determinar la utilización de anchura de banda "real". El valor por defecto es **pointToPoint** para todas las llamadas. Debe reconocerse que el tipo de llamada puede cambiar dinámicamente durante la misma, y que el tipo de llamada final puede no ser conocido cuando se envía la ARQ.

callModel (modelo de llamada) – Si es **direct**, el punto extremo es solicitando el modelo de llamada directo de terminal a terminal. Si es **gatekeeperRouted**, el punto extremo está solicitando el modelo mediado por el controlador de acceso. No es necesario que el controlador de acceso acceda a esta petición.

endpointIdentifier (identificador de punto extremo) – Es un identificador de punto extremo que fue asignado al terminal por RCF.

destinationInfo (información de destino) – Secuencia de direcciones de alias para el destino, tales como **dialledDigits**, **PartyNumber** (**e164number** o **privateNumber**) o **h323-ID**. Cuando se envía el ARQ para responder a una llamada, **destinationInfo** indica el destino de la llamada (el punto extremo que responde). Si en un controlador de acceso se registra al menos un alias y en la ARQ no

se registran dos alias a distintas personas, el controlador de acceso reconocerá la ARQ como referente a la identidad registrada. En el caso de alias en conflicto se rechazará la petición de admisión con la causa **AliasesInconsistent**. Si el controlador de acceso no proporciona esta validación, considerará que el destino es la primera dirección registrada.

destCallSignalAddress (dirección de señalización de llamada de destino) – Dirección de transporte utilizada en el destino para la señalización de llamada.

destExtraCallInfo (información de llamada suplementaria de destino) – Contiene direcciones externas para múltiples llamadas.

srcInfo (información scr) – Secuencia de direcciones de alias para el punto extremo de origen, tales como **dialledDigits**, **PartyNumber** (**e164number** o **privateNumber**) o **h323-ID**. Cuando se envía la ARQ para responder a una llamada, **srcInfo** indica el originador de la llamada.

srcCallSignalAddress (dirección de señalización de llamada scr) – Dirección de transporte utilizada en el origen para la señalización de llamada.

bandWidth (anchura de banda) – La anchura de banda bidireccional solicitada para la llamada en unidades de 100 bits por segundo. Por ejemplo, una llamada de 128 kbit/s se señalizaría como una petición de 256 kbit/s. El valor se refiere sólo a la velocidad binaria de audio y de vídeo, incluidos encabezamientos y tara.

callReferenceValue (valor de referencia de llamada) – El CRV de los mensajes de señalización de llamada H.225.0 para esta llamada; sólo tiene validez local. Lo utiliza un controlador de acceso para asociar la ARQ con una determinada llamada.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

callServices (servicios de llamada) – Proporciona información sobre el soporte de protocolos facultativos de la serie Q para el controlador de acceso y el terminal llamado.

conferenceID (ID de conferencia) – Identificador de conferencia exclusivo.

activeMC – Si es VERDADERO, la parte llamante tiene un MC activo; en los demás casos, es FALSO.

answerCall – Se utiliza para indicar a un controlador de acceso que la llamada es una llamada entrante.

canMapAlias (puede copiar alias) – Si está fijado a VERDADERO, indica que si la ACF resultante contiene los campos **destinationInfo**, **destExtraCallInfo** y/o **remoteExtensionAddress**, el punto extremo copiará esta información en los campos **destinationAddress**, **destExtraCallInfo** y **remoteExtensionAddress**, respectivamente, del mensaje Establecimiento, o en el IE número de la parte llamada, si procede. Si el punto extremo es una pasarela utilizada para salir de la red H.323, la pasarela convertirá la información de destino en el formato de señalización apropiado fuera de la red H.323 (por ejemplo, DTMF). Si el controlador de acceso reemplaza la información de direccionamiento de la ARQ y **canMapAlias** es FALSO, deberá rechazar la ARQ. Los sistemas conformes a H.225.0 versión 4 y posteriores fijarán este campo a VERDADERO.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

srcAlternatives (alternativas src) – Secuencia de alternativas de punto extremo de origen prioritarias para **srcInfo**, **srcCallSignalAddress**, o **rasAddress**.

destAlternatives (alternativas de destino) – Secuencia de alternativas de punto extremo de destino prioritarias para **destinationInfo** o **destCallSignalAddress**.

gatekeeperIdentifier (identificador de controlador de acceso) – Un **gatekeeperIdentifier** que el punto extremo recibió en la lista de **alternateGatekeeper** en un mensaje RCF proveniente del controlador de acceso cuando se registró o en un mensaje ARJ anterior.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

transportQOS (calidad de servicio de transporte) – Puede ser utilizado por un punto extremo para indicar su capacidad para reservar recursos de transporte. La estructura de TransportQOS incluye lo siguiente:

- **endpointControlled (controlado por punto extremo)** – El punto extremo aplicará su propio mecanismo de reserva.
- **gatekeeperControlled (controlado por controlador de acceso)** – El controlador de acceso efectuará la reserva de recursos en nombre del punto extremo.
- **noControl (sin control)** – No es necesaria ninguna reserva de recursos.

willSupplyUUIEs (suministrará UUIE) – Si está fijado a VERDADERO, indica que el punto extremo suministrará información de mensaje de señalización de llamada H.225.0 en mensajes IRR, si la solicita el controlador de acceso.

callLinkage (vinculación de llamada) – El contenido de este campo suele ser controlado por un servicio de vinculación de llamada. Para los procedimientos y semántica de este campo, véase la cláusula 10/H.323.

gatewayDataRate (velocidad de datos de pasarela) – La velocidad de datos solicitada para el lado RCC de una llamada a través de una pasarela. Esta velocidad de datos, si está presente, será igual a la velocidad de datos especificada en el IE capacidad portadora del mensaje Establecimiento. Un controlador de acceso podría utilizar este campo en la selección de una pasarela para el tratamiento de la llamada.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor en un instante dado, suponiendo que el controlador de acceso confirma la ARQ enviando una ACF. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity**.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos utilizados para la llamada.

desiredProtocols (protocolos deseados) – Identifica el tipo de protocolos, por orden de preferencia, que el punto extremo desea para su llamada (por ejemplo, voz y fax). Una entidad de resolución puede utilizar este campo para localizar un punto extremo que también soporte el protocolo, teniendo en cuenta el orden de preferencia.

desiredTunnelledProtocol (protocolo tunelizado deseado) – Este campo identifica un protocolo cuya tunelización se solicita.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

canMapSrcAlias (puede transcribir Alias Src) – Si está fijado a VERDADERO, indica que si el mensaje ACF resultante contiene el campo **modifiedSrcInfo**, el punto extremo copiará esta información en el campo **sourceInfo** del mensaje Establecimiento y/o en el IE número de la parte llamante, si procede. Si el controlador de acceso reemplaza la información de direccionamiento de la ARQ y **canMapSrcAliases** es FALSO, deberá rechazar la ARQ.

NOTA – Tanto **destinationInfo** como **destCallSignalAddress** son facultativos; no obstante, cuando el punto extremo no esté respondiendo a una llamada, al menos uno de los dos estará presente. No hay una regla absoluta sobre cuál de los dos deberá preferirse, lo que puede depender de la ubicación; no obstante, debe proporcionarse la dirección si está disponible. Se advierte que los mejores resultados se obtendrán considerando la naturaleza de los protocolos de transporte que se estén utilizando.

7.11.2 Confirmación de admisión (ACF, *admissionConfirm*)

El mensaje ACF incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Será el mismo valor que fue pasado en la ARQ.

bandWidth (anchura de banda) – La máxima anchura de banda permitida para la llamada; puede ser menor que la solicitada.

callModel (modelo de llamada) – Dice al terminal si la señalización de llamada enviada en **destCallSignalAddress** va a un controlador de acceso o a un terminal. Un valor de **gatekeeperRouted** indica que la señalización de llamada se está pasando a través del controlador de acceso, mientras que **direct** indica que está en uso el modo llamada de punto extremo a punto extremo.

destCallSignalAddress (dirección de respuesta) – La dirección de transporte a la que se envía señalización de llamada H.225.0, pero puede ser una dirección de punto extremo o de controlador de acceso según el modelo de llamada en uso.

irrFrequency (frecuencia irr) – La frecuencia, en segundos, con que el terminal enviará IRR al controlador de acceso mientras está en una llamada, incluido cuando está en retención. Si no está presente, el punto extremo no envía IRR mientras está activa en una llamada, y se cree que el controlador de acceso interrogará secuencialmente el punto extremo.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

destinationInfo (información de destino) – Dirección del canal inicial utilizada cuando se efectúa una llamada a través de una pasarela.

destExtraCallInfo (información de llamada extra de destino) – Necesario para efectuar posibles llamadas de canal adicional, es decir, para una llamada 2 × 64 kbit/s en el lado RCC. Sólo contendrá direcciones **dialledDigits** o **PartyNumber**, y no contendrá el número del canal inicial.

destinationType (tipo de destino) – Especifica el tipo del punto extremo de destino.

remoteExtensionAddress (dirección de extensión distante) – Contiene la dirección de alias de un punto extremo llamado en los casos en que es necesaria esta información para atravesar múltiples pasarelas.

alternateEndpoints (puntos extremos alternativos) – Secuencia de alternativas de puntos extremos prioritarios para **destCallSignalAddress** o **destinationInfo**.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

transportQOS (calidad de servicio de transporte) – El controlador de acceso puede indicar al punto extremo qué entidad se ocupa de la reserva de recursos. Si el controlador de acceso recibió **TransportQOS** en ARQ, incluirá entonces **transportQOS** (posiblemente modificado según la implementación del controlador de acceso) en ACF.

willRespondToIRR (responderá a IRR) – VERDADERO si el controlador de acceso envía un mensaje IACK o INAK en respuesta a un mensaje IRR no solicitado cuando el campo **needsResponse** de IRR está fijado a VERDADERO.

uuiesRequested (uuie solicitadas) – El controlador de acceso puede solicitar al punto extremo que notifique al controlador de acceso los mensajes de señalización de llamada H.225.0 que el punto extremo envía o recibe si el punto extremo indicó esta capacidad en la ARQ fijando **willSupplyUUIEs** en VERDADERO. **uuiesRequested** indica el conjunto de mensajes de señalización de llamada H.225.0 que el punto extremo notificará al controlador de acceso.

language (idioma) – Indica el o los idiomas en que el usuario desea recibir anuncios y avisos. El campo contiene uno o más rótulos de idioma que satisfacen la norma RFC 1766.

alternateTransportAddresses (direcciones de transporte alternativas) – Este campo lleva direcciones de señalización de llamada para transportes diferentes de TCP. La inclusión de una dirección indica el soporte del transporte correspondiente.

useSpecifiedTransport (usar transporte especificado) – Este campo permite al controlador de acceso ordenar al punto extremo que utilice un determinado protocolo de transporte de señalización para marcar la llamada. Si se incluye este campo y el transporte especificado no es **tcp**, las **alternateTransportAddresses** se incluirán también en este mensaje.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos RCC utilizados para la llamada. Por ejemplo, permite a un controlador de acceso ordenar a una pasarela de salida que seleccione determinadas facilidades RCC que habrán de utilizarse en la llamada.

usageSpec (especificación de utilización) – El controlador de acceso puede incluir este campo para pedir al punto extremo que tome y comunique información de utilización en los instantes especificados de la llamada en cuestión.

supportedProtocols (protocolos soportados) – Este campo indica los protocolos soportados por el punto extremo de destino.

serviceControl (control de servicio) – Este campo contiene datos específicos de servicio, o referencias a los mismos, que podrían ser utilizados por un punto extremo (por ejemplo, un mensaje que se aplicará al llamante) como se describe, por ejemplo, en el anexo K/H.323.

multipleCalls (múltiples llamadas) – Si es VERDADERO, este campo indica que el punto extremo de destino puede señalizar múltiples llamadas por una sola conexión de señalización de llamada. Si es FALSO, el punto extremo de destino no tiene esta capacidad. Si este campo está ausente, el controlador de acceso no sabe si el punto extremo distante tiene esta capacidad.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada en cuestión.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

modifiedSrcInfo (información Src modificada) – Direcciones de alias que deberán utilizarse para el punto extremo de origen, como **dialledDigits**, **PartyNumber** (**e164Number** o **privateNumber**) o los **h323-ID**. Este campo deberá utilizarse cuando la dirección de alias del punto extremo llamante se traduce/modifica al intentar encaminar la llamada a su destino primario o a cualquier punto extremo alternativo. El punto extremo deberá utilizar estas direcciones únicamente para esta llamada.

7.11.3 Rechazo de admisión (ARJ, *admissionReject*)

El mensaje ARJ incluye lo siguiente:

requestSeqNum (número esencial de petición) – Será el mismo valor que fue pasado en la ARQ.

RejectReason (motivo del rechazo) – Indica el motivo por el que se denegó la petición de admisión. Se señala que el campo **rejectReason** de **routeCallToSCN** es una opción adecuada sólo cuando el ARJ está dirigido a una pasarela de ingreso (la ARQ fue enviada por una pasarela y el BOOLEANO **answerCall** en la ARQ es FALSO). Si **rejectReason** es **routeCallToSCN**, el campo **rejectReason** para esta opción también incluye un número de teléfono, o lista de números de teléfono, al cual la pasarela puede redirigir la llamada en la RCC si soporta tal procedimiento. Si **rejectReason** es **exceedsCallCapacity**, el controlador de acceso ha determinado que el destino no tiene la capacidad de aceptar esta llamada en este momento. Un **rejectReason** de **collectDestination** indica que el controlador de acceso solicita que la pasarela tome la dirección de destino final, y que el campo **serviceControl** del ARJ indique la invitación que habrá de presentarse al usuario. Un **rejectReason** de **collectPIN** indica que el controlador de acceso solicita que la pasarela tome un número de identificación personal o código de autorización, y que el campo **serviceControl** del ARJ indique la invitación que habrá de presentarse al usuario. Un motivo del tipo **genericDataReason (motivo datos genéricos)** indica que la petición fue rechazada como resultado de una característica o un elemento genéricos; en este caso, se puede especificar información adicional en el campo **genericData**. El punto extremo deberá volver a registrarse en el controlador de acceso si recibe un error **invalidEndpointIdentifier**.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

callSignalAddress (dirección de señalización de llamada) – Es la dirección de señalización de llamada del controlador de acceso devuelta cuando el motivo del rechazo es **routeCallToGatekeeper**.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor

coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

serviceControl (control de servicio) – Este campo contiene datos específicos de servicio, o referencias a los mismos, que podrían ser utilizados por un punto extremo (por ejemplo, para visualizar el motivo por el cual fracasó la llamada) como se describe, por ejemplo, en el anexo K/H.323.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada en cuestión.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.12 Peticiones de terminal a controlador de acceso de cambios de anchura de banda

El mensaje BRQ pide que a un punto extremo le sea concedido un cambio en la asignación de anchura de banda LAN por el controlador de acceso, que concede la petición con una BCF o la deniega con un BRJ.

El controlador de acceso puede solicitar que un punto extremo eleve o reduzca la anchura de banda en uso con una BRQ. Si la petición es de elevar la velocidad, el punto extremo puede responder con un BRJ o BCF. Si lo que se pide es una velocidad inferior, el punto extremo responderá con una BCF si la velocidad inferior es soportada, sino con BRJ.

7.12.1 Petición de anchura de banda (BRQ, *bandwidthRequest*)

El mensaje BRQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

endpointIdentifier (identificador de punto extremo) – Es un identificador de punto extremo que fue asignado al terminal por RCF.

conferenceID (ID de conferencia) – ID de la llamada a la que tiene que cambiarse la anchura de banda.

callReferenceValue (valor de referencia de llamada) – El CRV de los mensajes de señalización de llamada H.225.0 para esta llamada; sólo tiene validez local. Es utilizado por un controlador de acceso para asociar la BRQ con una determinada llamada.

callType (tipo de llamada) – Mediante este valor, el controlador de acceso puede intentar determinar la utilización de anchura de banda "real".

bandWidth (anchura de banda) – La nueva anchura de banda bidireccional solicitada para la llamada en unidades de 100 bits por segundo. Es un valor absoluto que incluye sólo trenes de bits de audio y de vídeo sin contar encabezamientos ni tara. Los trenes multidifusión únicos sólo añadirán a la utilización de anchura de banda total una vez, aunque haya múltiples recibientes del tren de medios.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

gatekeeperIdentifier (identificador de controlador de acceso) – Un **gatekeeperIdentifier** que el punto extremo recibió en la lista de **alternateGatekeeper** en un mensaje RCF proveniente del controlador de acceso cuando se registró o en un mensaje BRJ anterior.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

answeredCall (llamada respondida) – Fijado a VERDADERO para indicar que esta parte fue el destino original (esta parte respondió la llamada).

callLinkage (vinculación de llamada) – El contenido de este campo suele controlarse por un servicio de vinculación de llamada. Para los procedimientos y semántica de este campo, véase la cláusula 10/H.323.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor en un momento dado, suponiendo que el controlador de acceso confirma el mensaje BRQ enviando una BCF. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity**.

usageInformation (información de utilización) – Este campo permite al punto extremo comunicar información de utilización para esta llamada. Un controlador de acceso no incluirá este campo cuando envíe un mensaje BRQ.

bandwidthDetails (detalles de anchura de banda) – Proporciona información de anchura de banda para cada tren de medios que el punto extremo está transmitiendo o recibiendo en ese momento, en las mismas unidades utilizadas en el campo **bandWidth**. Cada tren multidifusión se informará una sola vez, aunque haya múltiples recibientes del tren de medios.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.12.2 Confirmación de anchura de banda (BCF, *bandwidthConfirm*)

El mensaje BCF incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la BRQ.

bandWidth (anchura de banda) – El máximo permitido en ese momento en incrementos de 100 bits.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de

integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor en un instante dado. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity**. No se incluye cuando la BCF lo envía el controlador de acceso.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.12.3 Rechazo de anchura de banda (BRJ, *bandwidthReject*)

El mensaje BRJ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la BRQ.

rejectReason (motivo del rechazo) – Motivo por el que el cambio fue rechazado por el controlador de acceso.

allowedBandWidth (anchura de banda permitida) – El máximo permitido en ese momento en incrementos de 100 bits, incluida la asignación vigente.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.13 Mensajes de petición de localización

La LRQ solicita que un controlador de acceso proporcione traducción de dirección. El controlador de acceso responde con una LCF que contiene la dirección de transporte del destino, o rechaza la petición con LRJ.

7.13.1 Petición de localización (LRQ, *locationRequest*)

El mensaje LRQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

endpointIdentifier (identificador de punto extremo) – Es un identificador de punto extremo que fue asignado al terminal por RCF.

destinationInfo (información de destino) – Secuencia de direcciones de alias para el destino, tales como **dialledDigits**, **partyNumber (e164Number** o **privateNumber)** o **h323-ID**. Si en un controlador de acceso se registra al menos un alias y en el mensaje LRQ no se registran dos alias a distintas personas, el controlador de acceso reconocerá la petición de ubicación como referente a la identidad registrada. En el caso de alias en conflicto la petición se rechazará con la causa **AliasesInconsistent**. Si el controlador de acceso no proporciona esta validación, considerará que el destino es la primera dirección registrada.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

replyAddress (dirección de respuesta) – Dirección de transporte para enviar LCF/LRJ.

sourceInfo (información de origen) – Indica el emisor de la LRQ. El controlador de acceso puede utilizar esta información para decidir cómo responder a la LRQ.

canMapAlias (puede copiar alias) – Si está fijado a VERDADERO, indica que, si la LCF resultante contiene los campos **destinationInfo**, **destExtraCallInfo** y/o **remoteExtensionAddress**, el punto extremo puede copiar esta información en los campos **destinationAddress**, **destExtraCallInfo** y **remoteExtensionAddress** del mensaje Establecimiento, respectivamente. Si el controlador de acceso reemplaza la información de direccionamiento proveniente de la LRQ y **canMapAlias** es FALSO, el controlador de acceso debe rechazar la LRQ. Los sistemas conformes a H.225.0 versión 4 y posteriores fijarán este campo a VERDADERO.

gatekeeperIdentifier (identificador de controlador de acceso) – Un **gatekeeperIdentifier** que el punto extremo recibió en la lista de **alternateGatekeeper** en el mensaje RCF proveniente del controlador de acceso cuando se registró o en un mensaje LRJ anterior.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

desiredProtocols (protocolos deseados) – Identifica el tipo de protocolos, por orden de preferencia, que el punto extremo de origen desea para su llamada (por ejemplo, voz o fax). Una entidad de resolución puede utilizar este campo para localizar un punto extremo que también soporte el protocolo, teniendo en cuenta el orden de preferencia.

desiredTunnelledProtocol (protocolo tunelizado deseado) – Este campo identifica un protocolo cuya tunelización se solicita.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

hopCount (cuenta de saltos) – Este campo define el número de controladores de acceso a través de los cuales se puede propagar este mensaje. Cuando un controlador de acceso recibe una LRQ y decide que el mensaje debería ser reenviado a otro controlador de acceso, lo primero que hace es decrementar la **hopCount**. Si la **hopCount** es entonces superior a 0, el controlador de acceso inserta el nuevo valor de la cuenta de saltos en el mensaje que se ha de reenviar. Si la **hopCount** llega a 0, el controlador de acceso no reenviará el mensaje.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos RCC utilizados para la llamada.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización de Control de llamada empleada en esta Recomendación. Cuando se envía un mensaje LRQ en soporte de otra ARQ o ESTABLECIMIENTO, el controlador de acceso copiará el identificador de llamada de la ARQ o ESTABLECIMIENTO en la LRQ. Un punto extremo que envía un LRQ como preparación para el inicio de una llamada rellenará este campo con el identificador de llamada que le corresponda. Las LRQ enviadas fuera de este contexto de llamada no incluirán el campo identificador de llamada.

bandWidth (anchura de banda) – Anchura de banda bidireccional solicitada para la llamada en unidades de 100 bits por segundo. Por ejemplo, una llamada de 128 kbit/s se señalizaría como una petición de 256 kbit/s. El valor se refiere sólo a la velocidad binaria de audio y vídeo, excluidos encabezamientos y tara.

sourceEndpointInfo (información del punto extremo de origen) – Secuencia de direcciones de alias del punto extremo de origen, como **dialledDigits**, **PartyNumber** (**e164Number** o **privateNumber**) o **h323-ID**. El controlador de acceso copiará la información del punto extremo en nombre del cual envía la LRQ, o, si reenvía una LRQ recibida, el controlador de acceso copiará la **sourceEndpointInfo** de la LRQ recibida.

canMapSrcAlias (puede copiar alias Src) – Si está fijado a VERDADERO, indica que si la LCF resultante contiene el campo **modifiedSrcInfo**, el punto extremo puede copiar esa información en el campo **sourceInfo** del mensaje Establecimiento. Si un controlador de acceso envía el mensaje LRQ al haber recibido una ARQ, el controlador de acceso copiará este campo de la ARQ. Si el controlador de acceso sustituye la información de direccionamiento de la LRQ y **canMapSrcAliases** es FALSO, el controlador de acceso rechazará la LRQ.

7.13.2 Confirmación de localización (LCF, *locationConfirm*)

El mensaje LCF incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Será el mismo valor que fue pasado en la LRQ.

callSignalAddress (dirección de señalización de llamada) – La dirección de transporte a la que se envía señalización de llamada H.225.0; utiliza el puerto conocido o dinámico fiable, pero puede ser una dirección de punto extremo o de controlador de acceso según el modelo de llamada en uso.

rasAddress (dirección ras) – Dirección de registro, de admisiones y de situación para el punto extremo localizado.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

destinationInfo (información de destino) – Secuencia de direcciones de alias para el destino, tales como **dialledDigits**, **partyNumber** (**e164Number** o **privateNumber**) o **h323-ID**.

destExtraCallInfo (información de llamada extra de destino) – Contiene direcciones exteriores para múltiples llamadas.

destinationType (tipo de destino) – Especifica el tipo del punto extremo de destino.

remoteExtensionAddress (dirección de extensión distante) – Contiene la dirección de alias de un punto extremo llamado en los casos en que es necesaria esta información para atravesar múltiples pasarelas.

alternateEndpoints (puntos extremos alternativos) – Secuencia de alternativas de puntos extremos prioritarios para **callSignalAddress**, **rasAddress**, o **destinationInfo**.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

alternateTransportAddresses (direcciones de transporte alternativo) – Este campo lleva direcciones de señalización de llamada para transportes diferentes de TCP. La inclusión de una dirección indica el soporte de transporte correspondiente.

supportedProtocols (protocolos soportados) – Este campo indica los protocolos soportados por el punto extremo.

multipleCalls (múltiples llamadas) – Si es VERDADERO, este campo indica que el punto extremo localizado puede señalizar múltiples llamadas por una sola conexión de señalización de llamada. Si es FALSO, el punto extremo de destino no tiene esta capacidad. Si este campo está ausente, el controlador de acceso no sabe si el punto extremo tiene esta capacidad.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada en cuestión.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos RCC utilizados para la llamada.

serviceControl (control de servicio) – Este campo contiene información de direccionamiento que el punto extremo puede utilizar para comunicación de control de servicio relacionado con la llamada con la red como se describe, por ejemplo, en el anexo K/H.323.

modifiedSrcInfo (información de Src modificada) – Direcciones de alias que deberán utilizarse para el punto extremo de origen, como **dialledDigits**, **PartyNumber** (**e164Number** o **privateNumber**) o **h323-ID**. Este campo se utilizará cuando la dirección de alias del punto extremo llamante se traduce/modifica al intentar encaminar la llamada a su destino primario, o a cualquier punto extremo alternativo. Si el mensaje LCF origina una respuesta ACF al punto extremo, este campo deberá copiarse en el mensaje ACF.

bandWidth (anchura de banda) – La máxima anchura de banda permitida para la llamada, que puede ser inferior a la solicitada.

7.13.3 Rechazo de localización (LRJ, *locationReject*)

El mensaje LRJ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Será el mismo valor que fue pasado en la LRQ.

rejectReason (motivo del rechazo) – Indica el motivo por el que se denegó la petición de localización. Si **rejectReason** es **routeCallToSCN**, el **motivo del rechazo** incluirá también un número de teléfono o lista de números de teléfono a los que la pasarela pueda redirigir la llamada en la RCC, si la pasarela soporta ese procedimiento. Un motivo de **resourceUnavailable** indica que la anchura de banda está utilizada más de lo debido o que, en este momento, ninguna entidad registrada en el controlador de acceso tiene capacidad para tratar una llamada a la ubicación solicitada. Un motivo del tipo **genericDataReason (motivo datos genéricos)** indica que la petición fue rechazada como resultado de una característica o un elemento genérico; en este campo, se puede especificar información adicional en el campo **genericData (datos genéricos)**.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden requerirse para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas relacionadas con la llamada.

genericData (**datos genéricos**) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

serviceControl (**control de servicio**) – Este campo contiene información de direccionamiento que el punto extremo puede utilizar para comunicación de control de servicio relacionado con la llamada con la red como se describe, por ejemplo, en el anexo K/H.323.

7.14 Mensajes de desligamiento

7.14.1 Petición de desligamiento (DRQ, *disengageRequest*)

Si se envía de un terminal a un controlador de acceso, la DRQ informa al controlador de acceso que un punto extremo está siendo abandonado. Si se envía de un controlador de acceso a un punto extremo, la DRQ obliga a abandonar una llamada; dicha petición no será rechazada. La DRQ no se envía directamente entre puntos extremos.

Adviértase que DRQ no es la misma que **ReleaseComplete**, dado que su finalidad es informar al controlador de acceso de la terminación de una llamada; el controlador de acceso puede no recibir la liberación completa si no está terminando el canal de señalización de llamada.

El mensaje DRQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

endpointIdentifier (identificador de punto extremo) – Es un identificador de punto extremo que fue asignado al terminal por RCF.

conferenceID (ID de conferencia) – ID de la llamada de la que ha de liberarse la anchura de banda.

callReferenceValue (valor de referencia de llamada) – El CRV de los mensajes de señalización de llamada H.225.0 para esta llamada; sólo tiene validez local. Es utilizado por un controlador de acceso para asociar el mensaje con una determinada llamada.

disengageReason (motivo del desligamiento) – Motivo por el que fue solicitado el cambio por el controlador de acceso o el terminal.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

gatekeeperIdentifier (identificador de controlador de acceso) – Un **gatekeeperIdentifier** que el punto extremo recibió en la lista de **alternateGatekeeper** en el mensaje RCF procedente del controlador de acceso cuando se registró o en un mensaje DRJ anterior.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

answeredCall (llamada respondida) – Fijado a VERDADERO para indicar que esta parte fue el destino inicial (esta parte respondió la llamada).

callLinkage (vinculación de llamada) – El contenido de este campo se controla generalmente por un servicio de vinculación de llamada. Para los procedimientos y semántica de este campo, véase la cláusula 10/H.323.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor en un momento dado, suponiendo que el controlador de acceso confirma el mensaje DRQ enviando una DCF. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapability**. Este campo no se incluye cuando la DRQ lo envía un controlador de acceso.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos RCC utilizados para la llamada.

usageInformation (información de utilización) – Este campo permite a un punto extremo comunicar información de utilización para esta llamada. Un controlador de acceso no incluirá este campo cuando envíe un mensaje DRQ.

terminationCause (causa de terminación) – Este campo indica el motivo por el cual terminó la llamada. Esta información es más específica que el motivo proporcionado por el campo **disengageReason**. Un controlador de acceso no incluirá este campo cuando envíe un mensaje DRQ.

serviceControl (control de servicio) – Este campo contiene datos específicos de servicio, o referencias a los mismos, que podrían ser utilizados por un punto extremo como se describe, por ejemplo, en el anexo K/H.323. El controlador de acceso podría utilizar este campo para indicar que la llamada va a terminar porque ha expirado el período de validez de alguna cuenta, o porque la cantidad pagada por la llamada ha sido consumida.

genericData (**datos genéricos**) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.14.2 Confirmación de desligamiento (DCF, *disengageConfirm*)

El mensaje DCF incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la DRQ.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

capacity (capacidad) – Este campo indica la capacidad de llamada disponible del punto extremo emisor después de que la llamada indicada en la DCF ha sido desligada. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity**. Este campo no se incluye cuando la DCF lo envía un controlador de acceso.

circuitInfo (información de circuito) – Este campo proporciona información sobre el circuito o los circuitos utilizados para la llamada.

usageInformation (información de utilización) – Este campo permite a un punto extremo comunicar información de utilización para esta llamada. Un controlador de acceso no incluirá este campo cuando envíe un mensaje DCF.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.14.3 Rechazo de desligamiento (DRJ, *disengageReject*)

DRJ es enviado por el controlador de acceso si el punto extremo es desregistrado.

El mensaje DRJ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la DRQ.

rejectReason (motivo del rechazo) – Motivo por el que se rechazó la petición.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con características que están definidas fuera de la especificación H.225.0 de base. Estos parámetros pueden utilizarse, por ejemplo, para tunelizar información transparentemente a través de RAS.

7.15 Mensajes de petición de situación

La IRQ es enviada desde un controlador de acceso a un terminal solicitando información de estado en forma de una IRR. La IRR puede también ser enviada por el terminal en un intervalo especificado en el mensaje ACF sin el recibo de una IRQ procedente del controlador de acceso. Este mensaje no debe confundirse con el mensaje Estado de señalización de llamada H.225.0.

Cuando una IRR no solicitada es enviada por un punto extremo a un controlador de acceso de la versión 2 o versión más alta, puede indicar en el campo **needResponse** que desea que el controlador de acceso acuse recibo de la IRR. En este caso, rellena el campo **requestSeqNum** con un número distinto de 1. El controlador de acceso devuelve un mensaje IACK (acuse de recibo positivo) o bien un mensaje INAK (acuse de recibo negativo) y devolverá el mismo número en el campo **requestSeqNum**.

7.15.1 Petición de información (IRQ, *infoRequest*)

El mensaje IRQ incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

callReferenceValue (valor de referencia de llamada) – CRV de la llamada sobre la que trata la interrogación. Si es cero, este mensaje se interpreta como una petición de una IRR para cada llamada en la que el terminal está activo. Si el terminal no está activo en ninguna llamada, se enviará IRR en respuesta a un **valor de referencia de llamada** de cero con los campos apropiados.

Si **callReferenceValue** es cero, el punto extremo ignorará **callIdentifier**. En este caso el controlador de acceso fijará **callIdentifier** en cero.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

replyAddress (dirección de respuesta) – Una dirección de transporte para enviar IRR, quizás no al controlador de acceso.

callIdentifier (identificador de llamada) – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

uuiesRequested (uuies solicitadas) – El controlador de acceso puede solicitar al punto extremo que notifique al controlador de acceso los mensajes de señalización de llamada H.225.0 que el punto extremo envía o recibe si el punto extremo indicó esta capacidad en la ARQ fijando **willSupplyUUIEs** en VERDADERO. **uuiesRequested** indica el conjunto de mensajes de señalización de llamada H.225.0 que el punto extremo notificará al controlador de acceso.

callLinkage (vinculación de llamada) – El contenido de este campo es controlado generalmente por un servicio de vinculación de llamada. Para los procedimientos y semántica de este campo, véase la cláusula 10/H.323.

usageInfoRequested (información de utilización solicitada) – Un controlador de acceso puede incluir este campo para pedir que el punto extremo comunique, en el mensaje IRR, la información de utilización de llamada indicada.

segmentedResponseSupported (respuesta segmentada soportada) – Este campo indica si el controlador de acceso permitirá al punto extremo retornar información de llamada para todas las llamadas en múltiples mensajes IRR, o "segmentos". Si este campo está presente, la segmentación está permitida. De lo contrario, no está permitida. Este campo sólo tiene sentido cuando el controlador de acceso envía una IRQ con un **callReferenceValue** de 0 y no estará presente en los demás casos.

nextSegmentRequested (segmento siguiente solicitado) – Si el controlador de acceso envía un mensaje IRQ con un **callReferenceValue** de 0 e incluye el campo **segmentedResponseSupported**, el punto extremo puede retornar una IRR con sólo parte de la información de llamada, lo que se indica incluyendo el campo segmento en la IRR. El controlador de acceso puede solicitar el segmento siguiente retransmitiendo el anterior mensaje IRQ con el campo **nextSegmentRequested** fijado al valor del segmento siguiente que el controlador de acceso espera recibir.

capacityInfoRequested (información de capacidad solicitada) – Si está presente, este campo indica que el controlador de acceso pide al punto extremo que incluya información de capacidad de llamada en la IRR.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.15.2 Respuesta a petición de información (IRR, *infoRequestResponse*)

El mensaje IRR incluye lo siguiente:

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

requestSeqNum (**número secuencial de petición**) – En el caso de una IRR solicitada, este campo contendrá el número secuencial procedente de la IRQ. En caso de un informe no solicitado a un controlador de acceso de la versión 1, este campo contendrá uno (1). En todas las demás IRR no solicitadas, contendrá un número monótonamente creciente (que será devuelto por el controlador de acceso en su respuesta si **needResponse** es VERDADERO).

endpointType (tipo de punto extremo) – Proporciona información acerca del punto extremo.

endpointIdentifier (identificador de punto extremo) – Valor asignado por el controlador de acceso en la RCF.

rasAddress (dirección ras) – Dirección para registro, admisiones, etc.

callSignalAddress (dirección de señalización de llamada) – Dirección de señalización de llamada H.225.0.

endpointAlias (alias de punto extremo) – Alias para el punto extremo.

perCallInfo (información por llamada) – Información sobre cada llamada:

- **nonStandardData (datos no normalizados)** – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).
- **callReferenceValue (valor de referencia de llamada)** – CRV (ID de llamada) de señalización de llamada H.225.0 de esa llamada sobre la que trata la respuesta.
- **conferenceID (ID de conferencia)** – Identificador de conferencia único.
- **originator (originador)** – Si es VERDADERO, el punto extremo interrogado fue el originador de la llamada; si es FALSO, el punto extremo fue el destino de la llamada.
- **audio** – Información sobre el canal o canales de audio. Se incluirá el elemento **multicast** si la sesión es de multidifusión.
- **video (vídeo)** – Información sobre el canal o canales de vídeo. Se incluirá el elemento **multicast** si la sesión es de multidifusión.
- **data (datos)** – Información sobre el canal o canales de datos.
- **h245** – Dirección de transporte del canal de control H.245.
- **callSignalling (señalización de llamada)** – Dirección de transporte del canal de señalización de llamada H.225.0.
- **callType (tipo de llamada)** – Proporciona información sobre la topología de las llamadas.
- **bandwidth (anchura de banda)** – Utilización actual en incrementos de 100 bit/s; incluye sólo audio y vídeo, excluidos encabezamientos y tara.
- **callModel (modelo de llamada)** – Indica que el punto extremo sabe cuál es el modelo de llamada que se utiliza.
- **callIdentifier (identificador de llamada)** – Identificador de llamada único a nivel mundial fijado por el punto extremo de origen que puede utilizarse para asociar la señalización RAS con la señalización Q.931 modificada que se utiliza en esta Recomendación.

- **tokens (testigos)** – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.
- **cryptoTokens** – **Testigos** criptados.
- **substituteConfIDs (ID de conferencia de sustitución)** – Listado de todos los ConferenceID recibidos en los mensajes SubstituteCID H.245 pertenecientes a **perCallInfo conferenceID** de RAS original.
- **pdu (unidad de datos de protocolo)**:
  - **h323pdu** – Copia de una PDU H.225.0 y Q.931 solicitada por el controlador de acceso en **uuiesRequested** en ACF o bien en IRQ.
  - **sent (enviado)** – Fijado a VERDADERO para indicar que el punto extremo envió la **h323pdu**; fijado en FALSO para indicar que el punto extremo recibió la **h323pdu**.
- **callLinkage (vinculación de llamada)** – El contenido de este campo suele ser controlado por un servicio de vinculación de llamada. Para los procedimientos y semántica de este campo, véase la cláusula 10/H.323.
- **usageInformation (información de utilización)** – Este campo permite al punto extremo comunicar información de utilización para la llamada en cuestión.
- **circuitInfo** (**información de circuitos**) – Este campo proporciona información sobre el circuito o los circuitos RCC utilizados para la llamada.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

needResponse (necesidad de respuesta) – Si está fijado a VERDADERO y el controlador de acceso indicó en RCF o ACF que responderá a las IRR no solicitadas (fijando **willRespondToIRR** en VERDADERO), el controlador de acceso responderá con IACK o INAK. Si el controlador de acceso no indicó en RCF ni en ACF que responderá a las IRR no solicitadas (fijando **willRespondToIRR** en FALSO), ignorará la variable BOOLEANA **needResponse**.

capacity (capacidad) – Indica la capacidad de llamada del punto extremo emisor en un momento dado. Cuando envíe este campo, el punto extremo incluirá el elemento **currentCallCapacity** y solamente incluirá el elemento **maximumCallCapacity** cuando responda a una IRQ que incluya el elemento **capacityInfoRequested**.

irrStatus (estado de IRR) – Este elemento debe retornarse en mensajes IRR en respuesta a un mensaje IRQ enviado por el controlador de acceso. La ausencia de este elemento indica que el mensaje IRR contiene información detallada completa de la llamada. Son posibles los siguientes valores:

- **complete (completo)** – Indica que este mensaje IRR contiene el último segmento de la información de llamada para una IRQ que solicita todos los detalles de la llamada. Cuando no se emplea segmentación, este campo indica que la IRR contiene todos los detalles de la llamada en un solo mensaje IRR.

- **incomplete (incompleto)** – Indica que el punto extremo no puede colocar en un solo mensaje IRR toda la información de llamada solicitada cuando responde a un mensaje IRQ que contenía un **callReferenceValue** de 0.
- **segment (segmento)** – Este campo indica el número de segmento, que es un valor módulo 65536, que aumenta monótonamente, de este mensaje IRR, cuando se envían IRR segmentados en respuesta a una IRQ que contiene un **callReferenceValue** de 0.
- **invalidCall (llamada no válida)** – Este campo indica que la llamada a que se hace referencia en el mensaje IRQ no existe.

unsolicited (no solicitado) – Los puntos extremos de la versión 4 y posteriores de H.323 fijarán este campo a VERDADERO en los mensajes IRR no solicitados descritos en 8.4.2/H.323 y lo fijarán a FALSO en los mensajes IRR solicitados.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.15.3 Acuse de recibo positivo de petición de información (IACK, *infoRequestAck*)

El mensaje IACK incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Este campo contendrá el **requestSeqNum** que estaba en IRR.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

7.15.4 Acuse de recibo negativo de petición de información (INAK, *infoRequestNak*)

El mensaje INAK incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Este campo contendrá el **requestSeqNum** que estaba en IRR.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

nakReason (motivo de acuse de recibo negativo) – Motivo por el cual el acuse de recibo de IRR fue negativo.

altGKInfo (información de controlador de acceso alternativo) – Información facultativa sobre controladores de acceso alternativos.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

7.16 Mensaje no normalizado

La estructura de un **NonStandardMessage** es la siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

featureSet (**conjunto de características**) – Este campo especifica un conjunto de características genéricas.

genericData (**datos genéricos**) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.17 Mensaje no entendido

Este mensaje se envía siempre que un punto extremo H.323 recibe un mensaje RAS que no entiende o no puede decodificar. En aquellos casos en que la dirección de transporte de destino para el mensaje XRS no está disponible (es decir, el mensaje RAS recibido no pudo decodificarse), el XRS puede enviarse a la dirección de transporte desde la cual se recibió el mensaje RAS que no fue entendido. Esta dirección de transporte puede obtenerse de la capa de transporte subyacente. No se enviará un mensaje XRS en respuesta a un mensaje XRS. Los puntos extremos H.323 deben transmitir no más de un mensaje XRS por segundo a la misma dirección de transporte, para evitar congestión de red en situaciones en que se reciben mensajes corruptos.

RequestSeqNum (número secuencial solicitado) – Si el mensaje desconocido puede ser decodificado, este campo es el **requestSeqNum** del mensaje desconocido. Si el mensaje desconocido no puede ser decodificado, este campo es un número monótonamente creciente, único para el emisor. El **RequestSeqNum** debe utilizarse para asegurar la compatibilidad hacia atrás con puntos entremos H.323 versión 3 y anteriores. Los puntos extremos H.323 versión 4 y posteriores deben examinar el parámetro **messageNotUnderstood** para asociar el XRS con un mensaje transmitido antes.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

messageNotUnderstood (mensaje no entendido) – Copia del mensaje que fue recibido y no fue entendido.

7.18 Mensajes de disponibilidad de recursos de pasarela

La indicación disponibilidad de recursos (RAI, *resource availability indication*) es una notificación enviada por una pasarela a un controlador de acceso indicando su capacidad de llamada en esos momentos para cada protocolo de la serie H y la velocidad de datos para ese protocolo. El controlador de acceso responde con una confirmación de disponibilidad de recursos (RAC, *resource availability confirmation*) tras recibir una RAI para acusar recibo de su recepción.

7.18.1 Indicación de disponibilidad de recursos (RAI)

El mensaje RAI incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

protocolIdentifier **(identificador de protocolo)** – Identifica la antigüedad del punto extremo emisor.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

endpointIdentifier (identificador de punto extremo) – Un controlador de acceso asignó cadena de identidad de punto extremo.

protocols (protocolos) – Indica las velocidades de datos actuales para cada protocolo que puede ser soportado dado el estado actual del dispositivo.

almostOutOfResources (casi sin recursos) – Cuando está fijado a VERDADERO, el dispositivo alcanza su plena capacidad o se acerca a ella. Cualquier acción basada en este campo queda a juicio del fabricante. Si el dispositivo no alcanza su plena capacidad ni se acerca a ella, este campo se fijará en FALSO.

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

capacity (capacidad) – Indica la capacidad de llamada del punto extremo emisor en un momento dado. Obsérvese que, si se proporciona **capacity**, no se deberá tener en cuenta la variable BOOLEANA **almostOutOfResources** pues el campo **capacity** proporciona más información

detallada; sin embargo, la variable BOOLEANA **almostOutOfResources** deberá ser fijada con el fin de mantener la retrocompatibilidad. Cuando envíe el campo **capacity**, el punto extremo incluirá los elementos **currentCallCapacity**.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.18.2 Confirmación de disponibilidad de recursos (RAC)

El mensaje RAC incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en la RAI.

protocolIdentifier **(identificador de protocolo)** – Identifica la antigüedad del controlador de acceso aceptador.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.19 Temporizadores RAS y petición en curso (RIP, *request in progress*)

El cuadro 23 muestra los valores de temporización por defecto para responder a los mensajes RAS y los cómputos de reintentos subsiguientes recomendados si no se recibe una respuesta. (Estos valores pueden cambiar a medida que se vaya disponiendo de más experiencia y datos en relación con la implementación.)

Cuadro 23/H.225.0 – Valores de temporización por defecto recomendados

Mensajes RAS	Valor de temporización (s)	Cómputo de reintentos
GRQ	5	2
RRQ (nota 1)	3	2
URQ	3	1
ARQ	5	2
BRQ	3	2
IRQ	3	1
IRR (nota 2)	5	2
DRQ	3	2

Cuadro 23/H.225.0 – Valores de temporización por defecto recomendados

Mensajes RAS	Valor de temporización (s)	Cómputo de reintentos
LRQ	5	2
RAI	3	2
SCI	3	2
NOTA 1 – El valor de temporización se ha de volver a calcular en base al tiempo de vida (que puede ser indicado por el controlador de acceso en el mensaje RCF) y el número deseado de reintentos. NOTA 2 – En los casos en que se espere que el controlador de acceso responda a una IRR no solicitada con IACK o INAK, puede activarse la temporización si no se recibe ninguna respuesta a la IRR.		

Si una entidad recibe una petición de una entidad de versión 2 (o posterior) para la que no puede generarse una respuesta dentro de un periodo de temporización de reintento típico, puede enviar un mensaje RIP especificando el periodo (en el campo **demora**) tras el que deberá haberse generado una respuesta. En cuanto esté disponible una respuesta, la entidad respondedora deberá enviarla sin esperar a que concluya el retardo de la RIP. Si una entidad solicitante no ha recibido una respuesta en el momento en que concluye el retardo de la RIP, volverá a enviar la petición. La entidad respondedora puede enviar una respuesta duplicada o bien otro mensaje RIP. En la figura 2 se muestra un ejemplo de intercambio de mensajes con el que se describen varios aspectos de estrategia de los reintentos.

Los vendedores han de saber que cualquier reintento repercutirá en el tiempo de establecimiento de la comunicación, que debería reducirse al mínimo. Por ello, conviene que los tiempos de reintento sean breves. Para que las entidades distantes puedan anticipar tiempos de reintento típicos, a fin de decidir cuándo se envía un mensaje RIP, las entidades deberán evitar periodos de reintento inferiores a 100 ms. Para los tiempos de ida y vuelta se recomienda el cálculo exponencial y ajustes. Las entidades pueden utilizar el tiempo de ida y vuelta medido del proceso de registro RRQ/RCF para modificar una estimación inicialmente conservadora (de unos pocos segundos) a estos efectos. Las entidades pueden también utilizar el proceso de registro para intercambiar números de versiones de modo que se asegure la no utilización del mecanismo de reintentos basado en la RIP cuando participen entidades de versión 1 en la señalización.

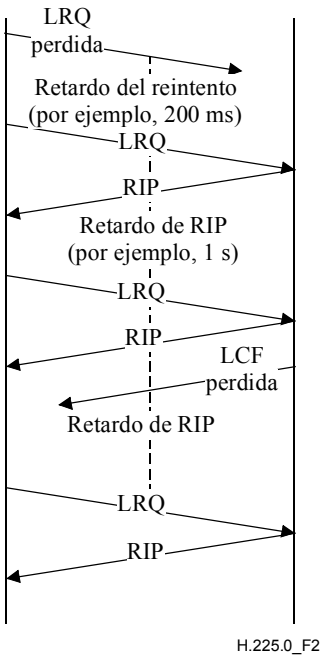


Figura 2/H.225.0 – Ejemplo de utilización del mensaje RIP

El mensaje RIP incluye lo siguiente:

requestSeqNum (número secuencial de petición) – Es el **requestSeqNum** de la petición que se está procesando.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden ser necesarios para permitir la operación. Los datos se insertarán en el mensaje, si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

delay (retardo) – Especifica el tiempo en milisegundos que esperará un punto extremo antes de tratar de efectuar un reintento. El punto extremo respondedor puede responder antes que concluya este periodo.

7.20 Mensajes de control de servicio

7.20.1 Indicación de control de servicio (SCI, *serviceControlIndication*)

El mensaje SCI lo envía un proveedor de servicio para indicar al cliente de servicio que podrá iniciarse una sesión de control de servicio individual hacia la dirección dada. Puede ser enviado por un controlador de acceso a un punto extremo (por ejemplo, para presentación de características de servicio al usuario) o por un punto extremo a un controlador de acceso (por ejemplo, para telecargar un guión de procesamiento de llamada). Obsérvese que las entidades H.323 versión 3 o anteriores no tienen capacidad para decodificar este mensaje, y no responderán.

El mensaje SCI contiene lo siguiente:

requestSeqNum (número secuencial solicitado) – Es un número monótonamente creciente, único para el emisor. Será retornado por el receptor en cualquier respuesta asociada con este mensaje concreto.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

serviceControl – Transporta un conjunto informaciones de sesión de control de servicio.

endpointIdentifier (identificador de punto extremo) – Se fija al valor recibido del controlador de acceso en el mensaje RCF, si el mensaje lo envía un punto extremo a su controlador de acceso.

callSpecific (específico de la llamada) – Se proporciona si las sesiones dadas se relacionan con una llamada concreta. El **callIdentifier**, **conferenceID** y **answeredCall** se fijarán al mismo valor que el contenido en el mensaje ARQ con el que se relaciona la sesión de servicio.

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.20.2 Respuesta de control de servicio (SCR, *serviceControlResponse*)

El mensaje SCR se envía para acusar recibo de un mensaje SCI, pero no significa necesariamente que el cliente del servicio iniciará la sesión como se indica en SCI.

El mensaje SCR contiene lo siguiente:

requestSeqNum (número secuencial de petición) – Debe ser el mismo valor que fue pasado en el SCI.

result (resultado) – Este campo indica el resultado del procesamiento de la información contenida en el mensaje SCI. Se definen los valores siguientes:

- **started (comenzado)** – El control de servicio solicitado fue comenzado.
- **failed (fracasado)** – Hubo algún error en la petición, y por eso fracasó.
- **stopped (detenido)** – El control de servicio fue detenido.
- **notAvailable (no disponible)** – El control de servicio solicitado no estaba disponible en el momento de la petición.

nonStandardData (datos no normalizados) – Lleva información no definida en esta Recomendación (por ejemplo, datos privados).

tokens (testigos) – Se trata de algunos datos que pueden necesitarse para permitir la operación. Los datos se insertarán en el mensaje si están disponibles.

cryptoTokens – **Testigos** criptados.

integrityCheckValue (valor de verificación de integridad) – Proporciona la integridad/autenticación del mensaje mejorada de los mensajes RAS. El valor de verificación de integridad sobre una base criptográfica es calculado por el emisor aplicando un algoritmo de integridad negociado y la clave secreta en todo el mensaje. Antes de calcular el **integrityCheckValue**, este campo deberá ser ignorado y estar vacío. Después del cálculo, el emisor coloca el valor de verificación de integridad calculado en el campo **integrityCheckValue** y transmite el mensaje.

featureSet (conjunto de características) – Este campo especifica un conjunto de características genéricas.

genericData (datos genéricos) – Este campo es una lista de elementos genéricos relacionados con las características que se definen fuera de la especificación H.225.0 básica. Estos parámetros se pueden utilizar, por ejemplo, para tunelizar la información de manera transparente mediante RAS.

7.21 Secuencia de confirmación de admisión (AdmissionConfirmSequence)

AdmissionConfirmSequence es una secuencia de uno o más mensajes RAS ACF. El controlador de acceso puede utilizarla para responder a un único mensaje ARQ, en vez de a un único mensaje ACF, cuando tiene distintos testigos de seguridad, distinta información de origen traducida, etc., que no pueden expresarse fácilmente en un único mensaje ACF. Los puntos extremos indican su capacidad para soportar la recepción de AdmissionConfirmSequence fijando la bandera **supportsACFSequences** en el mensaje RRQ.

8 Mecanismos para mantener la calidad de servicio

8.1 Planteamiento general e hipótesis

La calidad de servicio (QoS, *quality of service*) de transporte de una red de paquetes incluye características tales como:

- tasa de errores de bit;
- tasa de pérdida de paquetes;
- retardo.

Cualquier señalización relacionada con la QoS de transporte (por ejemplo, una petición de reserva a un encaminador) es efectuada por el terminal cuanto antes o por el controlador de acceso en su nombre. El terminal puede desear formular algunas reservas, ya que el controlador de acceso lógicamente no puede estar cerca del terminal, ni formular peticiones relacionadas con la QoS en nombre del terminal. El modo en que el terminal o el controlador de acceso hace reservas de QoS o de anchura de banda cae fuera del alcance de esta Recomendación.

Los informes de emisor y de receptor de RTCP serán el medio por el que se evaluará la QoS.

Hay dos tipos de retraso relacionado con la congestión que podrían medirse:

- Aumentos de corta duración del retardo que producirían una reducción perceptible, pero no molesta, de la velocidad de trama.
- Un aumento general del retardo debido a la congestión de la red de paquetes en el tiempo de manera que sea de utilidad un mecanismo basado en la realimentación.

Esencialmente, las ráfagas de corta duración son aproximadas mediante ocultación de errores, y una congestión de más larga duración es aproximada mediante reducción de la carga multimedios. Se adopta la hipótesis de que todos los terminales multimedios red de paquetes son terminales H.323, y todos intentarán reducir la utilización de la red de paquetes a medida que la congestión aumenta, más que "robarse" anchura de banda entre sí.

Los errores de bit en una red de paquetes son corregidos por lo general en una capa inferior, o dan lugar a pérdida de paquetes, por lo que no se consideran en esta cláusula.

La pérdida de paquetes exige que el receptor pueda compensar los paquetes perdidos de una manera que oculte los errores en la máxima medida posible. Para datos y control, se utiliza retransmisión en la capa de transporte. Para audio y vídeo, la retransmisión queda en estudio.

Un determinado nivel de QoS de transporte produce un nivel de la QoS de audio/vídeo percibida por el usuario que es función en parte de la efectividad de los métodos utilizados para superar problemas de QoS de transporte.

8.2 Utilización del RTCP al medir la calidad de servicio

8.2.1 Informes de emisor

El informe de emisor cumple tres fines principales:

1) Permite la sincronización de múltiples trenes RTP, tales como audio y vídeo.
2) Permite al receptor conocer la velocidad de datos y la velocidad de paquetes esperadas.
3) Permite al receptor medir la distancia en tiempo al emisor.

De estos tres fines, 1 es el más pertinente para esta Recomendación. Los fabricantes pueden utilizar los informes del remitente de otros modos a su discreción.

El campo pertinente para la sincronización de trenes es la indicación de tiempo RTP y la indicación de tiempo NTP en el informe de emisor del RTCP. La indicación de tiempo NTP (si está disponible) indica la hora "de reloj de pared" y corresponde a la indicación de tiempo que tiene las mismas unidades y desplazamiento aleatorio de la indicación de tiempo de captura RTP en los paquetes de medios.

8.2.2 Informes de receptor

Se utilizan cuatro partes de los informes de receptor en esta Recomendación para medir la QoS:

1) Fracción perdida.
2) Los paquetes acumulativos perdidos.
3) El número secuencial más alto extendido recibido.
4) Fluctuación entre llegadas.

Los apartados 2 y 3 se utilizan para calcular el número de paquetes perdidos desde el informe de receptor anterior. Esta medida puede tomarse como una medida a corto plazo de la congestión de la red de paquetes. Véase en RFC 3550 [37] sección 6.4.4 un ejemplo de cálculo. Si esta velocidad de pérdida sobrepasa un valor fijado por el fabricante, el terminal H.225.0 debería reducir las velocidades de medios en el lado red de paquetes de acuerdo con los procedimientos expuestos más adelante en 8.4. Si el apartado 1 sobrepasa un valor fijado por el administrador, puede también ser conveniente ejercer una acción correctiva.

Si el intervalo entre informes de receptor sobrepasa un valor fijado por las especificaciones del fabricante, los terminales H.323 deben utilizar el apartado 1 como un indicador de congestión grave que exige reducción de velocidad de medios en el lado red de paquetes.

El apartado 4 debe utilizarse como una indicación de congestión inminente. Si la fluctuación entre llegadas aumenta en tres informes de receptor consecutivos, el terminal emisor H.323 debe ejercer acción correctiva.

8.3 Procedimientos de fluctuación de audio/vídeo

La Rec. UIT-T H.245 proporciona instrucciones y procedimientos para indicaciones de retardo de ida y vuelta utilizando **petición de retardo de ida y vuelta (RoundTripDelayRequest)** y

respuesta de retardo de ida y vuelta (RoundTripDelayResponse). En una llamada multipunto, el MC responde a una petición del punto extremo. RTCP contiene un método de calcular retardos de ida y vuelta basándose en los mensajes de informe de emisor y de informe de receptor. Adviértase que la magnitud que se mide en cada caso no es la misma, por lo que no hay contradicción en utilizar ambos métodos para medir la fluctuación.

Véase en 6.2.5/H.323 un análisis de la posible forma de utilizar la señalización de nivel H.245 para reducir opcionalmente los retardos relacionados con la fluctuación.

8.4 Procedimientos de sesgo de audio/vídeo

Véase en 6.2.6/H.323 un análisis sobre la forma de utilizar la señalización de nivel H.245 para limitar el sesgo entre diferentes canales lógicos.

8.5 Procedimientos para mantener la calidad de servicio

Existen algunos métodos para que la pasarela/el terminal H.323 responda a un aumento en la pérdida de paquetes o en la fluctuación entre llegadas en el receptor de extremo distante. Estos métodos pueden agruparse en los que son apropiados para una rápida respuesta a un problema de corta duración, tal como un paquete perdido o retardado, o los que son apropiados para una respuesta a un problema de mayor duración tal como el crecimiento en la congestión en la red de paquetes. Adviértase que estos métodos no pretenden mantener la actual calidad de servicio, sino más bien proveer una degradación ordenada del servicio. Se observaron las siguientes prioridades, de manera que, si aparecen, los medios se degradarán en el orden siguiente: Vídeo, Datos, Audio, Control.

Respuestas a corto plazo

- Reducción de la velocidad de trama durante un breve periodo de tiempo, lo que puede dar lugar a que la pasarela H.323 envíe tramas de relleno H.261 adicionales en el sentido red de paquetes a RCC para compensar el subflujo de paquetes.
- Reducción de la velocidad de paquetes por conmutación al modo opcional, en el que el audio/vídeo se mezclan en un paquete (queda en estudio).
- La velocidad de paquetes puede también reducirse mediante el uso de fragmentación MB del tren de vídeo.

Respuestas a más largo plazo

- Reducción de la velocidad binaria de medios (por ejemplo, conmutación de 384 kbit/s a 256 kbit/s): Esto puede exigir una simple instrucción al codificador en un terminal, o el uso de una función reductora de velocidad en la pasarela H.323. Estos cambios se señalizan mediante instrucciones **control de flujo (FlowControl)** H.245, o mediante señalización de canal lógico, según convenga.
- Desactivación de medios de menor importancia (por ejemplo, desactivación de vídeo para permitir un mayor volumen de tráfico T.120).
- Devolución de una señal de ocupado (ocupado adaptativa) al receptor como una indicación de congestión de la red de paquetes. Ésta puede combinarse con la desactivación de un medio, o de incluso todos los medios que no sean el puerto de transporte de control. Ocupado adaptativo es señalizado mediante un valor de causa Q.931 en Liberación completa.

Debe señalarse que responder a fluctuación entre llegadas en un trayecto multiencaminadores en el que llegan un gran porcentaje de paquetes deteriorados resulta difícil. Puede resultar imposible distinguir la fuente de fluctuación de otras fuentes, o basar la estrategia de base de recuperación tras errores en la fluctuación medida. Sin embargo, la pérdida de paquetes es cuantificable e inambigua.

8.6 Control de eco

El control del eco acústico incumbe al terminal de la serie H. En general, dado el retardo que interviene en la compresión de vídeo/audio, se supone que todos los terminales H.320, H.323 y H.324 tienen alguna forma de control de eco (compensación o conmutación).

Sin embargo, cuando el terminal H.323 está en comunicación con un teléfono de la RTGC, suele darse el caso de que el teléfono RTGC no dispone de control de eco. Por tanto, el usuario del terminal H.323 puede oír retorno de eco acústico procedente del lado RTGC. Este retorno de eco acústico puede minimizarse utilizando un teléfono de altavoz con control de eco, o utilizando un microteléfono o auriculares. Los fabricantes pueden añadir pérdida al trayecto de audio cuando un terminal H.323 está conectado a un teléfono POTS de la RTGC.

Para el control del eco híbrido (de dos a cuatro hilos), el circuito híbrido proporciona una interfaz entre sistemas de transmisión a cuatro hilos y terminales a dos hilos. Para llamadas RDSI de habla transportadas a través de la RTGC a 64 kbit/s no se requiere compensación de eco. Para llamadas de datos a 64 kbit/s no se permite compensación de eco.

En el caso de una pasarela constituida por varios componentes, interconectada a una red SS7, las indicaciones del aprovisionamiento de compensación de eco se transportan en el mensaje de señalización de parte usuario de la RDSI, como se especifica en la Rec. UIT-T Q.115. El controlador de pasarela de medios (MGC, *media gateway controller*) puede interpretar la información de señalización y habilitar o inhabilitar la compensación de eco en la pasarela de medios (MG, *media gateway*). En el caso de llamadas de habla, el MGC puede habilitar la compensación de eco sin que se produzcan efectos perjudiciales en la calidad del habla, incluso si la RTGC ha proporcionado compensación de eco en la propia RTGC.

En el caso de llamadas de datos en la banda vocal (llamadas de módem) que atraviesan o terminan en una red H.323, los módems proporcionan el control de compensación de eco mediante tonos dentro de banda. Ni los elementos de red RTGC, ni los MGC, requieren señalización fuera de banda.

Anexo A

RTP/RTCP

RTP y RTCP se definen en la referencia [37]. También se hace referencia a dicha referencia en el apéndice I. Tanto este anexo como el apéndice I se mantienen para guardar la equivalencia con versiones anteriores en la presente Recomendación.

El lector debe advertir que la referencia [37] corresponde a una bibliografía, y no es normativa, con excepción de la referencia a ISO/CEI 10646-1, que también aparece en la cláusula de referencias de esta Recomendación.

Los lectores deben también advertir que la terminología utilizada en [37] difiere algo de la utilizada en la Rec. UIT-T H.323 y esta Recomendación, de acuerdo con el cuadro A.1.

Cuadro A.1/H.225.0 – Correspondencia terminológica

Término H.323 y H.225.0	Término de la referencia [37] (RTP/RTCP)
tren de medios	Datos
dirección de transporte	dirección de transporte
dirección de red de paquetes	dirección de red
identificador de TSAP	puerto
anexo A	especificación o documento
deberá	debe
debería	debería

Debe además señalarse que los "traductores" y "mezcladores" no forman parte del sistema H.323. Los puntos extremos H.323, tales como pasarelas y MCU, tienen algunas de las características de los traductores y mezcladores, por lo que este texto se ha conservado como una guía para el implementador. Sin embargo, el soporte de traductores y mezcladores no forma parte de la H.323, y estas cláusulas se considerarán informativas.

Anexo B

Perfil RTP

El perfil RTP se define en la referencia [38]. También se hace referencia a dicha referencia ([38]) en el apéndice II. Tanto este anexo como el apéndice II se mantienen para guardar la equivalencia con versiones anteriores de la presente Recomendación.

Véase la introducción al anexo A; todas las advertencias allí indicadas se aplican igualmente a este anexo.

Anexo C

Formato de cabida útil RTP para trenes de vídeo H.261

El formato de cabida útil RTP para trenes de vídeo H.261 se define en la referencia [39]. También se hace referencia a dicha referencia ([39]) en el apéndice III. Tanto este anexo como el apéndice III se mantienen para guardar la equivalencia con versiones anteriores de la presente Recomendación.

Véase la introducción al anexo A; todas las advertencias allí indicadas se aplican igualmente a este anexo.

Anexo D

Formato de la cabida útil del RTP para trenes de vídeo H.261A

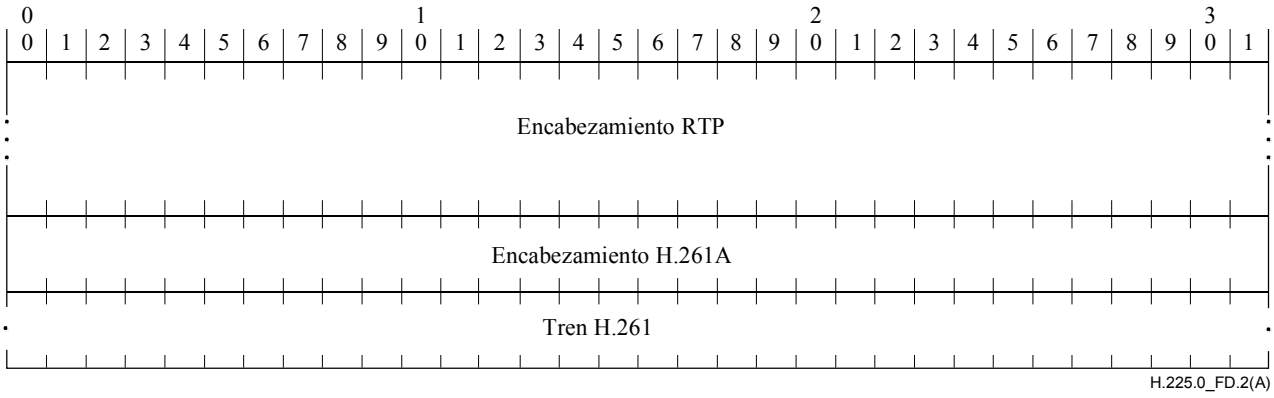
D.1 Introducción

Para facilitar la interconexión de trenes vídeo H.323 con la RCC a través de las pasarelas, la Rec. UIT-T H.323 define una forma modificada de la cabida útil de vídeo H.261 RTP. Esto facilita la gestión de la memoria tampón y el interfuncionamiento con códecs RCC distantes. El soporte del tipo de cabida útil H.261A se señaliza utilizando conjuntos de capacidades H.245 y en el mensaje **apertura de canal lógico** utilizando tipos de cabida útil dinámica RTP.

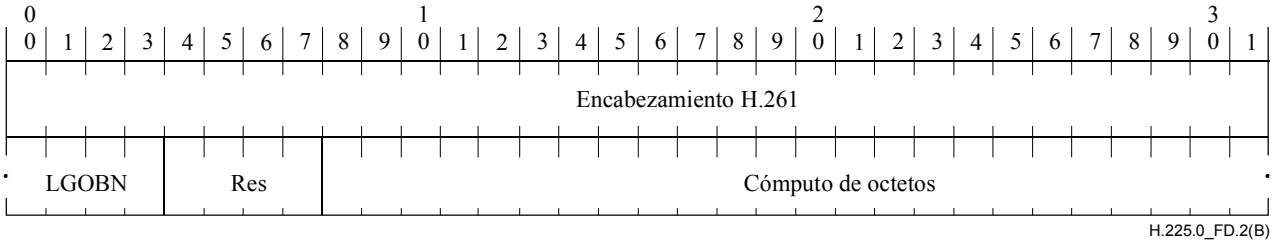
D.2 Paquetización RTP H.261A

Esta versión es una ampliación de la versión descrita en el anexo C, salvo que se añade una palabra adicional de 32 bits al encabezamiento H.261. Los procedimientos que se describen en el anexo C se aplican también a este anexo.

Los datos H.261A seguirán al encabezamiento RTP como se indica a continuación:



El encabezamiento H.261A se define como:



Los campos de encabezamiento H.261A tienen los siguientes significados:

Encabezamiento H.261: 32 bits – Como se describe en el anexo C.

*Último número GOB (*LGOBN*, last GOB number)*: 4 bits – El número GOB del último GOB en el paquete RTP (el número GOB máximo es 12 para la Rec. UIT-T H.261).

*Reservado (*RES*, reserved)*: Reservado.

Cómputo de octetos: 24 bits – Indica el número acumulado de octetos que han sido enviados en la parte de tren H.261 de los paquetes RTP. Si el último octeto de un paquete está rellenado sólo

parcialmente (como es indicado por EBIT), entonces no se cuenta en el cómputo acumulado de octetos. Este cómputo de octetos módulo 2^{24} comienza en un valor aleatorio y no se reinicia nunca.

Se puede utilizar ambos campos adicionales cuando se pierden paquetes o se entregan fuera de orden. El cómputo de octetos se puede utilizar para determinar cuánto relleno se necesitará en el tren RCC y facilitar la gestión de la memoria tampón. El último número GOB simplifica la determinación de cuáles GOB se han perdido debido a pérdida de paquetes.

Anexo E

Paquetización de vídeo

En este anexo se describe detalladamente la paquetización RTP para códecs de vídeo. El cuadro E.1 proporciona referencias a las definiciones de formatos de paquetización de vídeo que no están definidos en la presente Recomendación. En las cláusulas siguientes de este anexo se definen formatos de paquetización de vídeo adicionales.

Cuadro E.1/H.225.0 – Formatos de paquetización de vídeo definidos externamente

Nombre de la codificación	Definición de la paquetización
ISO/CEI 14496-2 (MPEG-4 Vídeo)	IETF RFC 3016, *RTP Payload Format for MPEG-4 Audio/Visual Streams*

E.1 H.263

En IETF RFC 2190 se especifica un formato de cabida útil del RTP para vídeo H.263 para trenes de bits de vídeo H.263 que no contienen las características nuevas adoptadas en la versión 2 (la versión de 1998) de la Rec. UIT-T H.263 (las características que utilizan PLUSPTYPE o anexos que siguen al anexo H/H.263). Más adelante se especificará un formato de cabida útil adicional que soporte las características mejoradas de los trenes de bits de la versión 2 de H.263. Un formato de paquetización heredado ampliamente utilizado en la industria (no especificado en IETF RFC 2190) sólo se puede emplear si la entidad par ha indicado que soporte ese formato en el intercambio de capacidades.

En RFC 3551 [38] sección 5 se describe el procedimiento a seguir para señalizar trenes de vídeo H.263.

Anexo F

Paquetización de audio y multiplexada

En este anexo se describen los detalles de la paquetización RTP para códecs de audio. El cuadro F.1 proporciona referencias a las definiciones de formatos de paquetización de audio que no están definidos en la presente Recomendación. El cuadro F.2 proporciona referencias a las definiciones de formatos de paquetización multiplexados. En las cláusulas siguientes de este anexo se definen formatos de paquetización de audio adicionales.

Cuadro F.1/H.225.0 – Formatos de paquetización de audio definidos externamente

Nombre de la codificación	Definición de la paquetización
ISO/CEI 14496-3 (MPEG-4 Audio)	IETF RFC 3016, *RTP Payload Format for MPEG-4 Audio/Visual Streams*

Cuadro F.2/H.225.0 – Formatos de paquetización de trenes multiplexados definidos externamente

Nombre de la codificación	Definición de la paquetización
Trenes multiplexados H.222 (trenes de transporte MPEG-2)	IETF RFC 2250, *RTP Payload Format for MPEG1/MPEG2 Video*

F.1 G.723.1

Esta Recomendación especifica una representación codificada que puede utilizarse para la compresión del componente señal vocal de los servicios multimedios a una velocidad binaria muy baja. Una trama G.723.1 puede tener uno de los tres siguientes tamaños: 24 octetos (trama de 6,3 kbit/s), 20 octetos (trama de 5,3 kbit/s) ó 4 octetos. Las tramas de 4 octetos se denominan tramas de descriptor de inserción de silencio (SID, *silence insertion descriptor*) y se utilizan para especificar parámetros de ruido de confort. No hay ninguna restricción con respecto a la forma en que se combinan entre sí las tramas de 4, 20 y 24 octetos. Los dos bits menos significativos del primer octeto de la trama determinan el tamaño de la trama y el tipo de códec (para más información sobre el orden de los bits, véanse los cuadros 5 y 6/G.723.1). Es posible pasar de una a otra de las dos velocidades en cualquier frontera de trama de 30 ms. Ambas velocidades (5,3 kbit/s y 6,4 kbit/s) son parte obligatoria del codificador y decodificador. Este codificador se optimizó para representar la señal vocal con una calidad próxima a la de los enlaces de larga distancia en las velocidades mencionadas utilizando un grado de complejidad limitado.

Todos los bits del tren de bits codificado se transmiten siempre desde el bit menos significativo al bit más significativo. Adviértase que esto se refiere al orden de los bits presentados a la capa de transporte y no al orden de los bits en el hilo conductor.

La paquetización G.723.1 es conforme al anexo B excepto en lo que respecta al intervalo de paquetización (30 ms frente a los 20 ms por defecto):

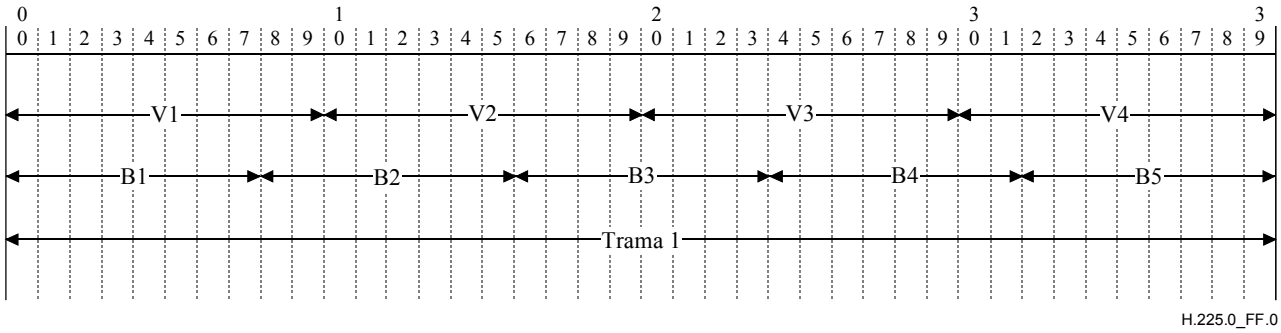
1) El primer paquete de un arranque de palabra (primer paquete tras un periodo de silencio) se distingue fijando el bit marcador en el encabezamiento de datos RTP.
2) La frecuencia de muestreo (frecuencia de reloj RTP) es 8000 Hz.
3) El intervalo de paquetización tendrá una duración de 30 ms (una trama) a diferencia de la paquetización por defecto de 20 ms.
4) Los códecs deben poder codificar y decodificar varias tramas consecutivas dentro de un solo paquete.
5) Un receptor debe aceptar paquetes que representen entre 0 y 180 ms de datos de audio a diferencia de los 0 y 200 ms por defecto.

F.2 G.728

1) *Paquetización de trama*

   Una trama G.728 (4 vectores: V1-V4, 10 bits cada uno, V1 es el más antiguo, el que se ha de reproducir primero) se organiza en 5 octetos (B1-B5). Respecto a la figura que aparece a continuación, el principio para el orden de bits es el de "mantenimiento de la importancia de los bits". Los bits de los vectores más antiguos son más significativos que los bits de los vectores más recientes. El bit más significativo (MSB, *most significant bit*) de la trama pasa

a ser el MSB de B1 y el bit menos significativo (LSB, *least significant bit*) de la trama pasa a ser el LSB de B5. Para mayor claridad: los bits más significativos de cada vector se colocan en los bits más significativos de B1-B5 (los bits más significativos del B de número más bajo).



Por ejemplo:

B1 contiene 8 bits más significativos de V1, el MSB de V1 es el MSB de B1.

B2 contiene 2 bits menos significativos de V2, el más significativo de los dos en su MSB, y 6 bits más significativos de V2, el más significativo de ellos es también más significativo de B2.

B1 será el primero del paquete (el octeto más significativo en RTP) y B5 el último.

2) *Paquetización de multitrama*

El envío de una sola trama en un paquete RTP puede dar lugar a una tara considerable en la red. Por ello se permite enviar un paquete multitrama de la siguiente manera:

Un paquete RTP G.728 deberá contener un número completo de tramas.

Las tramas más antiguas (las que se han de reproducir primero) deberán colocarse las primeras en el paquete RTP.

La indicación de tiempo reflejará el tiempo de captura de la primera muestra, en el primer vector (V1) de la primera trama (la información más antigua en el paquete).

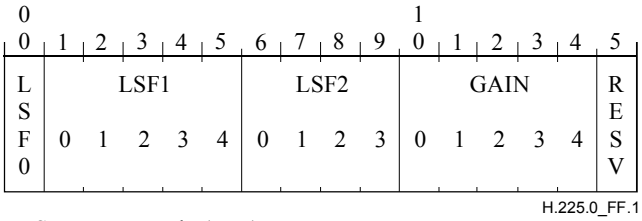
3) El bit marcador mantendrá el mismo significado que se le asigna en esta Recomendación.

F.3 G.729

Esta Recomendación especifica una representación codificada que puede utilizarse para la compresión del componente señal vocal de los servicios multimedios a una velocidad binaria de 8 kbit/s. Este codificador se optimizó para representar la señal vocal con una calidad similar a la de los enlaces de larga distancia o alámbricos en 8 kbit/s. Tiene robustez inherente contra errores aleatorios en los bits así como contra tramas borradas de manera aleatoria y por ráfagas. Representa la señal vocal con alta calidad cuando funciona en un entorno ruidoso. En el anexo A/G.729 se especifica una versión de complejidad reducida del algoritmo G.729. En el anexo C/G.729 se especifica una versión de coma flotante de estos dos algoritmos. Los algoritmos de codificación de habla del cuerpo principal de la Rec. UIT-T G.729, en los anexos A y C/G.729 son plenamente interoperables entre sí, por lo que no es necesaria una ulterior distinción entre ellos.

En el anexo B/G.729 se recomienda un algoritmo detector de actividad vocal (VAD, *voice activity detector*) y generador de ruido de confort (CNG, *comfort noise generator*). Este algoritmo se aplica al anexo F/G.729 (6,4 kbit/s con VAD/CNG), anexo G/G.729 (11,8 kbit/s con VAD/CNG), anexo B/G.729 (G.729 y anexo A/G.729 con VAD/CNG) y anexo I/G.729. Una trama G.729 o trama del anexo A/G.729 contiene 10 octetos; una trama del anexo D/G.729 contiene 8 octetos; una

trama del anexo E/G.729 contiene 15 octetos; y una trama de ruido de confort de los anexos B/G.729, F/G.729 y G/G.729 ocupa 2 octetos, como se muestra en la figura F.1.



RESV = Reservado (cero)

Figura F.1/H.225.0 – Formato de paquetización CNG de los anexos B/G.729, F/G.729 y G/G.729

Los parámetros transmitidos de una trama de 10 ms de G.729, anexo A/G.729 o anexo C/G.729 formada por 80 bits, están definidos en el cuadro 8/G.729. La correspondencia de estos parámetros se presenta en la figura F.2. Los bits están numerados en el mismo orden de Internet, es decir, el bit más significativo es el bit 0.

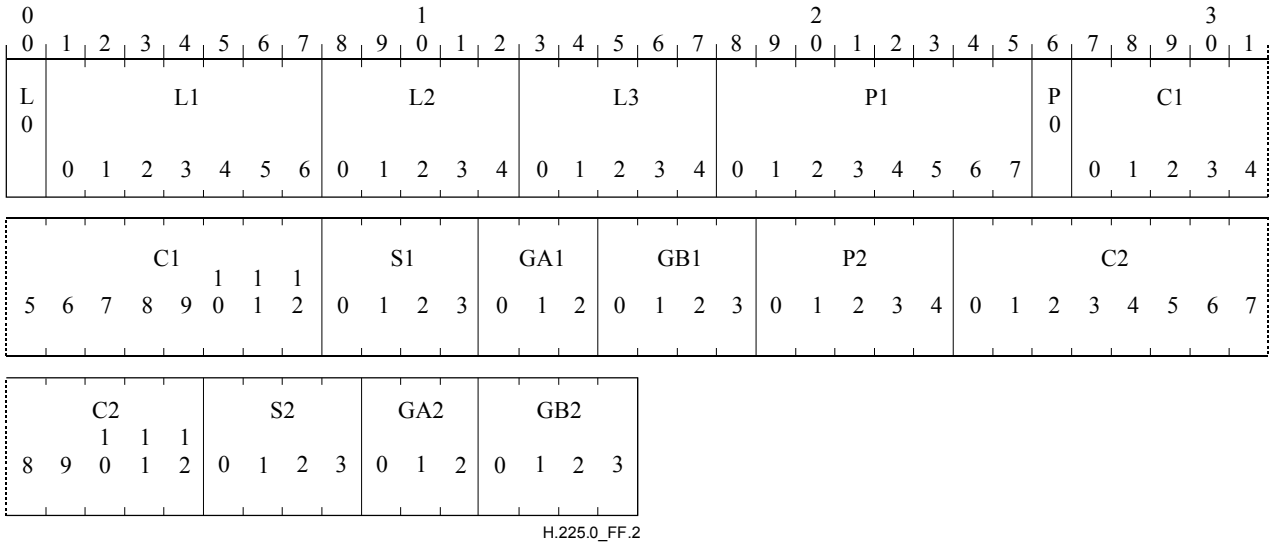


Figura F.2/H.225.0 – Formato de paquetización G.729, anexo A/G.729 y anexo C/G.729

En el anexo D/G.729 se define una ampliación de velocidad de 6,4 kbit/s de G.729 para una reducción momentánea de la capacidad de canal, por ejemplo para tratar situaciones de sobrecarga. En el anexo E/G.729 se proporciona una ampliación de 11,8 kbit/s de G.729 para una mejor calidad de funcionamiento en una vasta gama de señales de entrada, como habla con ruido de fondo y música. Además, el anexo E/G.729 presenta dos modos de funcionamiento, el modo adaptativo hacia atrás y el modo adaptativo hacia adelante, que son señalizados por los dos primeros bits del encabezamiento del paquete.

Los bits de una trama G.729-6,4 están formatados como se muestra en la figura F.3 (véase el cuadro D.1/G.729). Los bits están numerados en el orden de Internet, es decir, el bit más significativo es el bit 0. Se utilizan en total 64 bits.

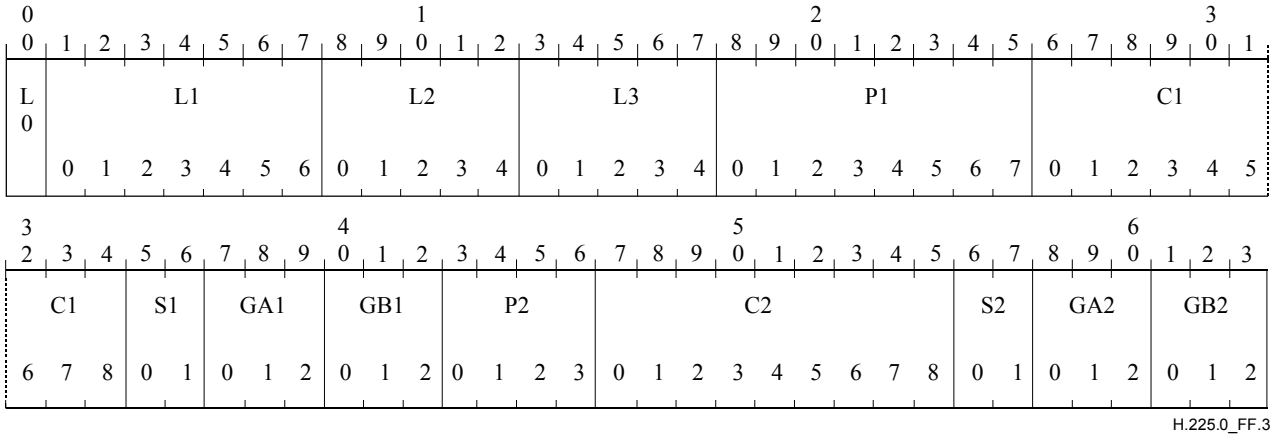


Figura F.3/H.225.0 – Formato de paquetización G.729-6,4

La velocidad binaria neta para el algoritmo del anexo E/G.729 es 11,8 kbit/s y se utilizan en total 118 bits. Los bits de una trama G.729-12 están formatados como se muestra en las figuras F.4 y F.5 (véase el cuadro E.1/G.729). Las figuras F.4 y F.5 describen los campos para los modos adaptativos hacia adelante y hacia atrás, respectivamente, del algoritmo del anexo E/G.729. Los dos bits menos significativos se incluyen como bits "intrascendentes" y se insertan con la finalidad de que la trama tenga un número entero de octetos.

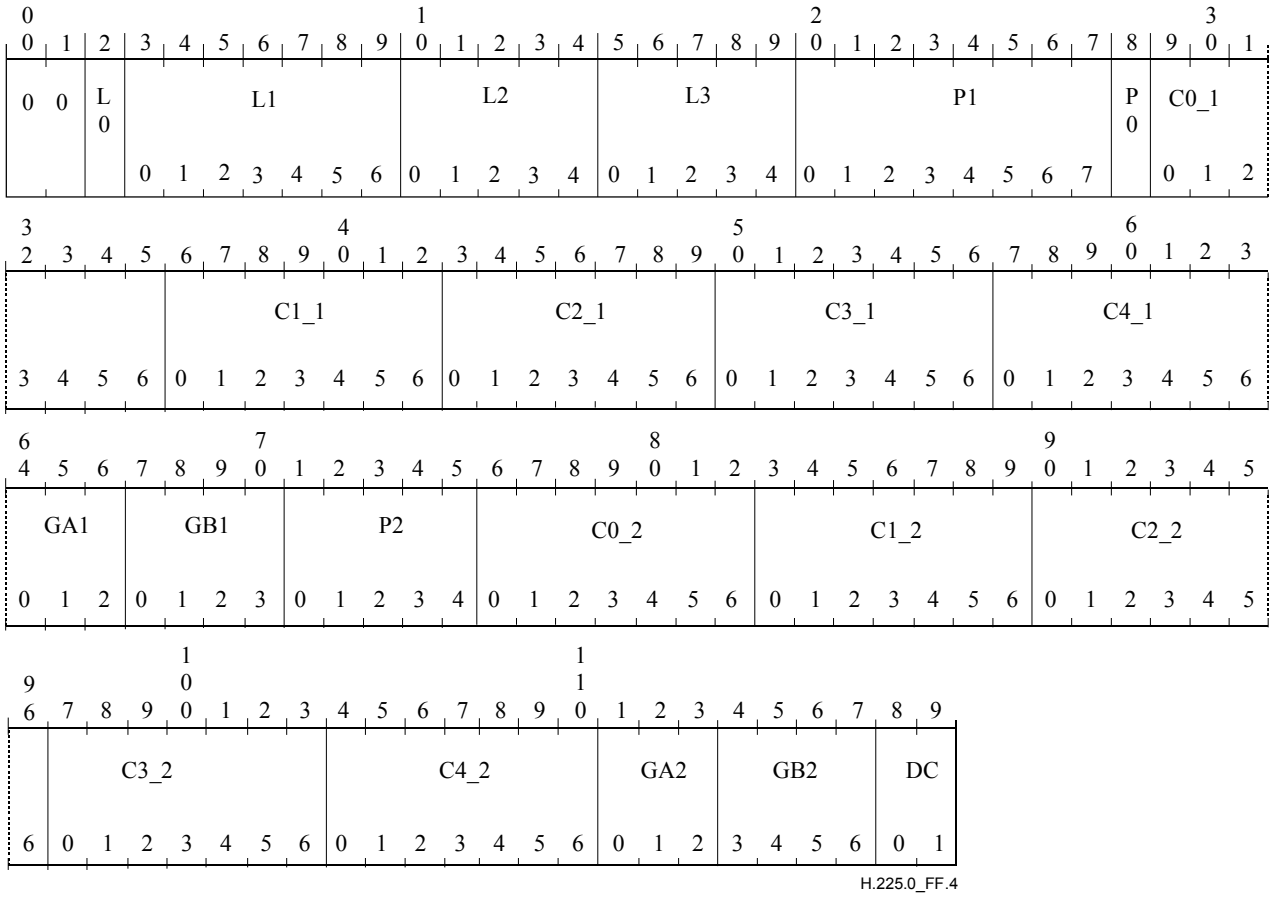


Figura F.4/H.225.0 – Formato de paquetización G.729-12 para el modo adaptativo hacia adelante

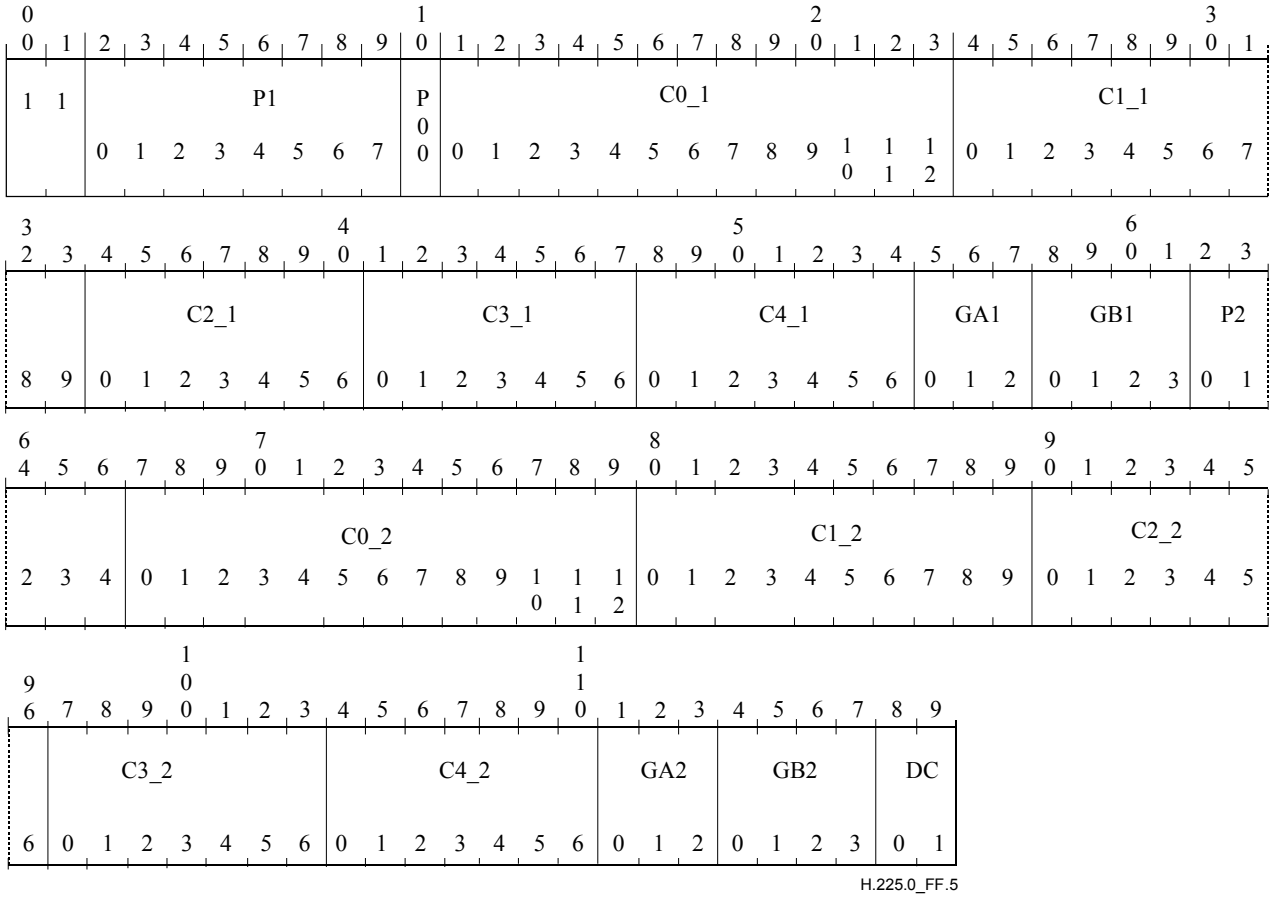


Figura F.5/H.225.0 – Formato de paquetización G.729-12 para el modo adaptativo hacia atrás

Un paquete RTP puede constar de cero o más tramas G.729 o tramas de los anexos A, C, D o E/G.729 seguidas de cero o una cabida útil del anexo B/G.729. La presencia de una trama de ruido de confort puede deducirse a partir de la longitud de la cabida útil RTP.

1) El primer paquete de un arranque de palabra (primer paquete tras un periodo de silencio) se distingue fijando el bit marcador en el encabezamiento RTP.

2) La frecuencia de muestreo (frecuencia de reloj RTP) es 8000 Hz.

3) El intervalo de paquetización por defecto deberá tener una duración de 20 ms. Aunque el valor de 20 ms se recomienda encarecidamente en algunas situaciones quizá convenga enviar paquetes de 10 ms. Considérese, por ejemplo, el tránsito de voz a ausencia de voz en los primeros 10 ms del paquete. Si fuese obligatorio un intervalo de paquetización de 20 ms, el transmisor tendría que esperar hasta que la señal vocal estuviera activa de nuevo.

4) Los códecs deben poder codificar y decodificar varias tramas consecutivas dentro de un solo paquete.

5) Un receptor debe aceptar paquetes que representen entre 0 y 200 ms de datos de audio.

F.4 Supresión de silencio

La Rec. UIT-T H.225.0 indica que los codificadores pueden enviar tramas de silencio antes de interrumpir la transmisión durante un periodo de silencio. Dado que no todos los codificadores de audio tienen señalización dentro de banda para silencio, se debe definir un mecanismo general a nivel del RTP. Por ejemplo, se podría enviar un paquete RTP vacío. Este asunto queda en estudio.

F.5 Códecs GSM

Los códecs de señales vocales GSM incluyen: GSM de velocidad total (FR, *full rate*) [F-1], GSM de media velocidad (HR, *half rate*) [F-2] y GSM de velocidad total mejorado (EFR, *enhanced full rate*) [F-3]. Cada códec produce tres tipos de trama de tráfico de señal vocal diferentes, a saber:

- Tramas de señales vocales: Contiene datos de señales vocales verdaderos.
- Tramas inactivas: Indica que no hay actividad vocal; todos los bits de datos están puestos a uno.
- Tramas de descriptor de silencio (SID, *silence descriptor*): Indica el comienzo de un periodo de silencio, los datos describen el ruido de fondo. Las tramas SID se marcan dentro de banda con un diagrama de bits fijo.

F.5.1 Paquetización de tramas

Con los tres códecs GSM los bits de trama de tráfico de señales vocales se empacan con el bit más significativo (MSB) de trama del RTP primero. Un paquete RTP puede contener una o más tramas de tráfico de señales vocales GSM. Todos los puntos extremos deben poder recibir e identificar una trama inactiva. Una trama de señales vocales GSM inactiva se rellena con unos binarios.

Si un punto extremo fija el parámetro `comfortNoise` en `VERDADERO`, enviará tramas SID como se indica en las especificaciones de ruido nivelador y transmisión discontinua (DTX, *discontinous transmission*) de un código GSM particular. Durante un periodo de silencio, se envía periódicamente una nueva trama SID con información de ruido (posiblemente) actualizada, es decir, cada 24 tramas. Después de un periodo de silencio, el bit marcador se pone a 1 en el encabezamiento RTP.

Códec de velocidad total

El códec de velocidad total GSM envía una trama de 260 bits (32,5 octetos) cada 20 ms. Esta información será empacada en la trama RTP con un prefijo de cuatro bits (0xD u 1101 binarios), denominado signatura. Por tanto, la cabida útil FR del GSM dentro del transporte en tiempo real RTP comprenderá 33 octetos. La trama del descriptor de silencio (SID) viene marcada dentro de banda por una palabra de código SID almacenada en parámetros códec como se describe en la referencia [F-4]. La dimensión de la cabida útil de una trama SID es de 33 octetos. La signatura de una trama SID de velocidad plena será la misma que la trama de señales vocales de velocidad plena (0xD). Las señales vocales de velocidad plena codificadas en RTP tendrán una velocidad binaria de 13 200 bit/s, no incluida la tara de paquetización.

Códec de media velocidad

El códec de media velocidad GSM envía una trama de 112 bits (14 octetos) cada 20 ms. Esta información se empacará dentro de un encabezamiento RTP sin ningún prefijo ni signatura. La trama SID está marcada dentro de banda por una palabra de código SID almacenada en parámetros códec como se describe en la referencia [F-4]. El tamaño de la cabida útil de una trama SID es de 14 octetos. Las señales vocales codificadas del RTP tendrán una velocidad binaria de 5600 bit/s, no incluida la tara de paquetización.

Velocidad total mejorado

El códec de velocidad total mejorado (EFR) del GSM envía una trama de 244 bits (30,5 octetos) cada 20 ms. Esta información será empacada dentro de un encabezamiento RTP con un prefijo de 4 bits (0xC o 1100 binarios), denominado signatura. La cabida útil de la velocidad total mejorado del GSM dentro del RTP constará de 31 octetos. La trama SID viene marcada dentro de banda por una palabra de código SID almacenada en parámetros códec como se describe en la referencia [F-4]. El tamaño de la cabida útil de una trama SID es de 31 octetos. Las señales vocales de

velocidad plena mejorada codificadas en el RTP tendrán una velocidad binaria de 12 400 bit/s, no incluida la tara de paquetización.

F.5.2 Referencias informativas

[F-1] GSM 06.10 (ETS 300 961), *Digital cellular telecommunications system; Full rate speech; Transcoding*.

[F-2] GSM 06.60 (ETS 300 726), *Digital cellular telecommunications system; Enhanced Full Rate (EFR) speech transcoding*.

[F-3] GSM 06.20 (ETS 300 969), *Digital cellular telecommunications system; Half rate speech; Half rate speech transcoding*.

[F-4] ETSI, TIPHON 03 001 (TS 101 318), *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Using GSM speech codecs within ITU-T Recommendation H.323*.

[F-5] GSM 06.31 (ETS 300 963), *Digital cellular telecommunications system; Full rate speech; Comfort noise aspect for full rate speech traffic channels*.

[F-6] GSM 06.81 (ETS 300 729), *Digital cellular telecommunications system; Discontinuous Transmission (DTX) for Enhanced Full Rate (EFR) speech traffic channels*.

[F-7] GSM 06.41 (ETS 300 972), *Digital cellular telecommunications system; Half rate speech; Discontinuous Transmission (DTX) for half rate speech traffic channels*.

[F-8] GSM 06.12 (ETS 300 963), *Full rate speech; Comfort noise aspect for full rate speech traffic channels*.

[F-9] GSM 06.62 (ETS 300 728), *Digital cellular telecommunications system; Comfort noise aspects for Enhanced Full Rate (EFR) speech traffic channels*.

[F-10] GSM 06.22 (ETS 300 971), *Digital cellular telecommunications system; Half rate speech; Comfort noise aspect for the half Rate speech traffic channels*.

[F-11] GSM 08.60 (ETS 300 737), *Digital cellular telecommunications system; (Phase 2+) (GSM); In-band control of remote transcoders and rate adaptors for Enhanced Full Rate (EFR) and full rate traffic channels*.

F.6 G.722.1

El algoritmo de codificación de habla definido en la Rec. UIT-T G.722.1 codifica señales de audio de banda ancha con frecuencias de 50 Hz a 7 kHz a una o dos velocidades binarias, 24 kbit/s o 32 kbit/s, utilizando tramas de 20 ms y una velocidad de muestreo de 16 kHz. La velocidad binaria puede cambiarse en cualquier demarcación de trama de 20 ms, si bien la notificación del cambio de la velocidad binaria no se proporciona dentro de banda con el tren de bits. En el caso del funcionamiento a 24 kbit/s se producen 480 bits (60 octetos) por trama, y en el caso del funcionamiento a 32 kbit/s se producen 640 bits (80 octetos) por trama. Por tanto, ambas velocidades binarias permiten la alineación de octetos sin necesidad de bits de relleno.

Una trama consta de un número fijo de bits. Sin embargo, dentro de esta trama de longitud fija, G.722.1 utiliza una codificación de longitud variable (por ejemplo la codificación Huffman) para representar la mayor parte de los parámetros codificados. Todos los parámetros de los trenes de bits, salvo los constituidos por los bits de control de categorización, se representan por códigos de longitud variable, con un número variable de bits. La figura F.6 ilustra este punto y el orden de los campos de parámetro transmitidos. Todos los códigos de longitud variable y los bits de categorización se transmiten en orden desde el bit más a la izquierda [bit más significativo (MSB)], hasta el bit más a la derecha [bit menos significativo (LSB)]. Al utilizarse la codificación Huffman

no existe la posibilidad de identificar los diversos parámetros/campos del codificador contenidos en el tren de bits sin que antes se haya finalizado la decodificación de la trama completa.

La figura F.7 ilustra la forma en que el tren de bits G.722.1 corresponde a una cabida útil RTP alineada en octetos. La cadena de bits del codificador se divide en una secuencia de octetos (60 u 80 según la velocidad binaria), y cada octeto se hace corresponder, a su vez, con un octeto RTP.

Un paquete RTP contendrá solamente tramas G.722.1 de la misma velocidad binaria. La indicación de tiempo RTP se dará en unidades de 1/16 000 de segundo.

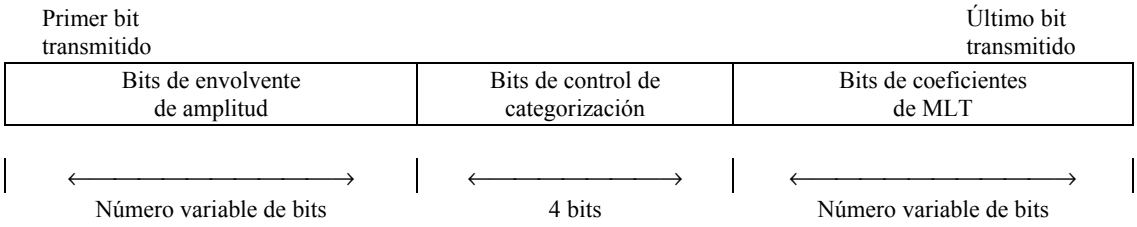


Figura F.6/H.225.0 – Principales campos de los trenes de bits G.722.1 y su orden de transmisión

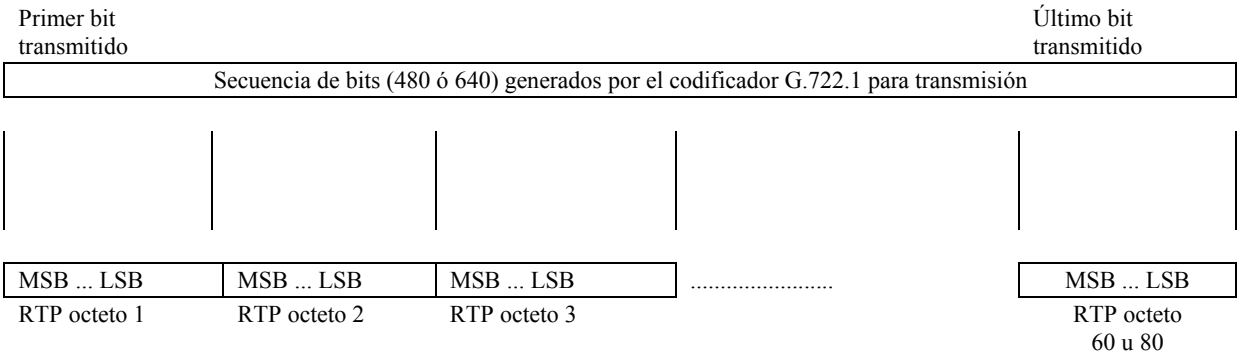


Figura F.7/H.225.0 – Correspondencia de un tren de bits codificado al protocolo RTP

F.7 TIA/EIA-136 ACELP

Este codificador de señales vocales (brevemente, vocodificador) está optimizado para sistemas celulares digitales TIA/EIA-136 TDMA y sistemas PCS. Incluye capacidades de detección de actividad vocal (VAD), sustitución de tramas perdidas y generación de ruido de confort (CNG). La velocidad de muestreo es 8000 Hz y la longitud de trama vocal comprimida es de 20 ms. El vocodificador produce un vector de habla de 148 bits, s0 a s147, para cada trama vocal de 20 ms. s0 es el bit más significativo (MSB). Para más detalles, véase la sección 4 de la referencia [F7-1].

F.7.1 Formato de trama TIA/EIA-136 ACELP

El vocodificador generará un bit de bandera de indicador, SP, que se pondrá a "1" para indicar una trama de habla, o a "0" para indicar una trama de silencio (ruido de confort). Este bit de bandera SP se insertará en la posición de bit 148. La posición de bit 149 es la del BFI_CN (indicador de trama mala o ruido de confort) y la posición de bit 150 es la de la bandera de actualización de ruido de confort (CNU, *comfort noise update*). La posición de bit 151 se pondrá siempre a 0.

A continuación se describen las combinaciones lógicas de estas tres banderas.

La trama de transmisión de 152 bits (19 octetos) se representa en la siguiente figura F.8. Los octetos se forman empezando por el LSB y avanzando hacia el MSB. El LSB se transmite primero.

bit 0 (MSB)	1 … 146	147	148	149	150	bit 151 (LSB)
s0	s1… s146	S147	SP	BFI_CN	CNU	Siempre 0
Vector de habla/ruido de confort			Bandera	Bandera	Bandera	Bit de relleno

Figura F.8/H.225.0 – Trama vocal de vocodificador ACELP

F.7.2 Modo supresión de silencio de TIA/EIA-136 ACELP

En modo silencio, el vocodificador genera una representación de trama de ruido ambiente. El vocodificador utiliza esta trama en el extremo receptor para regenerar el ruido ambiente del extremo transmisor. El vector de parámetros CN (ruido de confort) consta de sólo 38 bits, al final de los cuales se agregan los tres bits de bandera y siete bits de relleno (de valor todos ceros) para formar una trama de seis octetos.

La trama CN de 48 bits (6 octetos) se representa en la siguiente figura F.9. Los octetos se forman empezando por el LSB y avanzando hacia el MSB. El LSB se transmite primero.

bit 0 (MSB)	1 … 37	38	39	40	41	41-47 (LSB)
Cn0	cn1… cn37	S147	SP	BFI_CN	CNU	Siempre 0
Vector de habla/ruido de confort			Bandera	Bandera	Bandera	Bit de relleno

Símbolos utilizados:

SP Indicador de habla
BFI_CN Indicador de trama mala/indicador de ruido de confort
CNU Actualización de ruido de confort

A continuación se definen los valores lógicos de estas banderas y sus significados:

SP: 1 = trama de habla; 0 = ausencia de habla (trama de ruido de confort)

BFI_CN:
Si SP = 1
Y BFI_CN = 1
Entonces, ésta es una trama vocal mala
En otro caso (BFI_CN = 0), ésta es una trama vocal buena

Si SP = 0
Y BFI_CN = 1
Entonces, ésta es una trama de ruido de confort mala
En otro caso (BFI_CN = 0), ésta es una trama de ruido de confort buena

CN:
Si SP = 0
Y BFI_CN = 0
Y CN = 1
Entonces, ésta es una trama de actualización de ruido de confort
En otro caso, ésta es una trama CN no válida

NOTA – Un vocodificador móvil inalámbrico fijará el BFI_CN a 0. La estación de base receptora podrá fijar esta bandera a 1 si no tiene capacidad para corregir errores introducidos por el canal de radio.

Figura F.9/H.225.0 – Trama de supresión de silencio del vocodificador ACELP

F.7.3 Paquetización de TIA/EIA-136 ACELP

La paquetización de IS-ACELP será conforme al anexo B.

1) La duración de la paquetización será un múltiplo entero de 20 ms.
2) Cada paquete puede estar formado por una o más tramas.
3) Los códecs podrán codificar y decodificar varias tramas consecutivas en un mismo paquete.
4) Todos los bits del tren de bits decodificado se transmiten comenzando por el bit menos significativo y terminando por el bit más significativo.

F.7.4 Normas de TIA/EIA-136 ACELP a que se hace referencia

[F7-1] TIA/EIA-136, part 410, *TDMA Cellular/PCS – Radio Interface, Enhanced Full Rate Voice Codec (ACELP)*. Anteriormente IS-641.

F.8 TIA/EIA-136 US1

Este vocodificador está optimizado para sistemas celulares digitales TIA/EIA-136 TDMA y PCS. La referencia [F8-1] proporciona una descripción detallada del vocodificador.

F.8.1 Formato de trama TIA/EIA-136 US1

La velocidad de muestro es de 8000 Hz y la longitud de trama vocal comprimida es de 20 ms. El vocodificador produce 244 bits ordenados por cada trama vocal. Se añaden tres bits de bandera, BFI, SID y TAF, al vector de habla. Se añade un bit de relleno (en la posición de bit 247) para formar un número entero de octetos (31 octetos). El último bit es el bit menos significativo (LSB). Este vocodificador soporta también el modo silencio de transmisión discontinua (DTX).

La estructura de la trama vocal en transmisión se muestra en la figura F.10.

MSB – bit 0	**1 … 243**	**244**	**245**	**246**	**247 (LSB)**
s0	s1 … s243	BFI	SID	TAF	Siempre 0
Vector de habla		Bandera	Bandera	Bandera	Bit de relleno

Figura F.10/H.225.0 – Trama vocal del vocodificador US1

F.8.2 Tramas en modo silencio de TIA/EIA-136 US1 (TX-DTX)

En el modo silencio, se transmiten tramas especiales denominadas tramas SID (abreviatura del término inglés *silence descriptor*) según un calendario especificado en la sección 1.3 de la referencia [F8-1].

Una trama SID contiene el mismo número de bits que las tramas de habla normales, pero el mapa de bits es diferente. Para más detalles, véase la referencia [F8-1]. La trama SID contiene parámetros de ruido de confort (CN, *comfort noise*) y una palabra de código SID de 95 bits. La palabra de código SID es todos "0". Otros bits no utilizados en la cabida útil del vector de 244 bits también se ponen a "0". (Véase la figura F.11.)

MSB – bit 0	**1 … 243**	**244**	**245**	**246**	**247 (LSB)**
cn0	cn1 … cn243	BFI	SID	TAF	Siempre 0
Vector de ruido de confort		Bandera	Bandera	Bandera	Bit de relleno

Figura F.11/H.225.0 – Trama de transmisión de ruido de confort, de estación de base a línea terrestre (US1)

La lógica de las banderas BFI, SID y TAF es similar a la de las banderas equivalentes del vocodificador TIA/EIA-136 ACELP, descrito en F.7.

F.8.3 Paquetización de TIA/EIA-136 US1

Esta paquetización será conforme al anexo B.

1) La duración de la paquetización será un múltiplo entero de 20 ms.
2) Cada paquete puede estar formado por una o más tramas.
3) Los códecs podrán codificar y decodificar varias tramas consecutivas en un mismo paquete.
4) Todos los bits del tren de bits decodificado se transmiten siempre comenzando por el bit menos significativo y terminando por el bit más significativo.

F.8.4 Normas TIA/EIA-136 US1 a que se hace referencia

[F8-1] TIA/EIA-136, part 430, *TDMA Cellular/PCS – Radio Interface, US1 Full Rate Voice Codec*.

F.9 Códec EVRC IS-127

F.9.1 Descripción del códec EVRC IS-127

F.9.1.1 Generalidades

El códec mejorado de velocidad variable (EVRC, *enhanced variable rate codec*) TIA/EIA IS-127 está optimizado para sistemas celulares digitales TIA/EIA IS-95 CDMA y PCS. La velocidad de muestreo es de 8000 muestras por segundo y la longitud de trama vocal es de 20 ms (es decir, 160 muestras por trama). EVRC codifica habla activa a plena velocidad o a media velocidad, y ruido de fondo (sin habla presente) a un octavo de velocidad. El códec entrega habla de la calidad de la telefonía interurbana a una velocidad binaria promedio muy baja. Una descripción detallada del códec EVRC puede encontrarse en la norma TIA/EIA IS-127 [F9-1], que ya ha sido publicada.

F.9.1.2 Tasas de compresión

El códec EVRC comprime su señal de entrada utilizando una de tres tasas de compresión: compresión a plena tasa de compresión (tasa 1), a media tasa de compresión (tasa de 1/2), y a un octavo de tasa de compresión (tasa de 1/8). La compresión a plena tasa y a media tasa se utilizan principalmente para la codificación de habla activa, en tanto que la compresión a un octavo de tasa se utiliza para la codificación de ruido de fondo (modo silencio). Todas la tramas tienen una longitud de 20 ms, cualquiera que sea la velocidad de codificación.

F.9.1.3 Paquetes dejados en blanco

Para permitir señalización dentro de banda o tráfico secundario (véase la sección 1.4.1 de [F9-1]), las tramas vocales se dejan en blanco. El paquete vocal generado, simplemente, no se utiliza, y el decodificador lo trata como un paquete borrado. Para más detalles, véase [F9-1].

F.9.1.4 Media velocidad

Se utiliza la codificación a media velocidad, en lugar de la codificación normal a plena velocidad, cuando hay que añadir un mensaje de señalización al canal de tráfico.

F.9.1.5 Datos nulos transmitidos por un canal de tráfico a 1/8 de velocidad

Se considera que un paquete en el que todos los bits están puestos a "1" y que se transmite a un octavo de velocidad contiene datos de canal de tráfico nulo. Tales paquetes se declaran como "paquetes borrados" y se tratan como se describe en la sección 5 de [F9-1].

A los bits de salida del vocodificador se añaden bits de información de velocidad y de codificación de canal, para su transporte inalámbrico, de acuerdo con TIA/EIA IS-95.

En el siguiente cuadro F.3 se muestran los tipos de paquetes, el número de bits por paquete, las velocidades binarias brutas del vocodificador y las velocidades agregadas (bits del vocodificador más bits adicionales).

Cuadro F.3/H.225.0 – Paquetes y velocidades binarias del EVRC

Tipo de paquete (3 bits)	Velocidad	Bits/paquete	Velocidad binaria del vocodificador kbit/s	Velocidad agregada kbit/s
1	Plena	171	8,55 kbit/s	9,6 kbit/s
2	Media velocidad	80	4,0 kbit/s	4,8 kbit/s
3 (Nota)	Un cuarto (compatibilidad con opción de servicio 1)	40		
4	Un octavo	16	0,8 kbit/s s	1,2 kbit/s
5	En blanco	0	–	–
6	Plena velocidad con errores	171	–	–
7	Trama mala (paquetes borrados)	0	–	–
NOTA – Los paquetes de tipo 3 sólo pueden ser generados por codificadores IS-96 antiguos. El decodificador IS-127 tratará estos paquetes como paquetes borrados.				

F.9.2 Paquetización del EVRC IS-127

F.9.2.1 Requisitos generales

La paquetización de la transmisión será conforme al anexo B.

1) La duración de la paquetización será un múltiplo entero de 20 ms.
2) Cada paquete puede estar formado por ninguna, una o más tramas.
3) Los códecs podrán codificar y decodificar varias tramas consecutivas en un mismo paquete de transmisión.
4) Todos los bits del tren de bits decodificado se transmitirán siempre comenzando por el bit menos significativos y terminando por el bit más significativo.

F.9.2.2 Formatos de trama

F.9.2.2.1 Trama a plena velocidad – F1

La trama de transmisión a plena velocidad del EVRC, de 176 bits (22 octetos), (F1), se representa en la siguiente figura F.12. Los octetos se forman empezando por el LSB y avanzando hacia el MSB. El LSB (bit 175) se transmite primero.

Bit 0 (MSB)	Bits 1 a 170	Bits 171 a 175 (LSB)
s0	s1… s170	Siempre 0
Vector de habla		Bits de relleno

Figura F.12/H.225.0 – Trama EVRC a plena velocidad, F1

F.9.2.2.2 Trama a media velocidad – F2

La trama de transmisión a media velocidad del EVRC, de 80 bits (10 octetos), (F2), se representa en la siguiente figura F.13. Los octetos se forman empezando por el LSB y avanzando hacia el MSB. El LSB (bit 79) se transmite primero.

Bit 0 (MSB)	Bits 1 a 79 (LSB)
s0	s1… s79
Vector de habla	

Figura F.13/H.225.0 – Trama EVRC a media velocidad, F2

F.9.2.2.3 Trama a un octavo de velocidad – F3

La trama de transmisión a un octavo de velocidad del EVRC, de 16 bits (2 octetos) (F3) se representa en la siguiente figura F.14. Los octetos se forman empezando por el LSB y avanzando hacia el MSB. El LSB (bit 15) se transmite primero.

Bit 0 (MSB)	Bits 1 a 15 (LSB)
s0	s1… s15
Vector de habla	

Figura F.14/H.225.0 – Trama EVRC a un octavo de velocidad, F3

F.9.3 Normas IS-127 EVRC a que se hace referencia

[F9-1] TIA/EIA IS-127 (1997), *Enhanced Variable Rate Codec, Speech Service Option 3 for Wideband Spread Spectrum Digital Systems*.

[F9-2] TIA/EIA IS-95-B (1999), *Mobile Station-Base Station Compatibility Standard for Wideband Spread Spectrum Cellular Systems*.

F.10 Paquetización de MUX-PDU H.223

F.10.1 Introducción

La paquetización de MUX-PDU H.223 es la utilizada por un protocolo de multiplexación basado en paquetes para el intercambio de uno o más trenes de información entre entidades de capa superior tales como protocolos de datos y de control y códecs de audio y vídeo, como se define en la Rec. UIT-T H.223.

Cada tren de información se representa por un canal lógico unidireccional H.245 que se identifica por un número de canal lógico (LCN, *logical channel number*) único, que es un número entero entre 0 y 65535. LCN 0 es un canal lógico permanente asignado al canal de control H.245. Todos los demás canales lógicos son abiertos y cerrados dinámicamente por el transmisor utilizando los mensajes OpenLogicalChannel H.245 y CloseLogicalChannel. Todos los atributos necesarios del canal lógico se especifican en el mensaje OpenLogicalChannel. Para aplicaciones que requieren un canal en el sentido opuesto de transmisión, en la Rec. UIT-T H.245 también se define un procedimiento para abrir canales lógicos bidireccionales.

La estructura general del multiplexor se muestra en la figura 2/H.223. El multiplexor consta de dos capas distintas: una capa de múltiplex (MUX) una capa de adaptación (AL, *adaptation layer*).

El soporte del tipo de cabida útil H.223 se señaliza utilizando conjuntos de capacidades H.245 y, en el mensaje openLogicalChannel H.245, utilizando tipos de cabida útil dinámica RTP.

F.10.2 Formato de paquetización de MUX-PDU

La MUX-PDU H.223 especificada por la figura 3/H.223 se transporta como datos de cabida útil dentro del protocolo RTP. El orden de transmisión de los bits se especifica en 3.2.2/H.223, y el convenio para la correspondencia de los campos se presenta en 3.2.3/H.223.

Aunque una MUX-PDU puede ocupar más de un paquete RTP, una MUX-PDU comenzará por el primer octeto de una cabida útil de paquete RTP.

Cada paquete RTP contiene una indicación de tiempo que se obtiene a partir de la referencia de reloj del emisor. La indicación de tiempo representará el tiempo de transmisión deseado del primer octeto de la MUX-PDU H.223. La finalidad primordial de esta indicación de tiempo es permitir que el receptor calcule y reduzca toda fluctuación de fase inducida por la red y reproduzca el tren de bits H.223 con un velocidad binaria constante.

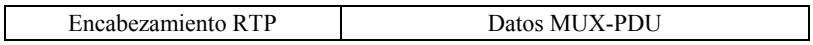
Los campos del encabezamiento RTP se utilizarán como sigue:

1) Se utiliza un tipo de cabida útil dinámica RTP.

2) La indicación de tiempo RTP representa el tiempo de transmisión deseado para el primer octeto de la MUX-PDU en el paquete a través del canal a velocidad binaria constante H.223. Esta indicación de tiempo se obtiene a partir de la frecuencia de reloj cuyo valor por defecto es de 90 kHz. El emisor puede cambiar esta frecuencia y el valor seleccionado se señaliza por el parámetro **BitRate** de la estructura **H223Capability** en mensajes H.245. Si una MUX-PDU ocupa más de un paquete RTP, la indicación de tiempo RTP será la misma en paquetes sucesivos. El cálculo de la indicación de tiempo deberá basarse en el número de octetos incluidos en las MUX-PDU transmitidas.

3) El bit marcador del encabezamiento RTP se pone a uno en el último paquete de una MUX-PDU, y en todos los demás caso debe ser cero. Por tanto, para detectar la demarcación de la MUX-PDU, no es necesario esperar hasta que llegue el paquete siguiente.

La MUX-PDU H.223 sigue al encabezamiento RTP, como se muestra a continuación:



Anexo G

Comunicación entre dominios administrativos

G.1 Alcance

Se prevé que la red H.323 global estará formada por subconjuntos más pequeños de equipos organizados de alguna manera, por ejemplo, por dominios administrativos. Debido al número potencialmente grande de elementos H.323 que existirá en las redes H.323, se necesita un protocolo eficaz para poder completar las llamadas entre dominios administrativos. El ejemplo más elemental es el de un usuario (un punto extremo) en un dominio administrativo que comunica con un usuario (un punto extremo) servido por otro dominio administrativo. Aunque el protocolo RAS H.225.0 puede tratar muchas de las necesidades de comunicación entre dominios administrativos, no está completo ni es eficaz a estos efectos.

Por el mismo motivo, es necesario también especificar un protocolo eficaz entre elementos H.323 dentro del mismo dominio administrativo.

El presente anexo describe los métodos que permiten la resolución de dirección, la autorización del acceso y la notificación de utilización entre dominios administrativos y dentro de éstos en los sistemas H.323 para completar llamadas. Los elementos H.323 que comunican mediante el procedimiento descrito en este anexo se conocen como elementos pares. Un dominio administrativo se muestra a los otros dominios administrativos a través de un tipo de elemento lógico conocido

como elemento de frontera. Los elementos de frontera son casos especiales de los elementos pares, por lo menos uno de cuyos pares pertenece a otro dominio administrativo. Un elemento par puede estar coubicado con cualquier otra entidad (por ejemplo, con un controlador de acceso). Según el anexo G, un dominio administrativo no tiene que revelar detalles sobre su organización o arquitectura. El anexo G no impone una arquitectura de sistema específica dentro de un dominio administrativo. Además, el anexo G soporta el uso de cualquier modelo de llamada (encaminamiento a través de un controlador de acceso o directamente hasta el punto extremo).

De acuerdo con el procedimiento general, los elementos pares intercambian información sobre las direcciones que cada dominio administrativo puede resolver. Los elementos de frontera intercambian información sobre las direcciones que sus dominios administrativos pueden resolver. Las direcciones pueden ser especificadas de manera general o con especificidad creciente. La información adicional permite que los elementos dentro de un dominio administrativo determinen el dominio administrativo más apropiado como destino para la llamada. Los elementos de frontera pueden controlar el acceso a sus direcciones presentadas, y requerir informes sobre la utilización hecha durante las llamadas a dichas direcciones.

En la figura G.1 se indican varios puntos de referencia que representan la señalización entre varios elementos en una red H.323. En la figura G.1, los dominios administrativos forman parte de una red de paquetes global sin bordes. Obsérvese que la figura G.1 no es una definición explícita de una arquitectura de sistema H.323, sino que ilustra los puntos de referencia de señalización.

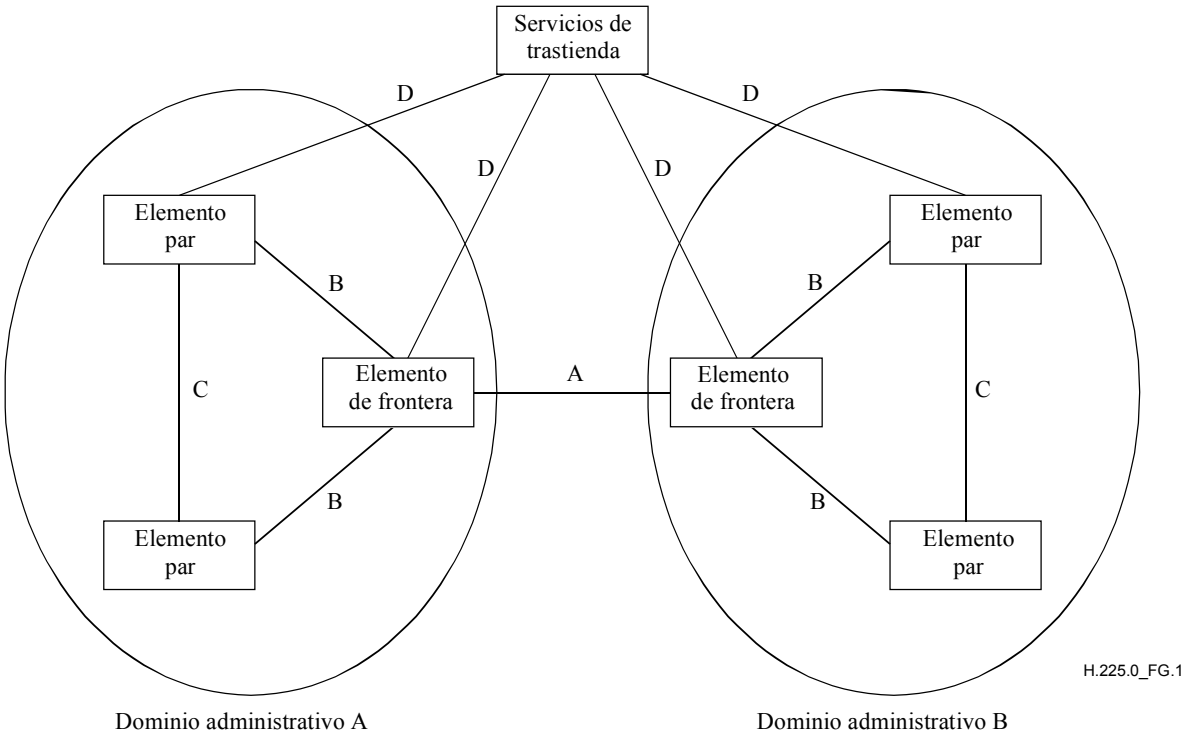


Figura G.1/H.225.0 – Puntos de referencia del sistema

En la figura G.1 se indican los siguientes puntos de referencia:

A – entre elementos de frontera pertenecientes a diferentes dominios administrativos.

B – entre elementos de frontera y elementos pares dentro del mismo dominio.

C – entre elementos pares dentro del mismo dominio.

D – entre elementos H.323 y servicios de trastienda (fuera del ámbito del presente anexo).

Los puntos de referencia A, B y C son el tema central de este anexo. Como se indica anteriormente, un elemento par puede estar coubicado con algún otro elemento H.323.

La cláusula G.7, Ejemplos de señalización, proporciona algunos ejemplos de señalización que pueden facilitar la comprensión.

G.2 Definiciones

En este anexo se definen los términos siguientes.

G.2.1 dominio administrativo: Conjunto de entidades H.323 administradas por una entidad administrativa. Un dominio administrativo puede constar de uno o varios controladores de acceso (es decir, una o varias zonas).

G.2.2 servicios de trastienda: Funciones tales como autenticación o autorización de usuario, contabilidad, facturación, tasación/tarificación, etc. Los servicios de trastienda y el protocolo para intercambiar información con dichos servicios (si son diferentes de los que figuran en este anexo) están fuera del ámbito del presente anexo.

G.2.3 elemento par: Como se define en la Rec. UIT-T H.501, un elemento par es un elemento lógico que origina o termina mensajes de señalización definidos en dicha Recomendación. Este elemento puede existir en combinación con otros elementos H.323, por ejemplo, una combinación de elemento par, controlador de acceso y pasarela. Un dominio administrativo puede contener cualquier número de elementos pares.

G.2.4 elemento de frontera: El elemento de frontera, que es un caso especial de elemento par, es un elemento funcional que tiene como mínimo un par que está fuera de su dominio administrativo. Permite el acceso público a un dominio administrativo a los efectos de la compleción de llamada o cualesquiera otros servicios que comprenden comunicación multimedios con otros elementos dentro del dominio administrativo. El elemento de frontera controla la visión externa del dominio administrativo.

G.2.5 centro de resolución: Servicio (posiblemente en forma de elemento de frontera) que puede resolver todas las direcciones (es decir, un tipo de punto de agregación).

G.3 Abreviaturas

En este anexo se utilizan las siguientes siglas.

AD Dominio administrativo (*administrative domain*)

BE Elemento de frontera (*border element*)

CH Centro de resolución (*clearing house*)

DST Diferencia por la hora de verano (*daylight saving time*)

EP Punto extremo (*endpoint*)

GK Controlador de acceso (*gatekeeper*)

GW Pasarela (*gateway*)

PE Elemento par (*peer element*)

RCC Red con conmutación de circuitos

T Terminal

G.4 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 Versión 4 (2000), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.

[2] Recomendación UIT-T H.235 Versión 2 (2000), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.

[3] Recomendación UIT-T H. 323 Versión 4 (2000), *Sistemas de comunicación multimedios basados en paquetes*.

[4] Recomendación UIT-T H.323 (2000) anexo K, *Canal de transporte de control de servicio basado en hipertexto (incorporado en H.323)*.

[5] Recomendación UIT-T H.501 (2002), *Protocolo para la gestión de movilidad y la comunicación intradominio e interdominio en los sistemas multimedios*.

[6] Recomendación UIT-T H.460.2 (2001), *Interfuncionamiento de la portabilidad de número entre una red H.323 y una red con conmutación de circuitos*.

G.5 Modelos de sistema

El anexo G no impone una arquitectura de sistema específica entre dominios administrativos o dentro de un dominio administrativo. A continuación se ofrecen algunas arquitecturas, a título ilustrativo, más no exhaustivo.

Se recuerda que un elemento par es un elemento funcional que puede existir junto con cualquier otro elemento H.323. En la figura G.2 se muestran algunos ejemplos de implementaciones de elementos pares en combinación con otros elementos.

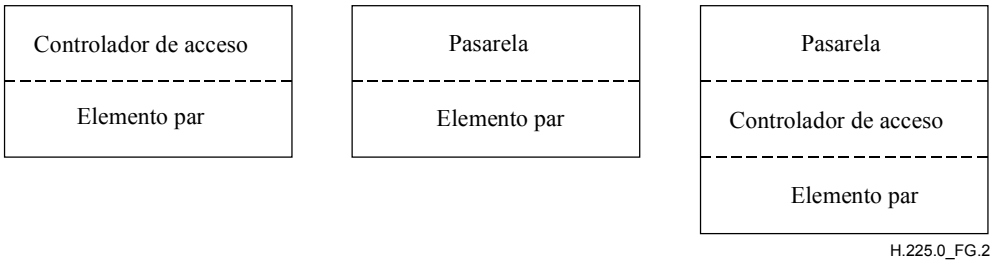


Figura G.2/H.225.0 – Ejemplos de colocación de elementos pares

En general, se considera que un dominio administrativo está formado por cualquier número de zonas y cualquier número de elementos pares. Las relaciones entre dominios administrativos y entre elementos pares dentro de un dominio administrativo, puede ser cualquiera de una variedad de organizaciones. En las siguientes cláusulas se dan ejemplos de las relaciones y organizaciones, que se describen entre dominios administrativos, pero los ejemplos de disposiciones jerárquicas, distribuidas o en malla completa y de agregación se podrían utilizar también para organizar elementos pares dentro de un dominio administrativo.

Obsérvese también que los siguientes ejemplos son ilustrativos, y no excluyen otras organizaciones posibles.

G.5.1 Disposición jerárquica

En la figura G.3 se muestra una disposición jerárquica simple entre dominios administrativos. En este caso, para resolver una dirección, un elemento de frontera de un determinado dominio administrativo consultaría a un elemento de frontera de un dominio administrativo superior en la jerarquía para resolver una dirección.

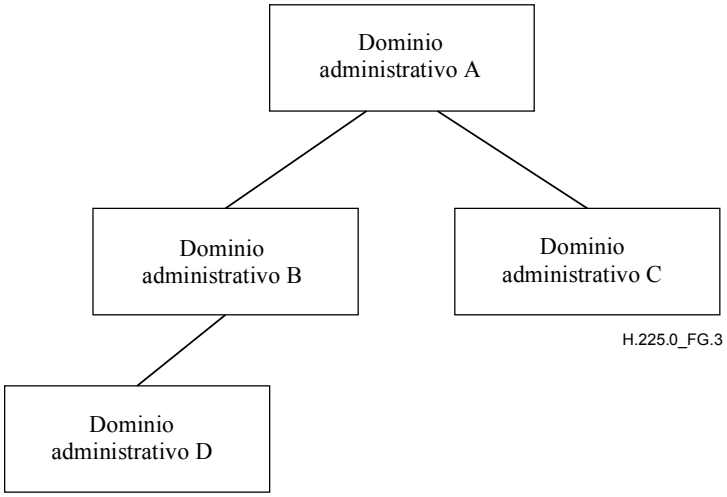


Figura G.3/H.225.0 – Ejemplo de organización jerárquica

G.5.2 Disposición distribuida o en malla completa

En la figura G.4 se ilustra un modelo totalmente distribuido o en malla completa. En este ejemplo, un elemento de frontera de cada dominio administrativo se comunica con los elementos de frontera de los otros dominios administrativos conocidos.

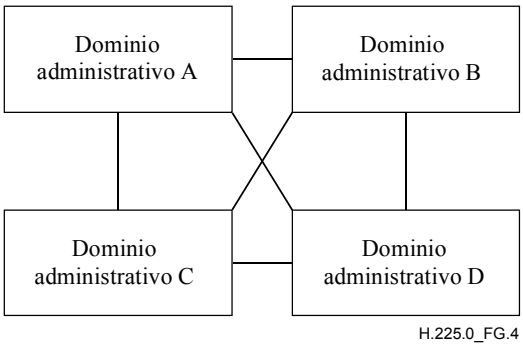


Figura G.4/H.225.0 – Ejemplo de organización distribuida

G.5.3 Centro de resolución

En la figura G.5 se muestra un ejemplo de disposición con centro de resolución. En esta disposición, cada dominio administrativo consulta al centro de resolución para resolver las direcciones. Obsérvese que como el centro de resolución es una entidad que existe fuera del dominio administrativo, los elementos pares que comunican con él son por definición elementos de frontera.

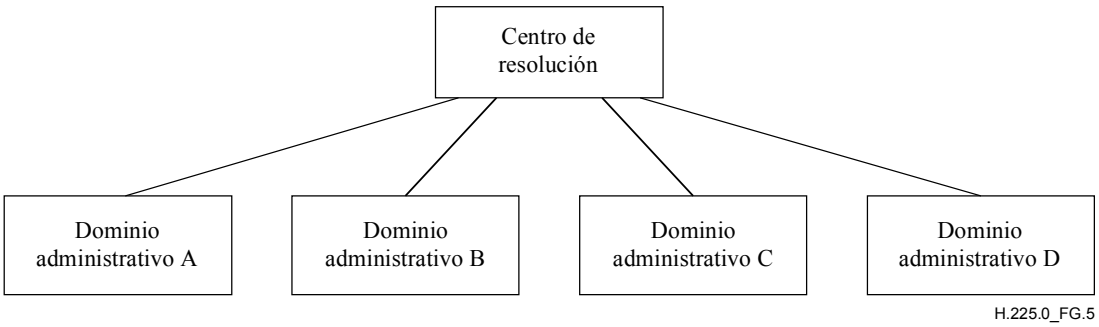


Figura G.5/H.225.0 – Ejemplo de organización con centro de resolución

G.5.4 Punto de agregación

En la figura G.6 se muestra un ejemplo de punto de agregación. En este ejemplo, el dominio administrativo B es un punto de agregación que puede resolver direcciones para sí mismo y para los dominios administrativos C y D. Por ejemplo, el dominio administrativo B puede transmitir peticiones de resolución del dominio administrativo A al dominio administrativo C, o puede indicar al dominio A que se dirija al dominio C directamente para ciertos destinos. Si el dominio administrativo B transmite una petición del dominio administrativo A al dominio administrativo C, el dominio administrativo B puede almacenar la respuesta del dominio administrativo C.

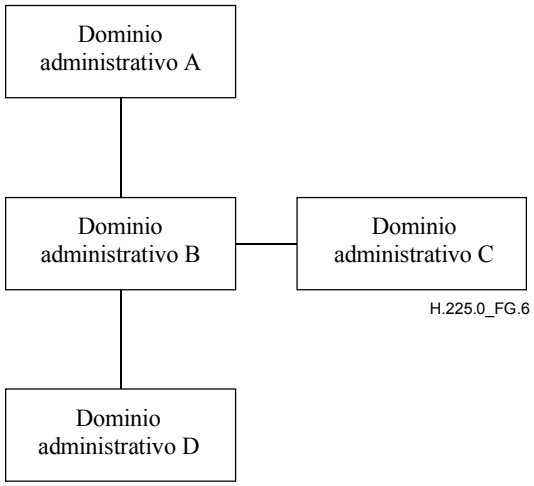


Figura G.6/H.225.0 – Ejemplo de punto de agregación

G.5.5 Dominios administrativos superpuestos

Más de un dominio administrativo puede ser capaz de resolver una determinada dirección. Por ejemplo, varios dominios administrativos podrían contener pasarelas que pueden completar una llamada a un terminal en la red telefónica general conmutada (RTGC). La selección del dominio administrativo de destino apropiado incumbe al dominio administrativo de origen. El algoritmo empleado para seleccionar el dominio administrativo de destino depende de la implementación.

G.6 Funcionamiento

G.6.1 Uso de mensajes H.501

Los sistemas que implementan el anexo G/H.225.0 utilizarán los mensajes definidos en la Rec. UIT-T H.501. Las entidades que intercambian mensajes H.501 se denominan en dicha Recomendación elementos pares.

A continuación se da una lista de los mensajes H.501 utilizados por el anexo G/H.225.0:

Petición de servicio (*ServiceRequest*)

Confirmación de servicio (*ServiceConfirmation*)

Rechazo de servicio (*ServiceRejection*)

Liberación de servicio (*ServiceRelease*)

Petición de descriptor (*DescriptorRequest*)

Confirmación de descriptor (*DescriptorConfirmation*)

Rechazo de descriptor (*DescriptorRejection*)

Petición de ID de descriptor (*DescriptorIDRequest*)

Confirmación de ID de descriptor (*DescriptorIDConfirmation*)

Rechazo de ID de descriptor (*DescriptorIDRejection*)

Actualización de descriptor (*DescriptorUpdate*)

Acuse de actualización de descriptor (*DescriptorUpdateAck*)

Petición de acceso (*AccessRequest*)

Confirmación de acceso (*AccessConfirmation*)

Rechazo de acceso (*AccessRejection*)

Petición en curso (*RequestInProgress*)

Petición no normalizada (*NonStandardRequest*)

Confirmación no normalizada (*NonStandardConfirmation*)

Rechazo no normalizado (*NonStandardRejection*)

Respuesta a mensaje desconocido (*UnknownMessageResponse*)

Petición de utilización (*UsageRequest*)

Confirmación de utilización (*UsageConfirmation*)

Rechazo de utilización (*UsageRejection*)

Indicación de utilización (*UsageIndication*)

Confirmación de indicación de utilización (*UsageIndicationConfirmation*)

Rechazo de indicación de utilización (*UsageIndicationRejection*)

Petición de validación (*ValidationRequest*)

Confirmación de validación (*ValidationConfirmation*)

Rechazo de validación (*ValidationRejection*)

Un elemento par del anexo G/H.225.0 que recibe un mensaje de petición H.501 no incluido en la lista anterior responderá con un mensaje UnknownMessageResponse.

Los mensajes contendrán todos los campos definidos por la Rec. UIT-T H.501 como obligatorios, y pueden contener campos facultativos, según sea necesario.

G.6.2 Plantillas y descriptores de dirección

Un elemento par obtiene plantillas de las maneras siguientes:

- mediante configuración estática;

- recibiendo descriptores de otros elementos pares en respuesta a peticiones generales;
- recibiendo respuestas a peticiones específicas.

G.6.2.1 Configuración estática

Un elemento par mantendrá plantillas para todas las zonas de las que es responsable. Estas plantillas pueden ser proporcionadas explícitamente en el elemento par o, cuando el elemento par coexiste con controladores de acceso, pueden formarse resumiendo la información obtenida de cada controlador de acceso con el cual comunica el elemento par. El elemento par puede poner esta información a disposición de otros elementos pares a través de respuestas a peticiones. Un dominio administrativo puede escoger el nivel de detalle que deben proporcionar sus elementos de frontera. A continuación figuran algunos ejemplos:

- Un elemento de frontera que desee ocultar la estructura interna podría proporcionar un descriptor (con una indicación de enviar un mensaje AccessRequest) que describa toda su zona y refiera a un controlador de acceso que tratará todas las llamadas entrantes.
- Un elemento de frontera que no tenga inconveniente en revelar su estructura interna podría suministrar un conjunto de plantillas, cada una con la descripción del controlador de acceso de una zona dentro del dominio.
- Un elemento de frontera que esté en un una barrera de seguridad (o uno que utilice el modelo de encaminamiento con controlador de acceso) podría suministrar una plantilla para toda la zona con una indicación de enviar un mensaje Setup (Establecimiento).
- Un elemento de frontera con vacíos en su dominio (debido a que se han trasladado números a otro dominio administrativo) suministra plantillas marcadas **enviar AccessRequest** que indican el elemento de frontera que se debe utilizar para dirigirse al otro dominio administrativo.
- Un elemento de frontera centro de resolución (por ejemplo, uno que tenga una copia completa de 44) podría tener una plantilla marcada **enviar AccessRequest** para cada dominio administrativo dentro de 44.

Los elementos pares no necesitan mantener una copia de toda la base de datos. Si un elemento par no tiene una copia de toda la base de datos, debe contener plantillas **enviar AccessRequest**, configuradas estáticamente, que indiquen un elemento de frontera centro de resolución que se utilizará para resolver otras consultas.

G.6.2.2 Recepción de descriptores

Un elemento par puede solicitar las plantillas configuradas estáticamente de otro elemento par. La respuesta a la petición es decidida por el elemento par al que se solicitan dichas plantillas. Para solicitar una transferencia, el elemento par envía un mensaje DescriptorRequest que especifica los descriptores que desea recibir. Si el elemento par propietario puede transferirlos, responde con un mensaje DescriptorConfirmation, en el que se especifican todas las plantillas.

El elemento par solicitante puede almacenar una copia de una plantilla recibida de esta manera hasta el final de la vida útil de dicha plantilla; en ese momento el elemento par debe eliminar dicha copia. Si el elemento par propietario cambia sus plantillas configuradas estáticamente antes de que haya finalizado su vida útil, enviará un mensaje DescriptorUpdate a los elementos pares de los que tiene conocimiento. Al recibir un mensaje DescriptorUpdate, un elemento par debe suprimir, añadir o modificar todas las plantillas indicadas que tiene almacenadas, o debe solicitar al propietario copias de los descriptores indicados.

Un elemento par intermedio (es decir un elemento par que está entre los dominios administrativos de origen y de destino, tal como un centro de resolución o un punto de agregación) puede publicar sus propios descriptores basándose en los descriptores que recibe. Por ejemplo, un centro de resolución puede indicarse a sí mismo como contacto para un mensaje AccessRequest aunque los

descriptores que haya recibido de otro elemento de frontera indiquen a ese otro elemento de frontera como contacto.

Un elemento par puede indicar en una plantilla el requisito para que un originador reciba la autorización de efectuar una llamada en un dominio administrativo. Cuando se coloca la bandera **callSpecific (específica de llamada)** en una plantilla y el tipo de mensaje indica que se enviará un mensaje AccessRequest, el originador proporcionará información por cada llamada en el mensaje AccessRequest. Si un elemento par recibe el mensaje AccessRequest sin información por cada llamada y la política es solicitar información por llamada, el elemento par responderá con un mensaje AccessRejection, con el motivo **needCallInformation (información de llamada necesaria)**.

Un elemento par puede enviar un mensaje DescriptorUpdate a otros elementos pares conocidos, o puede multidistribuir un mensaje DescriptorUpdate. En este último caso, el elemento par debe considerar el ámbito de la multidifusión. El mensaje DescriptorUpdate puede contener los descriptores que han cambiado. Alternativamente, el mensaje DescriptorUpdate puede indicar únicamente la identificación de los descriptores que cambiaron, permitiendo al destinatario solicitar la nueva información. Si han cambiado muchos descriptores, la información debe ser enviada en varios mensajes DescriptorUpdate, de modo que un determinado mensaje DescriptorUpdate no exceda del tamaño máximo de paquete de transporte.

G.6.2.3 Recepción de respuestas a consultas específicas

Un elemento par puede enviar un mensaje AccessRequest a otro elemento par pidiéndole la resolución de una dirección total o parcialmente calificada. El mensaje AccessRequest se envía generalmente por un medio de transporte no fiable (por ejemplo, UDP), aunque se puede enviar por un medio de transporte fiable (por ejemplo, TCP).

Al recibir un mensaje AccessRequest, un elemento par efectúa una búsqueda en su base de datos y responde con la plantilla más específica para el destino. Si varias plantillas satisfacen la petición, el elemento par devolverá todas las plantillas pertinentes. Si el elemento par de destino es responsable de la dirección de alias especificada, el elemento par responderá generalmente con una plantilla que indica que se debe enviar un mensaje AccessRequest o Setup. Si el elemento par de destino es un centro de resolución, responderá generalmente con una plantilla que indica que se debe enviar el mensaje AccessRequest.

El elemento par de destino puede también añadir a la respuesta las plantillas que considera serán útiles en el futuro. La adición de estas plantillas no debe alargar la respuesta de manera que la red de transporte tenga que fragmentarla (es decir, 576 octetos para IPv4 ó 1200 octetos para IPv6).

Por ejemplo, un elemento par estrechamente acoplado con una barrera de seguridad puede suministrar dos plantillas en su respuesta a los mensajes AccessRequest: una plantilla de corta duración (algunos minutos o segundos) que especifica a dónde se debe enviar un mensaje Setup y plantillas adicionales que especifican que los mensajes deben ser enviados al elemento de frontera para otras direcciones de alias en el dominio administrativo.

Un elemento par puede conservar una plantilla recibida en un mensaje AccessConfirmation hasta que expire.

G.6.3 Localización de un elemento par o de un conjunto de elementos pares

G.6.3.1 Estática

Un elemento par puede tener un conjunto administrado de otros elementos pares a los que puede dirigirse para la resolución de direcciones. Este conjunto administrado se puede definir mediante un conjunto de acuerdos bilaterales, por ejemplo, entre un dominio administrativo y otros dominios administrativos. Los dominios administrativos pueden utilizar opcionalmente el servicio de un centro de resolución.

G.6.3.2 Dinámica

En las redes IP, la propiedad de direcciones de tipo email-id (id de correo electrónico) es definida por el sistema DNS. Así, en ausencia de mejor información, un elemento de frontera puede examinar los registros SRV del DNS en la parte del id de correo electrónico situada a la derecha del signo "@" (por ejemplo, una búsqueda en los registros SRV del DNS en **_h2250-annex-g._udp.example.org** para **person@example.org**). La respuesta de esta búsqueda debe emplearse para sintetizar una plantilla **enviar AccessRequest** que pueda ser utilizada durante el proceso de resolución. Las plantillas sintetizadas a partir de peticiones DNS no deben conservarse más allá de la vida útil indicada en la respuesta del DNS.

G.6.3.3 Otros métodos

Queda en estudio la utilización de otros métodos para localizar otro elemento par.

G.6.4 Procedimientos de resolución

G.6.4.1 Procedimiento de resolución en un dominio administrativo

Cuando se pide a un elemento par que resuelva una dirección de alias (por ejemplo, mediante una pasarela o un controlador de acceso coubicados), encuentra las plantillas pertinentes en su lugar de almacenamiento.

Si hay más de una plantilla pertinente, se seleccionan y ordenan las plantillas apropiadas de acuerdo con la política local. Por ejemplo, las plantillas pueden ser ordenadas primero según la longitud del comodín (es mejor suministrar plantillas más específicas), luego según el tipo de protocolo especificado (**enviar Setup** es mejor que **enviar AccessRequest**).

Si varias plantillas satisfacen la petición, el elemento par indicará todas las plantillas que concuerdan.

Si el proceso de selección de plantilla no arroja ninguna plantilla marcada **enviar Setup**, el elemento par envía un mensaje AccessRequest con una dirección de destino específica a la dirección indicada en la plantilla. Cuando obtiene una respuesta del elemento par, puede almacenarla e indicar al solicitante la dirección a la que debe enviar el mensaje Setup.

G.6.4.2 Procedimiento de resolución entre dominios administrativos

Cuando un elemento de frontera recibe un mensaje AccessRequest de un elemento de frontera en otro dominio administrativo, busca en las plantillas que tiene almacenadas y encuentra la que concuerda con la dirección que figura en la consulta.

Si más de una plantilla concuerda, las plantillas concordantes se ordenan primero según la longitud del comodín (es mejor utilizar plantillas más específicas). Se ordenan después de acuerdo con el tipo de mensaje especificado (**enviar Setup** es mejor que **enviar AccessRequest**). En cada caso, se descartan todas las plantillas distintas de las que corresponden a la búsqueda más específica.

Si las plantillas que concuerdan están marcadas **enviar AccessRequest**, el elemento de frontera puede elegir reenviar el mensaje AccessRequest al(a los) elemento(s) de frontera especificado(s) en la(s) plantilla(s), o puede devolver las plantillas tal como están. Si el contador de saltos que figura en el mensaje AccessRequest recibido ha llegado a cero, el elemento de frontera no puede reenviar el mensaje AccessRequest a otro elemento de frontera; pero en cambio debe devolver las plantillas que concuerdan. Si el contador ha llegado a cero y el elemento de frontera no tiene ninguna información para proporcionar en un mensaje AccessConfirmation, el elemento de frontera debe responder con un mensaje AccessRejection que indique que se ha rebasado el cómputo de saltos.

En este punto, el elemento de frontera puede usar otro elemento de frontera (por ejemplo, un centro de resolución) para autorizar la petición de acceso. Para ello, envía un mensaje ValidationRequest, que lleva los testigos de acceso suministrados por el elemento de frontera solicitante en

AccessRequest. El elemento de frontera destinatario valida los testigos y devuelve ValidationConfirmation.

El elemento de frontera devuelve entonces un mensaje AccessConfirmation con las plantillas que ha hallado (éstas tendrán los mismos campos de dirección y tipo de mensaje), así como cualesquiera otras plantillas que considere útiles.

Si varias plantillas satisfacen la petición, el elemento de frontera devolverá todas las plantillas que corresponden.

Si la petición de acceso contiene información de llamada específica, las plantillas devueltas sólo son válidas para la llamada solicitada. Esto se utiliza cuando un dominio administrativo desea conceder acceso llamada por llamada. En ese caso, el dominio administrativo puede imponer la inclusión de información de llamada por cada petición de acceso que le es enviada, colocando una bandera en las plantillas que hacen referencia a él.

G.6.5 Intercambio de información sobre utilización

Los elementos pares pueden solicitar a otros elementos pares que les proporcionen información sobre la utilización de recursos en determinadas llamadas. Los mensajes UsageIndication se pueden proporcionar en cualquier etapa de la llamada. Asimismo, es posible enviar múltiples mensajes UsageIndication para la misma llamada, cada uno posiblemente con información más actualizada, o informando sobre segmentos de llamada consecutivos o el uso de diferentes tipos de medios. Para más detalles, véase G.6.5.1.

Los mensajes UsageIndication pueden ser intercambiados con independencia de si los dos elementos pares tienen una relación de servicio entre ellos. Sin embargo, la política de un elemento par puede no permitir estos intercambios sin una relación de servicio. En este caso, el elemento par puede rechazar el mensaje UsageIndication con un código de rechazo de **`noServiceRelationship`** **(`ninguna relación de servicio`)**.

Se enviarán peticiones de UsageIndication cuando un elemento par las requiera, ya sea en las plantillas para las que sirve de contacto o bien indicándolo en el mensaje ServiceRequest que envía durante el establecimiento de la relación de servicio con un elemento par distante, o indicándolo en cualquiera de los mensajes UsageRequest, AccessRequest, ValidationRequest y ValidationConfirmation enviados en el contexto de la llamada para la cual se requiere información de utilización.

G.6.5.1 Múltiples indicaciones de utilización en la misma llamada

Las múltiples indicaciones de utilización para la misma llamada proporcionan información cada vez más actualizada sobre los mismos tipos de medios, o información de utilización sobre nuevos tipos de medios creados en la misma llamada. Asimismo, como los elementos pares pueden tomar llamadas mientras están en la etapa de progresión, no todas las indicaciones de utilización necesariamente provienen del mismo elemento par. Las siguientes reglas definen la semántica:

1) Un mensaje UsageIndication recibido con **`usageCallStatus`** de **`callInProgress`** implica que se debe recibir una UsageIndication subsiguiente con los mismos **`callIdentifier`** y **`senderRole`**. Si el recibiente está configurado para recuperación tras avería, puede elegir llegar a la conclusión, después de un intervalo de tiempo configurado sin otros mensajes UsageIndication, de que se ha producido una avería y puede recuperar cualesquiera datos de los mensajes UsageIndication recibidos.

2) Los siguientes mensajes UsageIndication con los mismos identificadores **`usageField`** deben informar un **`startTime`** que concuerde con el **`endTime`** del mensaje anterior (aunque esto puede ser imposible para un elemento par alterno). Los recibientes supondrán que cada informe es para un periodo distinto. Otra información en **`usageField`** abroga la información recibida en mensajes anteriores con el mismo identificador **`usageField`**.

3) Un elemento par debe enviar un nuevo mensaje UsageIndication para cada cambio del tipo de medios durante la llamada, por ejemplo, audio detenido y fax arrancado, o cambio de un códec. Si se utilizan múltiples tipos de medios al mismo tiempo (por ejemplo, audio y vídeo), esto debe ser informado en el mismo mensaje UsageIndication.

G.6.5.2 Petición y negociación de información de utilización durante el establecimiento de relaciones de servicio

Un elemento par, PE_A, puede incluir un elemento **`UsageSpecification`** en un mensaje ServiceRequest para un segundo elemento par, PE_B. Este elemento **`UsageSpecification`** se utilizará para definir la información de utilización por defecto que se ha de notificar para todas las llamadas que se efectúan mientras existe la relación de servicio entre los dos elementos pares, PE_A y PE_B. Esta **`UsageSpecification`** se utilizará para todas las llamadas para las cuales PE_B envía UsageIndications a PE_A.

Si un elemento **`UsageSpecification`** llega a PE_B en otro mensaje de PE_A (por ejemplo, AccessConfirmation), entonces el nuevo **`UsageSpecification`** abroga el **`UsageSpecification`** por defecto para todas las llamadas relacionadas con el nuevo mensaje.

Un elemento par que recibe un mensaje ServiceRequest que contiene un elemento **`UsageSpecification`** debe actuar como sigue:

i) Si el elemento par receptor desea aceptar el mensaje ServiceRequest y el elemento **`UsageSpecification`** contenido dentro, enviará un mensaje ServiceConfirmation con el mismo **`UsageSpecification`** que el recibido en el mensaje ServiceRequest. **`UsageSpecification`** se aplicará a ambas llamadas entrantes al elemento par recibiente del elemento par solicitante y a las llamadas salientes del elemento par recibiente al elemento par solicitante.

ii) Si el elemento par receptor desea aceptar el mensaje ServiceRequest pero no desea aceptar el elemento **`UsageSpecification`** contenido en éste, enviará un mensaje ServiceConfirmation con un **`UsageSpecification`** diferente que especifique la información de utilización que puede proporcionar al elemento par solicitante, o un mensaje ServiceRejection con el motivo puesto a **`cannotSupportUsageSpec`** (imposible aceptar especificación de utilización).

iii) Si el elemento par receptor no soporta informe de utilización, devolverá un mensaje ServiceRejection con el motivo puesto a **`usageUnavailable`**.

Un elemento par que recibe un mensaje ServiceConfirmation debe actuar como sigue:

i) Si el elemento **`UsageSpecification`** en el mensaje ServiceConfirmation es igual al enviado en ServiceRequest, el elemento par de origen y el elemento par de terminación han establecido una relación de servicio entre ellos.

ii) Si el elemento **`UsageSpecification`** en el mensaje ServiceConfirmation es diferente al enviado en el mensaje ServiceRequest, y si el elemento par de origen desea utilizar el nuevo **`UsageSpecification`**, se establece la relación de servicio. Si el elemento par de origen no desea utilizar el nuevo **`UsageSpecification`**, enviará un mensaje ServiceRelease con el motivo puesto a **`terminated`**. El elemento par de origen podrá entonces analizar el elemento **`UsageSpecification`** devuelto en ServiceConfirmation, para construir un nuevo mensaje ServiceRequest con un elemento **`UsageSpecification`** modificado que pueda ser aceptable para ambos elementos pares.

iii) Si ServiceConfirmation no contiene un elemento **`UsageSpecification`** (y el mensaje ServiceRequest sí lo contiene), el elemento par que envió ServiceConfirmation no puede emplear o no empleará informe de utilización en el nivel de la relación de servicio. Éste es el caso, por ejemplo, cuando el elemento par receptor aplica la versión 1 de este anexo. En este caso, el elemento par de origen puede terminar la relación de servicio (enviando un

mensaje un mensaje ServiceRelease con el código de motivo puesto a **`terminated`**), o no terminar la relación de servicio. En cualquiera de los dos casos, si el elemento par de origen está interesado en recibir información de utilización sobre llamadas, debe solicitarla empleando los mecanismos descritos en la versión 1 de este anexo [es decir, enviando elementos **`UsageSpecification`** en mensajes AccessRequest, AccessConfirmation (con las plantillas de direcciones devueltas), UsageRequest, ValidationRequest o ValidationConfirmation messages].

G.6.6 Señalización de información de portabilidad de números

La Rec. UIT-T H.460.2 describe mecanismos para la portabilidad de números en redes H.323. El soporte de los mecanismos H.460.2 requiere que el procedimiento del anexo G sea capaz de transportar información de portabilidad de números a través de intercambios de mensajes de resolución de dirección. La interfaz entre el elemento de frontera del anexo G y los otros elementos de red H.323 con los cuales comunica no se trata en este anexo; se supone que esta interfaz es capaz de transportar la portabilidad de números H.460.2 a y desde el elemento de frontera del anexo G.

Cuando se envía un mensaje AccessRequest, éste transportará la información de portabilidad de números H.460.2, si existe, utilizando el campo **`genericData`** en la porción de información común del mensaje.

Los mensajes AccessConfirmation y AccessRejection transportarán también la correspondiente información de respuesta de portabilidad de número en el campo **`genericData`**. En el caso de un mensaje AccessRejection, el motivo del rechazo será **`genericDataReason`**.

G.7 Ejemplos de señalización

Estos ejemplos de señalización tienen por objeto ilustrar el funcionamiento básico. En estos ejemplos se supone que los dominios administrativos tienen acuerdos entre sí, de modo que los elementos de frontera disponen de información mutua (por ejemplo, puertos TCP). En muchos de los siguientes ejemplos, los mensajes RAS LRQ/LCF son intercambiados entre un controlador de acceso y un elemento de frontera dentro del mismo dominio administrativo Esto tiene fines puramente ilustrativos y se podrán intercambiar mensajes del anexo G análogos entre el elemento de frontera y un elemento par que reside dentro del controlador de acceso.

G.7.1 Red distribuida o malla completa

En la figura G.7 se muestra un ejemplo de red distribuida.

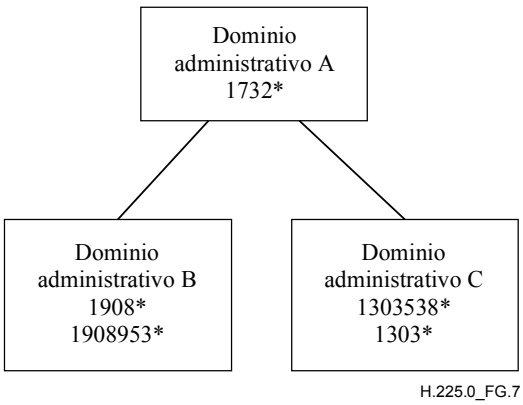


Figura G.7/H.225.0 – Ejemplos de red distribuida para señalización

Para este ejemplo, se supone que cada dominio administrativo tiene un elemento de frontera, y que los elementos de frontera están configurados para resolver direcciones como sigue:

Dominio administrativo	Definición de plantilla	Comentarios
A	Descriptor "d1": Patrón = 1732* Dirección de transporte = Dirección de señal de llamada de BE_A Tipo de mensaje = **sendSetup**	La señalización para cualquier llamada al dominio administrativo A se hará a través del elemento de frontera de dicho dominio administrativo.
B	Descriptor "d2": Patrón = 1908* Dirección de transporte = Dirección de anexo G de BE_B Tipo de mensaje = **sendAccessRequest** Descriptor "d3": Patrón = 1908953* Dirección de transporte = Dirección de señal de llamada de GW_{B1} Tipo de mensaje = **sendSetup**	Para las llamadas a 1908*, se requiere un mensaje AccessRequest para obtener la dirección de señalización de llamada de destino (es decir, una pasarela). Para las llamadas a 1908953*, el mensaje Setup se puede enviar directamente a esta pasarela.
C	Descriptor "d4": Patrón = 1303538* Dirección de transporte = Dirección de señal de llamada de GK_{C1} Tipo de mensaje = **sendSetup** Descriptor "d5": Patrón = 1303* Dirección de transporte = Dirección de anexo G BE_C Tipo de mensaje = **sendAccessRequest**	Las llamadas a 1303538* se encaminarán a través de este controlador de acceso. Las llamadas a 1303* pueden señalizarse directamente a la pasarela de destino, pero se debe enviar un mensaje AccessRequest para obtener la dirección de señalización de llamada de la pasarela.

G.7.1.1 Intercambio de información de zona

En la organización distribuida, o malla completa, cada dominio administrativo conoce los demás dominios administrativos, probablemente a través de varios acuerdos contractuales bilaterales. En todo momento, un elemento de frontera de un dominio administrativo puede consultar a otro dominio administrativo para obtener información de direccionamiento. En la figura G.8 se ilustra un ejemplo de esta señalización.

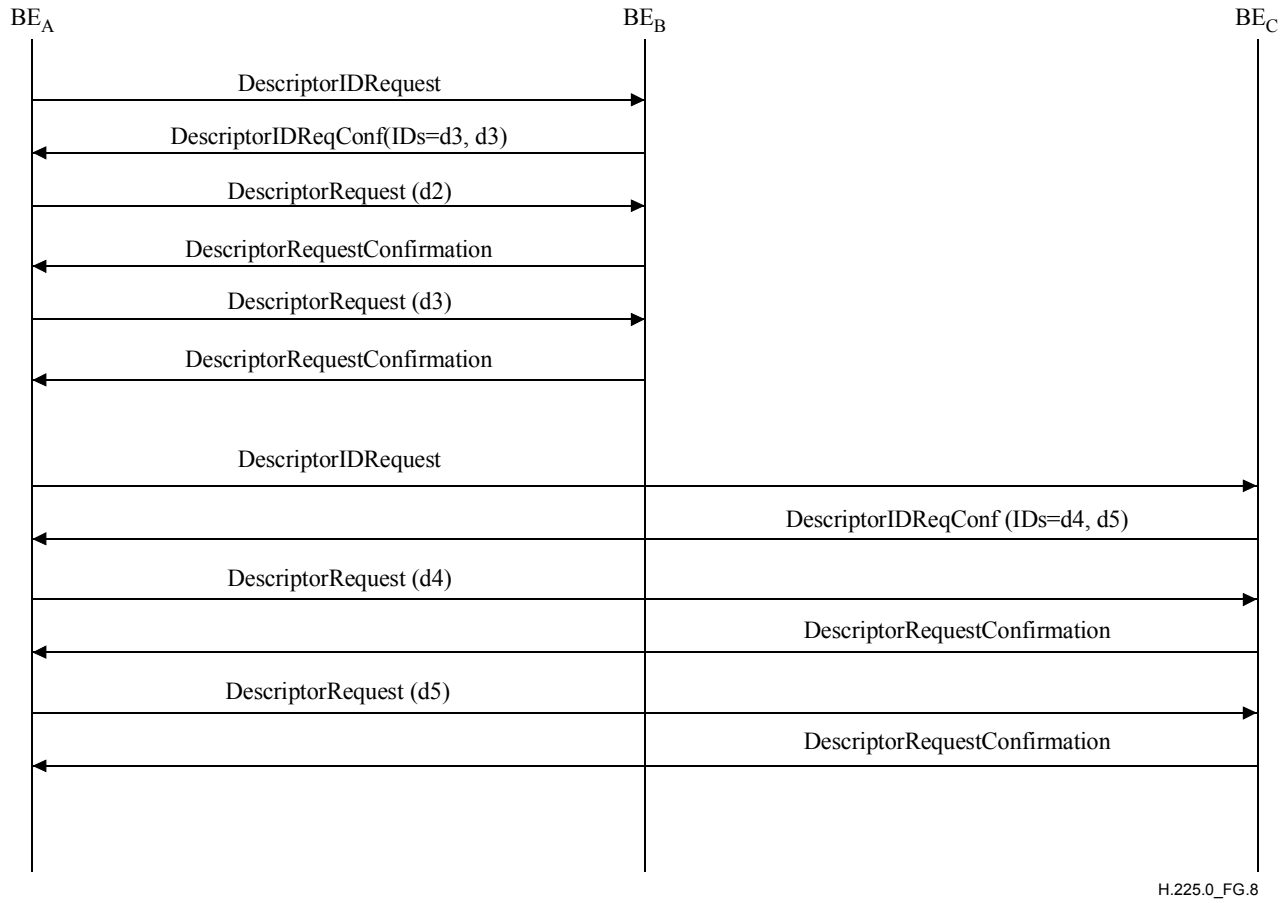


Figura G.8/H.225.0 – Ejemplo de intercambios de descriptores

De modo similar, BE_B consulta a BE_A y a BE_C, y BE_C consulta a BE_A y a BE_B.

G.7.1.2 Realización de una llamada

Se supone que T1, en el dominio administrativo A, inicia una llamada a 19085551515 (T2). Al recibir la ARQ de T1, el controlador de acceso de T1 envía una LRQ. Un elemento de frontera del dominio administrativo A, BE_A, ha recibido previamente los descriptores de zona y sabe cómo cursar la petición. Como se muestra en la figura G.9, BE_A envía un mensaje AccessRequest a BE_B, tal como se especifica en el descriptor BE_A recibido de BE_B. BE_B responde con la dirección de señalización de llamada de T2 (en este ejemplo, T2 podría ser cualquier tipo de punto extremo). Enseguida, T1 envía el mensaje Setup H.225.0 a la dirección de señalización de llamada de T2 de conformidad con los procedimientos normales definidos en la Rec. UIT-T H.323 y en sus anexos.

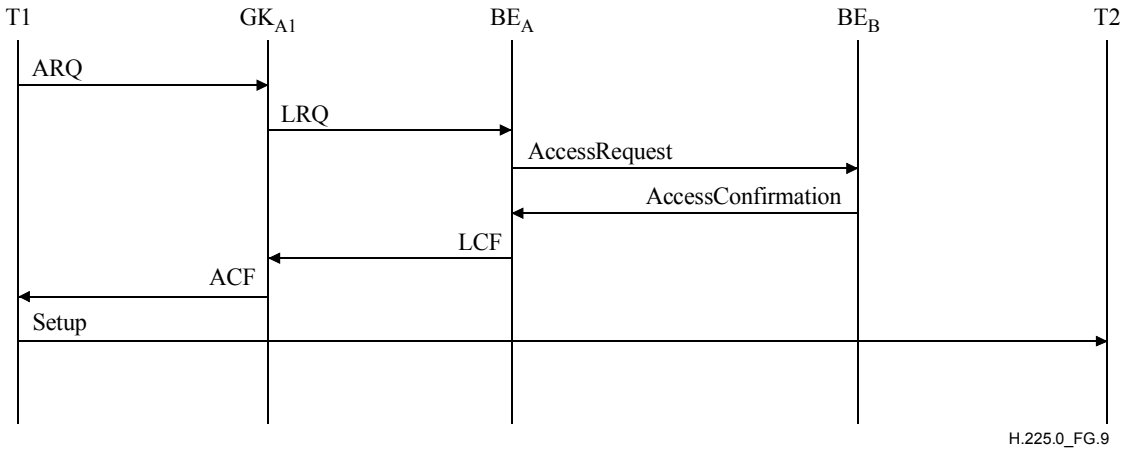


Figura G.9/H.225.0 – Ejemplo de llamada simple

Se supone ahora que T1 inicia una llamada a 19089532000. En este ejemplo, BE_A ha obtenido previamente la dirección de señalización de llamada de una pasarela del dominio administrativo que aceptará la llamada. Como se muestra en la figura G.10, BE_A puede responder a LRQ sin ningún intercambio de mensajes hacia el dominio administrativo B, lo que permite a T1 enviar el mensaje Setup directamente a la pasarela.

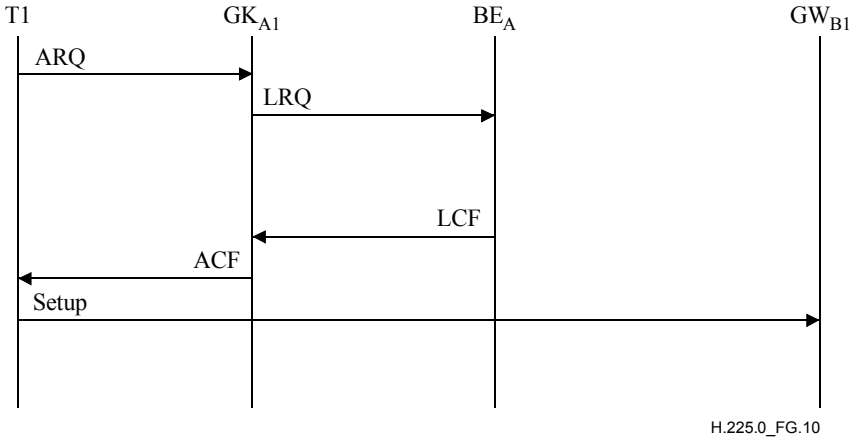


Figura G.10/H.225.0 – Ejemplo de llamada con dirección caché

En otro ejemplo, se supone que T1 inicia una llamada a 13035382899. El dominio administrativo C ha advertido que puede aceptar una llamada a este número, y aceptará la señalización de llamada a través de su controlador de acceso implementando el modelo de encaminamiento por controlador de acceso. Como se muestra en la figura G.11, BE_A puede responder a LRQ con LCF que contiene la dirección de señalización de llamada de un controlador de acceso del dominio administrativo C sin ningún intercambio de mensajes hacia el dominio administrativo C.

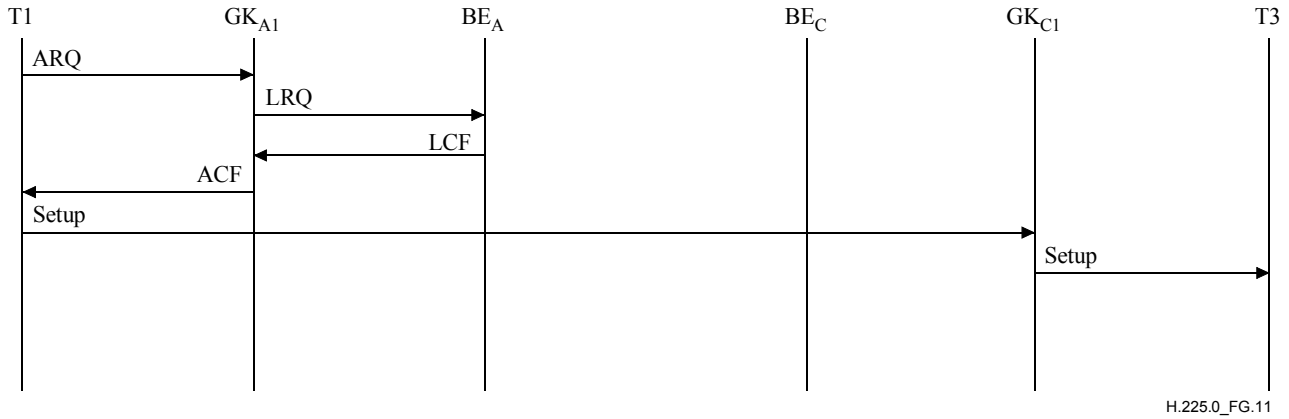


Figura G.11/H.225.0 – Ejemplo de llamada encaminada por un controlador de acceso distante

Como otra posibilidad, el controlador de acceso de T1 puede implementar el modelo de encaminamiento por controlador de acceso, tal como se muestra en la figura G.12.

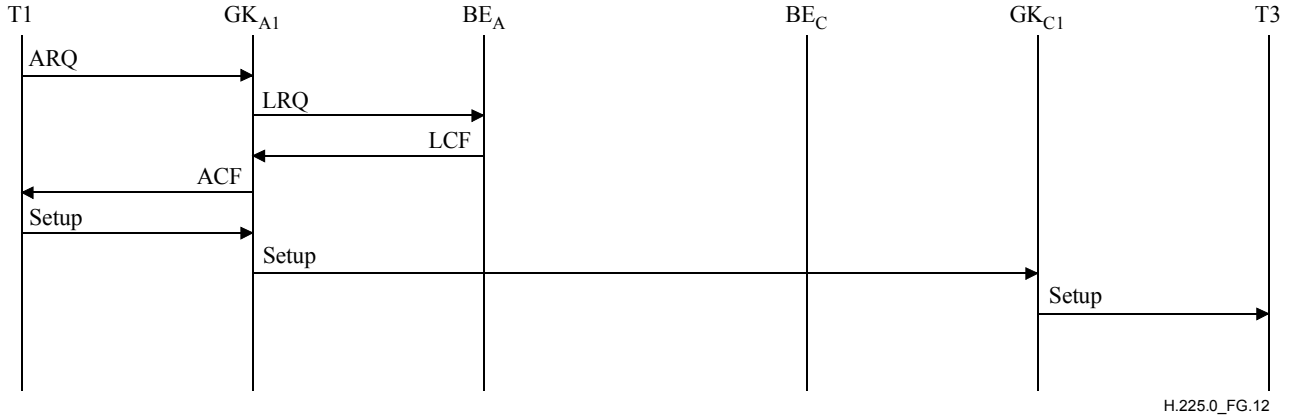


Figura G.12/H.225.0 – Ejemplo de llamada encaminada por un controlador de acceso local

G.7.2 Centro de resolución

En la figura G.13 se ilustra un ejemplo de configuración que utiliza un centro de resolución. Se hace referencia a esta figura para los ejemplos siguientes. En este ejemplo, el centro de resolución mantiene la información de direccionamiento de todos los dominios administrativos a los cuales presta servicio.

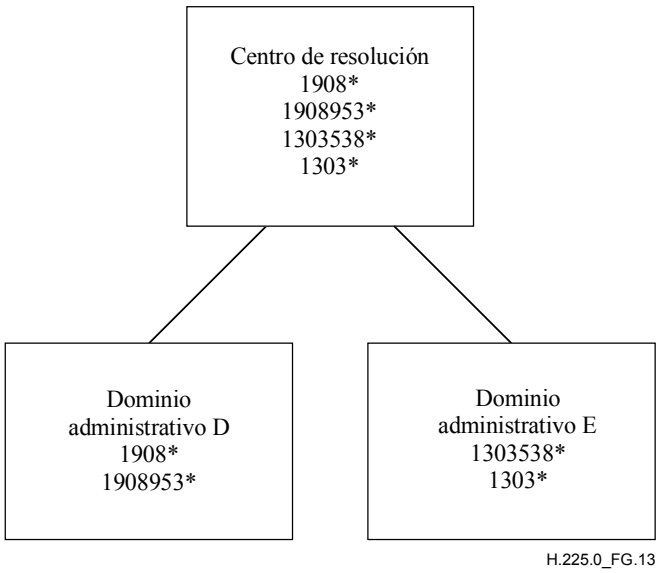


Figura G.13/H.225.0 – Ejemplo de configuración con centro de resolución

En este ejemplo, los elementos de frontera de los dominios administrativos D y E, así como el centro de resolución, contienen la información siguiente:

Dominio administrativo	**Definición de la plantilla**	**Comentarios**
D	Descriptor "d1": Patrón = 1908* Dirección de transporte = Dirección de anexo G de BE_D Tipo de mensaje = **enviar AccessRequest** Descriptor "d2": Patrón = 1908953* Dirección de transporte = Dirección de señalización de llamada de GW_{D1} Tipo de mensaje = **enviar Setup**	Para las llamadas a 1908* se necesita un mensaje AccessRequest para obtener la dirección de señalización de llamada de destino (es decir, una pasarela). Para las llamadas a 1908953*, el mensaje Setup se puede enviar directamente a esta pasarela.
E	Descriptor "d3": Patrón = 1303538* Dirección de transporte = Dirección de señalización de llamada de GK_{E1} Tipo de mensaje = **enviar Setup** Descriptor "d4": Patrón = 1303* Dirección de transporte = Dirección de anexo G de BE_E Tipo de mensaje = **enviar AccessRequest**	Las llamadas a 1303538* se encaminarán a través de este controlador de acceso. Las llamadas a 1303* pueden ser señalizadas directamente a la pasarela de destino, pero se debe enviar un mensaje AccessRequest para obtener la dirección de señalización de llamada de la pasarela.

Dominio administrativo	Definición de la plantilla	Comentarios
CH (centro de resolución)	Descriptor "d1": Patrón = 1908* Dirección de transporte = Dirección anexo G de BE_D Tipo de mensaje = **enviar AccessRequest** Descriptor "d2": Patrón = 1908953* Dirección de transporte = Dirección de señalización de llamada de GW_{D1} Tipo de mensaje = **enviar Setup** Descriptor "d3": Patrón = 1303538* Dirección de transporte = Dirección de señalización de llamada de GK_{E1} Tipo de mensaje = **enviar Setup** Descriptor "d4": Patrón = 1303* Dirección de transporte = Dirección anexo G de BE_E Tipo de mensaje = **enviar AccessRequest**	El centro de resolución obtiene descriptores de otros dominios administrativos y mantiene esta información para distribuirla durante el intercambio de descriptores.

G.7.2.1 Intercambio de información de zona

En este ejemplo, un centro de resolución intercambia información con dominios administrativos adscritos al servicio del centro de resolución. El centro de resolución conserva la información que recibe de cada dominio administrativo y la transmite a los otros dominios administrativos. En este ejemplo, el centro de resolución aparece como dominio administrativo E al dominio administrativo D, mientras que los dominios administrativos D y E no tienen necesariamente conocimiento mutuo. Véase la figura G.14.

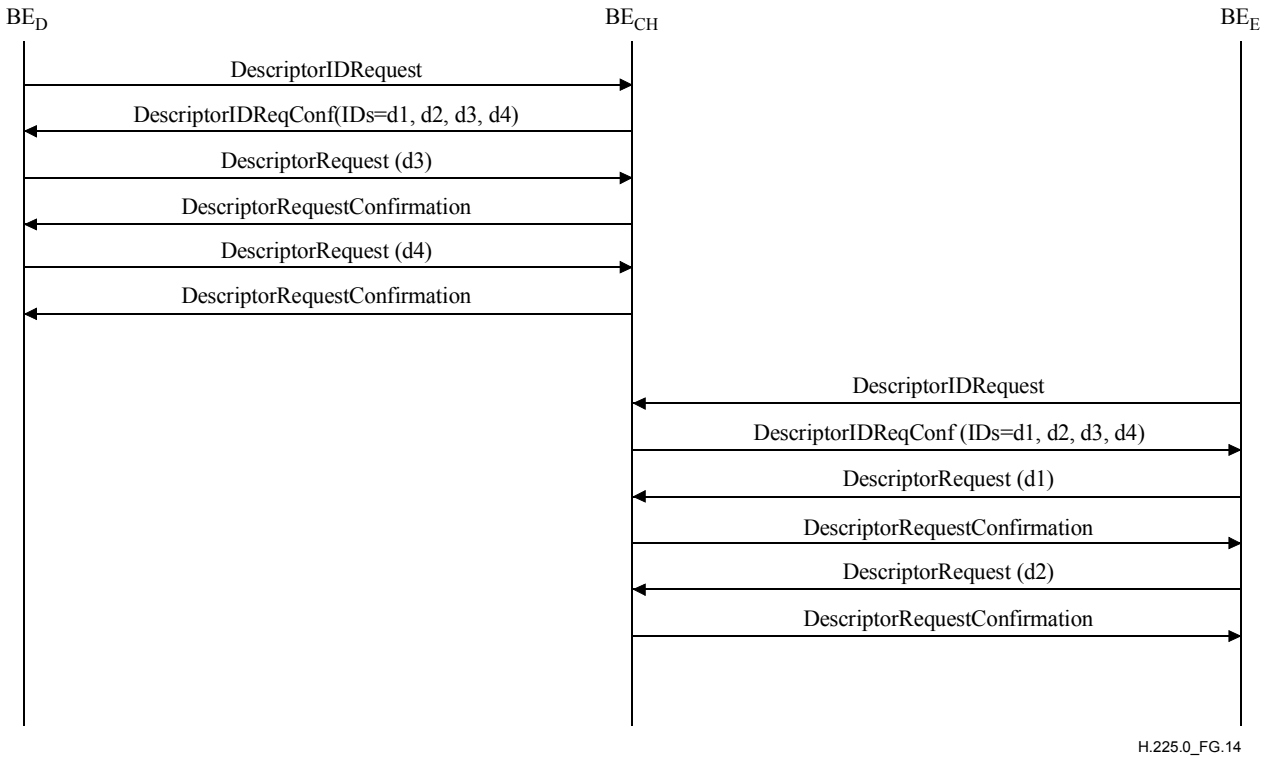


Figura G.14/H.225.0 – Ejemplo de intercambio de descriptores con centro de resolución

G.7.2.2 Realización de una llamada

Se supone que T1, en el dominio administrativo E, inicia una llamada a 19085551515. El elemento de frontera del dominio administrativo E ha recibido del centro de resolución los descriptores que indican que debe consultarse al centro de resolución para dicha llamada. El elemento de frontera envía un mensaje AccessRequest al elemento de frontera centro de resolución. Basándose en los descriptores que el elemento de frontera centro de resolución ha recibido del elemento de frontera del dominio administrativo D, el elemento de frontera centro de resolución envía un mensaje AccessRequest al elemento de frontera del dominio administrativo D. Cuando el elemento de frontera centro de resolución devuelve la confirmación al elemento de frontera del dominio administrativo E, la confirmación contiene la información enviada desde el elemento de frontera del dominio administrativo D. El controlador de acceso de T1 devuelve ACF con la destCallSignalAddress (dirección de señalización de llamada de destino) de T2, lo que permite a T1 enviar el mensaje Setup a T2. Véase la figura G.15.

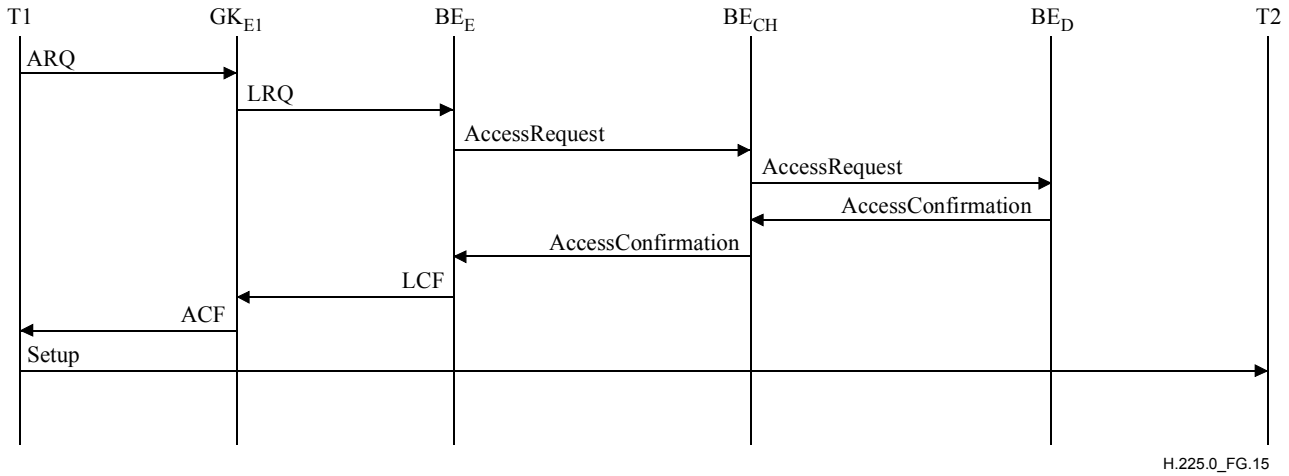


Figura G.15/H.225.0 – Ejemplo de llamada con centro de resolución

Alternativamente, el controlador de acceso de T1 podría encaminar la señalización de llamada como se muestra en la figura G.16.

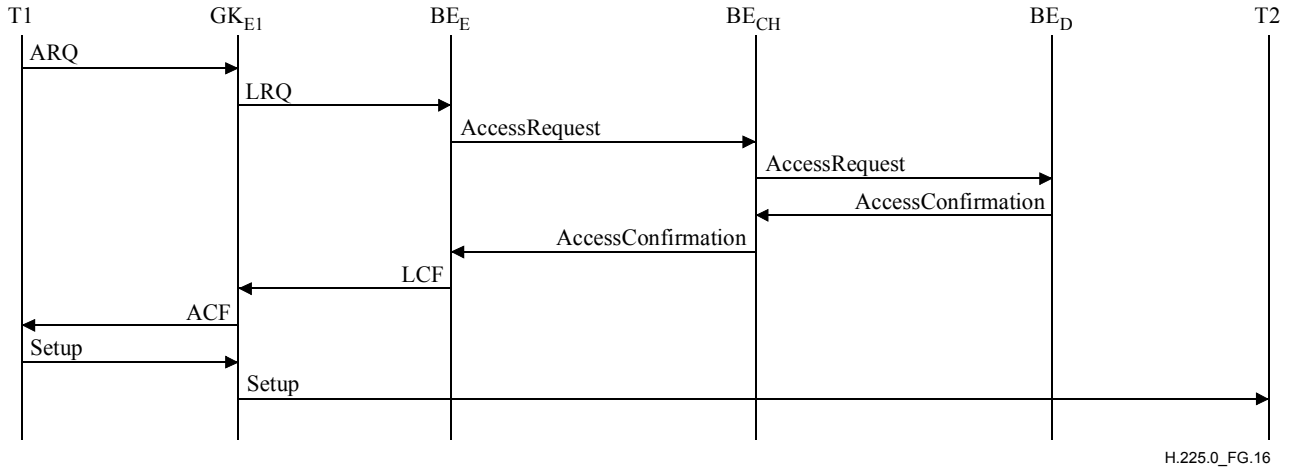


Figura G.16/H.225.0 – Ejemplo de llamada con centro de resolución encaminada por un controlador de acceso local

Otra posibilidad es que el centro de resolución responda al elemento de frontera del dominio administrativo E con la información de contacto del elemento de frontera del dominio administrativo D, como se muestra en la figura G.17.

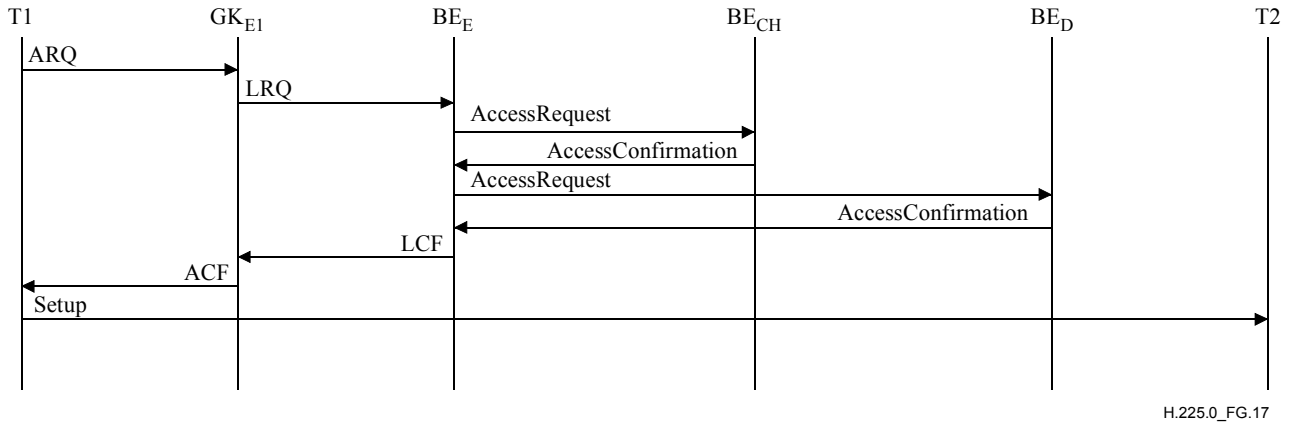


Figura G.17/H.225.0 – Ejemplo de encaminamiento con centro de resolución que utiliza información de contacto para responder al elemento de frontera distante

Se supone ahora que T1 inicia una llamada a 19089532000. Gracias a los descriptores intercambiados previamente, el elemento de frontera puede devolver la dirección de señalización de llamada a T1 sin consultar al centro de resolución, tal como se indica en la figura G.18.

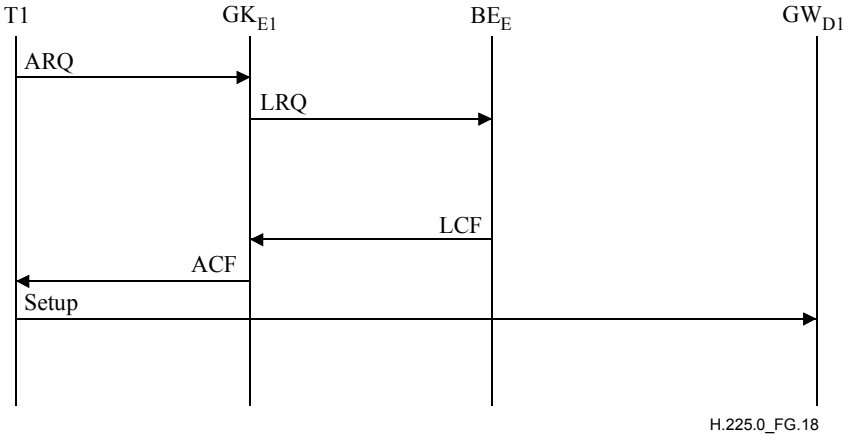


Figura G.18/H.225.0 – Ejemplo de llamada en que un elemento de frontera local utiliza un descriptor caché

A continuación, se considera una situación en la que T1 inicia una llamada a 13035382899. El elemento de frontera de un dominio administrativo E ha indicado previamente que las llamadas a 1303538* pueden ser encaminadas directamente a un controlador de acceso del dominio administrativo E sin necesidad de un mensaje AccessRequest, tal como se muestra en la figura G.19. (Este anuncio no indica que la entidad es un controlador de acceso, sino sólo que se podría enviar un mensaje Setup a una dirección especificada.) El elemento de frontera del dominio administrativo D ha recibido esta información del centro de resolución, suponiendo que el centro de resolución de este ejemplo no necesita proveer la resolución de dirección para estas llamadas.

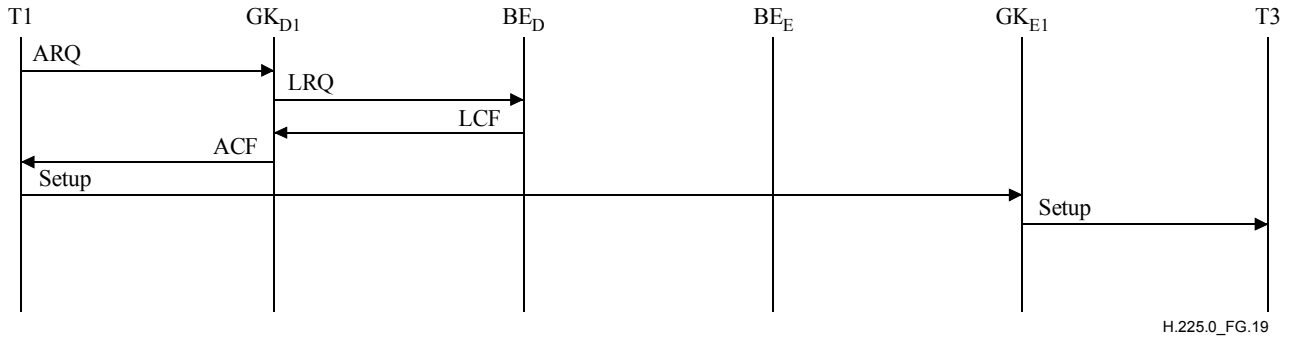


Figura G.19/H.225.0 – Ejemplo de llamada encaminada hacia el controlador de acceso utilizando descriptor caché

Se recuerda que un elemento de frontera puede estar combinado con un controlador de acceso, y puede también encaminar llamadas conforme al modelo de encaminamiento por controlador de acceso. En la figura G.20 se muestra un ejemplo de señalización alternativa. También es posible utilizar un elemento de frontera como controlador de acceso de encaminamiento hacia un dominio administrativo, si los descriptores están configurados para ello.

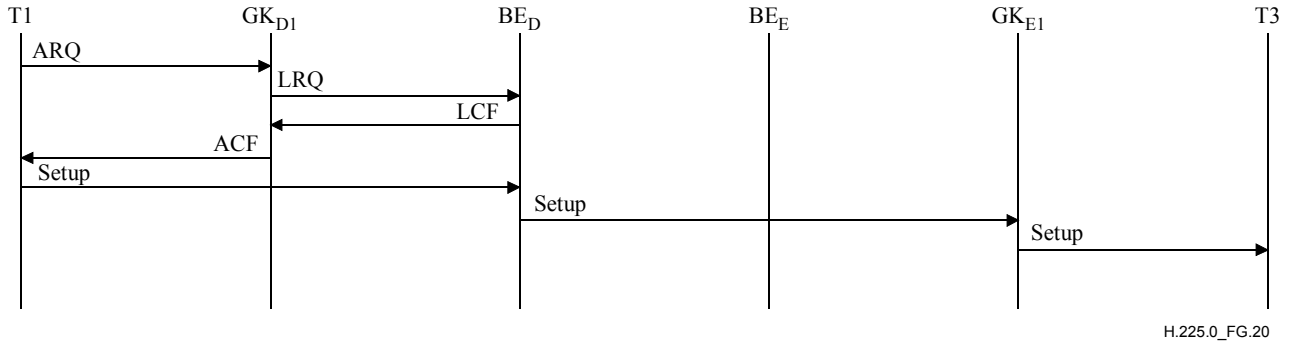


Figura G.20/H.225.0 – Ejemplo de llamada con elemento de frontera/encaminamiento de controlador de acceso combinados

En el ejemplo de la figura G.21, el centro de resolución valida la llamada para el dominio administrativo de terminación. El centro de resolución requiere también que los elementos de frontera de origen y de terminación envíen UsageIndications para las llamadas.

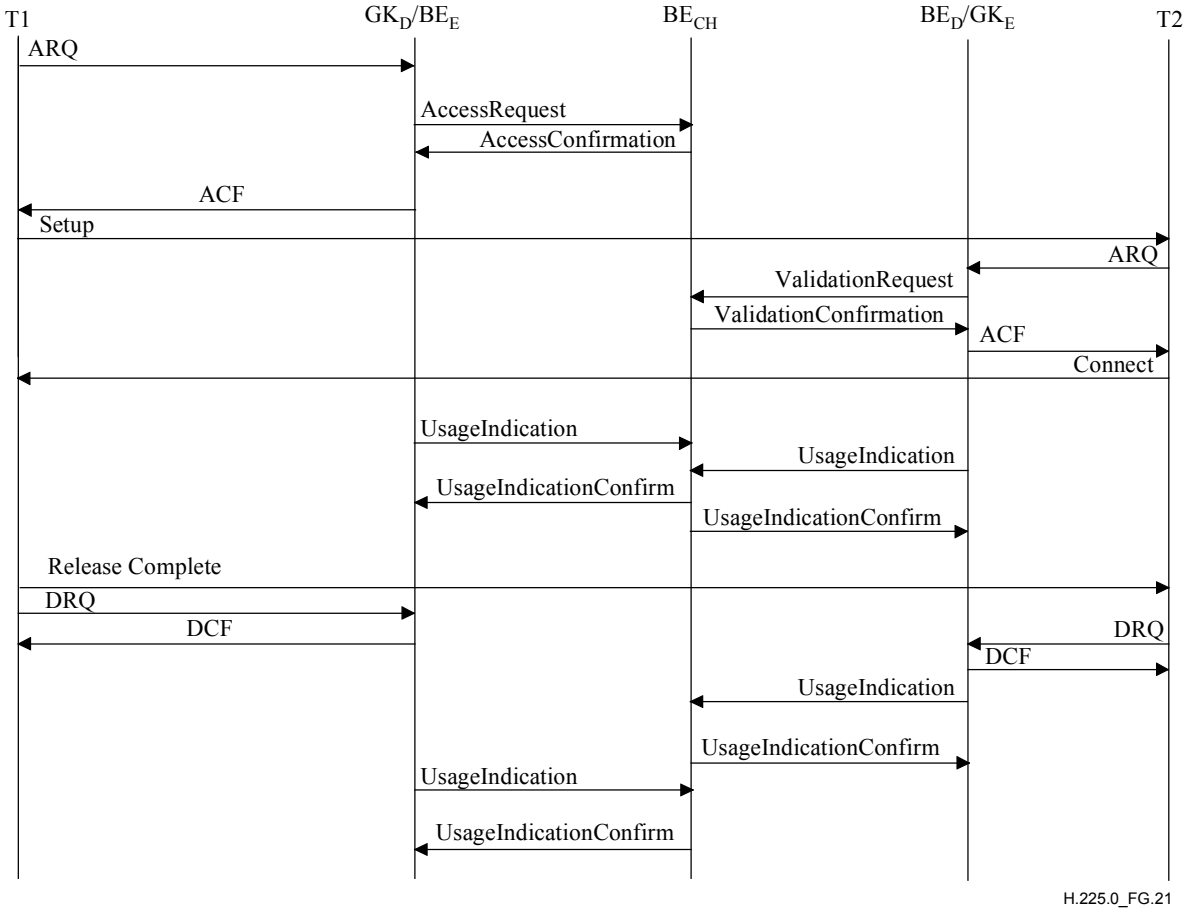


Figura G.21/H.225.0 – Ejemplo de validación e informe de utilización de llamada con coentro de resolución

G.8 Perfiles del anexo G

G.8.1 Introducción

La Rec. UIT-T H.501 ofrece un nutrido conjunto de mensajes y campos que el procedimiento del anexo G/H.225.0 puede utilizar para la interacción entre dominios administrativos y entre elementos pares dentro de un dominio administrativo. Muchos de los mensajes y campos son facultativos y pueden ser usados de diversas maneras para implementar diferentes servicios u opciones de servicio. En esta cláusula se especifican los perfiles de implementación que definen los mensajes, campos y procedimientos requeridos para alegar conformidad con un perfil específico.

G.8.1.1 Señalización y negociación de perfiles

El marco extensible genérico H.323 puede ser utilizado por un elemento par para señalizar a otro elemento par el conjunto de perfiles que necesita para que se pueda efectuar una transacción, el conjunto de perfiles que desea emplear y el conjunto de perfiles que soporta. Esta señalización de negociación de perfiles se puede hacer en un intercambio de mensajes (por ejemplo, en un intercambio AccessRequest/AccessConfirmation), o durante el establecimiento de una relación de servicio. Obsérvese que el establecimiento de una relación de servicio entre dos elementos pares puede no ser requerida por un perfil.

G.8.1.1.1 Procesamiento por la entidad solicitante

Una entidad solicitante (un elemento par) utiliza los elementos en la estructura **`FeatureSet`** (**`conjunto de características`**) para especificar los diversos perfiles que requiere. Especifica el conjunto de perfiles que necesita utilizando el campo **`neededFeatures`** (**`características`**

necesarias), el conjunto de perfiles que desea utilizando el campo **desiredFeatures** (**características deseadas**), y el conjunto de perfiles que soporte en el campo **supportedFeatures** (**características soportadas**). Los tres campos están en la estructura **FeatureSet**.

En respuesta a su petición, una entidad solicitante debe recibir un mensaje de confirmación o de rechazo.

Si la petición es rechazada, la entidad respondedora puede haber incluido un conjunto de **neededFeatures** que la entidad solicitante debe soportar para que la petición tenga éxito. Si éste es el caso, y la entidad solicitante soporta las características necesarias (por ejemplo, un perfil específico), la entidad solicitante puede emitir de nuevo una petición que especifica el soporte para el perfil necesario por la entidad respondedora.

Si la petición es aceptada, hay que aplicar procedimientos especiales para asegurar que la negociación funciona de una manera compatible hacia atrás. Esto se hace solicitando a la entidad que verifique que el perfil que ha especificado como necesario está enumerado como **supportedFeatures** en la respuesta. Si la entidad solicitante no observa los perfiles que necesita en el campo **supportedFeatures** del mensaje de respuesta, supondrá que la entidad respondedora no soporta los perfiles que ella necesita. Si la entidad solicitante determina que no puede continuar en estas circunstancias, anulará la operación que trataba de ejecutar (es decir, enviará un mensaje ServiceRelease si originalmente envió un mensaje ServiceRequest), para que la entidad respondedora vuelva a su estado original.

G.8.1.1.2 Procesamiento por la entidad respondedora

La entidad respondedora busca en los perfiles especificados en el campo **neededFeatures** de la petición para determinar si puede aceptarla. Busca también en los campos **neededFeatures**, **desiredFeatures** y **supportedFeatures** para determinar si los perfiles que necesita sean soportados por la entidad solicitante.

Si la entidad respondedora determina que los conjuntos de perfiles necesario son soportados por ambas entidades, la entidad respondedora puede acusar recibo de la petición. La entidad respondedora enumera el conjunto de perfiles que elige en el campo **supportedFeatures** de su respuesta. Si la petición es aceptada, todas las **neededFeatures** de la petición deben ser incluidas en el campo **supportedFeatures** de la respuesta. La entidad respondedora puede también incluir **desiredFeatures**.

Si la entidad respondedora necesita que la entidad solicitante soporte otros perfiles, rechazará la petición. Si desea declarar los perfiles que deben ser soportados para que la petición sea satisfecha, deberá especificarlo utilizando el campo **neededFeatures** del mensaje de rechazo. La entidad respondedora puede incluir también cualesquiera **desiredFeatures** y **supportedFeatures** en el mensaje de rechazo.

G.8.1.1.3 Identificadores

El siguiente identificador se utiliza dentro de un FeatureDescriptor para especificar que este descriptor se aplica a perfiles del anexo G/H.225.0.

Valor	Descripción
idAnnexGProfiles	Este identificador se utiliza en el campo "id" de FeatureDescriptor para indicar que éste describe los perfiles del anexo G necesarios/deseados/soportados.

El siguiente cuadro contiene una lista de los identificadores usados en el marco de extensibilidad genérico, que son pertinentes al anexo G/H.225.0.

Valor INTEGER normalizado	Descripción
0	Identificador dentro de FeatureDescriptor que indica que este descriptor describe perfiles del anexo G/H.225.0
1	Identificador dentro de EnumeratedParameter que identifica el perfil "A" del anexo G/H.225.0

G.8.2 Perfil "A": Encaminamiento de llamadas entre zonas a un controlador de acceso fiable

Este perfil especifica un simple servicio dentro del dominio: consultas llamada por llamada a otra zona fiable para determinación del punto extremo cuando la dirección de señalización del anexo G de las zonas fiables se proporciona estáticamente. Éste es uno de los usos más sencillos del procedimiento del anexo G y es similar al uso de RAS LRQ para indagar otra zona para un punto extremo. El mismo perfil se puede utilizar para indagar un elemento par fiable, que devuelve rutas de conocimiento de todo el dominio, o las obtiene mediante otras consultas del anexo G.

G.8.2.1 Mensajes requeridos

Las entidades conformes con este perfil soportarán los mensajes indicados como "obligatorios" (M, *mandatory*) en el siguiente cuadro:

Mensaje	Transmisión [obligatorio (M), opcional (O), recomendado (R)]	Recepción y ejecución [obligatorio (M), opcional (O), recomendado (R)]
ServiceRequest	O	M (nota 1)
ServiceConfirmation	O	O
ServiceRejection	M	O
ServiceRelease	O	O
DescriptorRequest	O	M (nota 1)
DescriptorConfirmation	R (nota 2)	O
DescriptorRejection	M	O
DescriptorIdRequest	O	M (nota 1)
DescriptorIdConfirmation	R (nota 3)	O
DescriptorIdRejection	M	O
DescriptorUpdate	O	M (nota 4)
DescriptorUpdateAck	M	O
AccessRequest	M	M
AccessConfirmation	M	M
AccessRejection	M	M
RequestInProgress	M	M
NonStandardRequest	O	M
NonStandardConfirmation	O	O
NonStandardRejection	M	O
UnknownMessageResponse	M	M
UsageRequest	O	M (nota 1)
UsageConfirmation	O	O
UsageRejection	M	O

Mensaje	Transmisión [obligatorio (M), opcional (O), recomendado (R)]	Recepción y ejecución [obligatorio (M), opcional (O), recomendado (R)]
UsageIndication	O	M (nota 1)
UsageIndicationConfirmation	O	O
UsageIndicationRejection	M	O
ValidationRequest	O	M (nota 1)
ValidationConfirmation	O	O
ValidationRejection	M	O
NOTA 1 – Será recibido y, como mínimo, rechazado. NOTA 2 – Se recomienda que una entidad devuelva, como mínimo, un descriptor para una plantilla con SendAccessRequest indicando a sí misma. NOTA 3 – Se recomienda que una entidad devuelva, como mínimo, un descriptor para una plantilla con SendAccessRequest indicando a sí misma. NOTA 4 – Será recibido y se acusará recibo, pero no tiene que ser procesado.		

G.8.2.2 Campos requeridos

Todos los campos definidos como obligatorios por la Rec. UIT-T H.501 son también obligatorios dentro de este perfil.

Las entidades conformes con este perfil soportarán también los campos especificados en el siguiente cuadro.

Otros campos definidos como opcionales por la Rec. UIT-T H.501 pueden estar presentes facultativamente.

Mensaje o estructura	Campo requerido	Comentarios
Mensaje AccessRequest	`destinationInfo`	Una dirección que contiene la dirección E.164 completamente calificada del destino
	`sourceInfo`	Incluye domainInfo y endpointType
	`callInfo`	
Mensaje AccessConfirmation	`templates`	Si hay plantillas presentes, hay una plantilla por cada pasarela/controlador de acceso de terminación
	`partialResponse`	Puesto a FALSO
Estructura AddressTemplate	`pattern`	Un patrón específico está presente con el número E.164
	`routeInfo`	Un ejemplar presente
	`timeToLive`	
Estructura RouteInformation	`messageType`	Presente
	`callSpecific`	Puesto a FALSO
	`contacts`	Un ejemplar presente
	`type`	Debe estar presente si messageType = **sendSetup**
Estructura ContactInformation	`transportAddress`	La dirección IP de la pasarela/controlador de acceso
	`priority`	

G.8.2.3 Procedimientos requeridos

En este perfil, las entidades pueden aplicar los procedimientos de localización estáticos del anexo G (véase G.6.3.1) y habrá una lista configurada de elementos de pares o controladores de acceso a los cuales se puede enviar peticiones. Esta lista puede contener alternativas que sólo se han de utilizar cuando el elemento primario no puede ser alcanzado o se puede simplemente añadir las alternativas (si hubiere alguna) a la lista.

Las entidades pueden también utilizar los procedimientos de localización dinámicos del anexo G (véase G.6.3.2).

Las entidades enviarán un mensaje AccessRequest a un elemento par o controlador de acceso seleccionado para cada llamada. Si se puede interrogar a más de un elemento par o controlador de acceso para una llamada determinada, no se especifica si deben ser consultados en secuencia o en paralelo. Esta opción se deja a la entidad solicitante.

La respuesta será ninguna o más plantillas. **`timeToLive`** se puede fijar a 60 segundos o menos para indicar que no se puede utilizar para otra llamada.

Para mejorar la interoperación con más pares generales, se sugiere que cuando el elemento par no soporte descriptores, se sigan los siguientes procedimientos:

- Si se recibe un mensaje DescriptorIDRequest, el elemento par debe devolver un mensaje DescriptorIDConfirmation que contiene un solo **`DescriptorInfo`**. Este **`DescriptorInfo`** describe un descriptor que contiene una sola plantilla que especifica **`sendAccessRequest`** apuntando al propio elemento par.
- Si se recibe un mensaje DescriptorRequest, el elemento par debe devolver un mensaje DescriptorConfirmation que contiene un solo descriptor. Este descriptor contendrá una sola plantilla que especifica **`sendAccessRequest`** apuntando al propio elemento par.

G.8.2.4 Identificadores para el perfil "A"

El siguiente identificador se utiliza en un **`EnumeratedParameter`** para indicar que **`EnumeratedParameter`** especifica el perfil A del anexo G/H.225.0.

Valor	Descripción
idAnnexGProfileA	Este identificador se utiliza en el campo "id" de un **`EnumeratedParameter`** para indicar que se necesita/desea/soporta al perfil A del anexo G. Obsérvese que el campo "content" (contenido) del **`EnumeratedParameter`** no está presente.

Anexo H

Sintaxis de mensajes H.225.0 (ASN.1)

Esta Recomendación define protocolos para RAS (esencialmente un protocolo de controlador de acceso) y señalización de llamada (esencialmente unidades de datos de protocolo que residen en un elemento de información usuario-usuario). Estos protocolos se definen conjuntamente en el siguiente árbol ASN.1. Las definiciones semánticas para los mensajes y diversos elementos figuran en cláusulas anteriores.

```
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;
H323-UserInformation ::= SEQUENCE     -- root for all H.225.0 call signalling
                                         messages
{
     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,     -- used when a Facility message is sent,
                                   -- but the Facility-UUIE is not to be invoked
                                   -- (possible when transporting supplementary
                                   -- services messages in versions prior to
                                   -- H.225.0 version 4)
          status              Status-UUIE,
          statusInquiry       StatusInquiry-UUIE,
          setupAcknowledge    SetupAcknowledge-UUIE,
          notify              Notify-UUIE
     },
     nonStandardData          NonStandardParameter OPTIONAL,
     ...,
     h4501SupplementaryService   SEQUENCE OF OCTET STRING OPTIONAL,
                              -- each sequence of octet string is defined as one
                              -- H4501SupplementaryService APDU as defined in
                              -- Table 3/H.450.1
```

```
    h245Tunnelling          BOOLEAN,
                            -- if TRUE, tunnelling of H.245 messages is enabled
    h245Control             SEQUENCE OF OCTET STRING OPTIONAL,
    nonStandardControl      SEQUENCE OF NonStandardParameter OPTIONAL,
    callLinkage             CallLinkage OPTIONAL,
    tunnelledSignallingMessage  SEQUENCE
    {
        tunnelledProtocolID     TunnelledProtocol, -- tunnelled signalling
                                                   protocol ID
        messageContent          SEQUENCE OF OCTET STRING, -- sequence of entire
                                                          -- message(s)
        tunnellingRequired      NULL OPTIONAL,
        nonStandardData         NonStandardParameter OPTIONAL,
        ...
    } OPTIONAL,
    provisionalRespToH245Tunnelling  NULL OPTIONAL,
    stimulusControl                  StimulusControl OPTIONAL,
    genericData                      SEQUENCE OF GenericData OPTIONAL
}

StimulusControl ::= SEQUENCE
{
    nonStandard                      NonStandardParameter OPTIONAL,
    isText                           NULL OPTIONAL,
    h248Message                      OCTET STRING OPTIONAL,
    ...
}

Alerting-UUIE ::= SEQUENCE
{
    protocolIdentifier          ProtocolIdentifier,
    destinationInfo             EndpointType,
    h245Address                 TransportAddress OPTIONAL,
    ...,
    callIdentifier              CallIdentifier,
    h245SecurityMode            H245Security OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
    multipleCalls               BOOLEAN,
    maintainConnection          BOOLEAN,
    alertingAddress             SEQUENCE OF AliasAddress OPTIONAL,
    presentationIndicator       PresentationIndicator OPTIONAL,
    screeningIndicator          ScreeningIndicator OPTIONAL,
    fastConnectRefused          NULL OPTIONAL,
    serviceControl              SEQUENCE OF ServiceControlSession OPTIONAL,
    capacity                    CallCapacity OPTIONAL,
    featureSet                  FeatureSet OPTIONAL
}

CallProceeding-UUIE ::= SEQUENCE
{
    protocolIdentifier          ProtocolIdentifier,
    destinationInfo             EndpointType,
    h245Address                 TransportAddress OPTIONAL,
    ...,
    callIdentifier              CallIdentifier,
    h245SecurityMode            H245Security OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
    multipleCalls               BOOLEAN,
    maintainConnection          BOOLEAN,
```

```
     fastConnectRefused          NULL OPTIONAL,
     featureSet                  FeatureSet OPTIONAL
}

Connect-UUIE ::= SEQUENCE
{
     protocolIdentifier          ProtocolIdentifier,
     h245Address                 TransportAddress OPTIONAL,
     destinationInfo             EndpointType,
     conferenceID                ConferenceIdentifier,
     ...,
     callIdentifier              CallIdentifier,
     h245SecurityMode            H245Security OPTIONAL,
     tokens                      SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
     fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
     multipleCalls               BOOLEAN,
     maintainConnection          BOOLEAN,
     language                    SEQUENCE OF IA5String (SIZE (1..32)) OPTIONAL,
                                 -- RFC 1766 language tag
     connectedAddress            SEQUENCE OF AliasAddress OPTIONAL,
     presentationIndicator       PresentationIndicator OPTIONAL,
     screeningIndicator          ScreeningIndicator OPTIONAL,
     fastConnectRefused          NULL OPTIONAL,
     serviceControl              SEQUENCE OF ServiceControlSession OPTIONAL,
     capacity                    CallCapacity OPTIONAL,
     featureSet                  FeatureSet OPTIONAL
}

Information-UUIE ::=SEQUENCE
{
     protocolIdentifier          ProtocolIdentifier,
     ...,
     callIdentifier              CallIdentifier,
     tokens                      SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
     fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
     fastConnectRefused          NULL OPTIONAL,
     circuitInfo                 CircuitInfo OPTIONAL
}

ReleaseComplete-UUIE ::= SEQUENCE
{
     protocolIdentifier          ProtocolIdentifier,
     reason                      ReleaseCompleteReason OPTIONAL,
     ...,
     callIdentifier              CallIdentifier,
     tokens                      SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
     busyAddress                 SEQUENCE OF AliasAddress OPTIONAL,
     presentationIndicator       PresentationIndicator OPTIONAL,
     screeningIndicator          ScreeningIndicator OPTIONAL,
     capacity                    CallCapacity OPTIONAL,
     serviceControl              SEQUENCE OF ServiceControlSession OPTIONAL,
     featureSet                  FeatureSet OPTIONAL
}

ReleaseCompleteReason ::= CHOICE
{
     noBandwidth                 NULL, -- bandwidth taken away or ARQ denied
     gatekeeperResources         NULL, -- exhausted
     unreachableDestination      NULL, -- no transport path to the destination
     destinationRejection        NULL, -- rejected at destination
     invalidRevision             NULL,
```

```
    noPermission                NULL, -- called party's gatekeeper rejects
    unreachableGatekeeper       NULL, -- terminal cannot reach gatekeeper
                                      -- for ARQ
    gatewayResources            NULL,
    badFormatAddress            NULL,
    adaptiveBusy                NULL, -- call is dropping due to LAN crowding
    inConf                      NULL, -- called party busy
    undefinedReason             NULL,
    ...,
    facilityCallDeflection      NULL, -- call was deflected using a Facility
                                      -- message
    securityDenied              NULL, -- incompatible security settings
    calledPartyNotRegistered    NULL, -- used by gatekeeper when endpoint has
                                      -- preGrantedARQ to bypass ARQ/ACF
    callerNotRegistered         NULL, -- used by gatekeeper when endpoint has
                                      -- preGrantedARQ to bypass ARQ/ACF
    newConnectionNeeded         NULL, -- indicates that the Setup was not
                                      -- accepted on this connection, but that
                                      -- the Setup may be accepted on
                                      -- a new connection
    nonStandardReason           NonStandardParameter,
    replaceWithConferenceInvite ConferenceIdentifier, -- call dropped due to
                                                      -- subsequent invitation
                                                      -- to a conference
                                                      -- (see 8.4.3.8/H.323)
    genericDataReason           NULL,
    neededFeatureNotSupported   NULL,
    tunnelledSignallingRejected NULL,
    invalidCID                  NULL,
    securityError               SecurityErrors,
    hopCountExceeded            NULL
}

Setup-UUIE ::= SEQUENCE
{
    protocolIdentifier      ProtocolIdentifier,
    h245Address             TransportAddress OPTIONAL,
    sourceAddress           SEQUENCE OF AliasAddress OPTIONAL,
    sourceInfo              EndpointType,
    destinationAddress      SEQUENCE OF AliasAddress OPTIONAL,
    destCallSignalAddress   TransportAddress OPTIONAL,
    destExtraCallInfo       SEQUENCE OF AliasAddress OPTIONAL,
    destExtraCRV            SEQUENCE OF CallReferenceValue OPTIONAL,
    activeMC                BOOLEAN,
    conferenceID            ConferenceIdentifier,
    conferenceGoal          CHOICE
    {
        create              NULL,
        join                NULL,
        invite              NULL,
        ...,
        capability-negotiation                NULL,
        callIndependentSupplementaryService   NULL
    },
    callServices            QseriesOptions OPTIONAL,
    callType                CallType,
    ...,
    sourceCallSignalAddress     TransportAddress OPTIONAL,
    remoteExtensionAddress      AliasAddress OPTIONAL,
    callIdentifier              CallIdentifier,
    h245SecurityCapability      SEQUENCE OF H245Security OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
```

```
    mediaWaitForConnect          BOOLEAN,
    canOverlapSend               BOOLEAN,
    endpointIdentifier           EndpointIdentifier OPTIONAL,
    multipleCalls                BOOLEAN,
    maintainConnection           BOOLEAN,
    connectionParameters         SEQUENCE  -- additional gateway parameters
    {
        connectionType               ScnConnectionType,
        numberOfScnConnections       INTEGER (0..65535),
        connectionAggregation        ScnConnectionAggregation,
        ...
    } OPTIONAL,
    language                     SEQUENCE OF IA5String (SIZE (1..32)) OPTIONAL,
                                 -- RFC1766 language tag
    presentationIndicator        PresentationIndicator OPTIONAL,
    screeningIndicator           ScreeningIndicator OPTIONAL,
    serviceControl               SEQUENCE OF ServiceControlSession OPTIONAL,
    symmetricOperationRequired   NULL OPTIONAL,
    capacity                     CallCapacity OPTIONAL,
    circuitInfo                  CircuitInfo OPTIONAL,
    desiredProtocols             SEQUENCE OF SupportedProtocols OPTIONAL,
    neededFeatures               SEQUENCE OF FeatureDescriptor OPTIONAL,
    desiredFeatures              SEQUENCE OF FeatureDescriptor OPTIONAL,
    supportedFeatures            SEQUENCE OF FeatureDescriptor OPTIONAL,
    parallelH245Control          SEQUENCE OF OCTET STRING OPTIONAL,
    additionalSourceAddresses    SEQUENCE OF ExtendedAliasAddress OPTIONAL,
    hopCount                     INTEGER (1..31) OPTIONAL
}

ScnConnectionType ::= CHOICE
{
    unknown     NULL,  -- should be seleceted when connection type is unknown
    bChannel    NULL,  -- each individual connection on the SCN is 64 kbit/s.
                       -- Note that where SCN delivers 56 kbit/s usable data,
                       -- the actual bandwidth allocated on SCN is still
                       -- 64 kbit/s.
    hybrid2x64  NULL,  -- each connection is a 128 kbit/s hybrid call
    hybrid384   NULL,  -- each connection is an H0 (384 kbit/s) hybrid call
    hybrid1536  NULL,  -- each connection is an H11 (1536 kbit/s) hybrid call
    hybrid1920  NULL,  -- each connection is an H12 (1920 kbit/s) hybrid call
    multirate   NULL,  -- bandwidth supplied by SCN using multirate.
                       -- In this case, the information transfer rate octet
                       -- in the bearer capability shall be set to multirate
                       -- and the rate multiplier octet shall denote the
                      -- number of B channels.
    ...
}

ScnConnectionAggregation ::= CHOICE
{
    auto          NULL,     -- aggregation mechanism is unknown
    none          NULL,     -- call produced using a single SCN connection
    h221          NULL,     -- use H.221 framing to aggregate the connections
    bonded-mode1  NULL,     -- use ISO/IEC 13871 bonding mode 1.
                            -- Use bonded-mode1 to signal a bonded call if the
                            -- precise bonding mode to be used is unknown.
    bonded-mode2  NULL,     -- use ISO/IEC 13871 bonding mode 2
    bonded-mode3  NULL,     -- use ISO/IEC 13871 bonding mode 3
    ...
}
```

```
PresentationIndicator ::= CHOICE
{
     presentationAllowed          NULL,
     presentationRestricted       NULL,
     addressNotAvailable          NULL,
     ...
}

ScreeningIndicator ::= ENUMERATED
{
     userProvidedNotScreened (0),
          -- number was provided by a remote user
          -- and has not been screened by a gatekeeper
     userProvidedVerifiedAndPassed (1),
          -- number was provided by user
          -- equipment (or by a remote network), and has
          -- been screened by a gatekeeper
     userProvidedVerifiedAndFailed (2),
          -- number was provided by user
          -- equipment (or by a remote network), and the
          -- gatekeeper has determined that the
          -- information is incorrect
     networkProvided (3),
          -- number was provided by a gatekeeper
     ...
}

Facility-UUIE ::= SEQUENCE
{
     protocolIdentifier           ProtocolIdentifier,
     alternativeAddress           TransportAddress OPTIONAL,
     alternativeAliasAddress      SEQUENCE OF AliasAddress OPTIONAL,
     conferenceID                 ConferenceIdentifier OPTIONAL,
     reason                       FacilityReason,
     ...,
     callIdentifier               CallIdentifier,
     destExtraCallInfo            SEQUENCE OF AliasAddress OPTIONAL,
     remoteExtensionAddress       AliasAddress OPTIONAL,
     tokens                       SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                 SEQUENCE OF CryptoH323Token OPTIONAL,
     conferences                  SEQUENCE OF ConferenceList OPTIONAL,
     h245Address                  TransportAddress OPTIONAL,
     fastStart                    SEQUENCE OF OCTET STRING OPTIONAL,
     multipleCalls                BOOLEAN,
     maintainConnection           BOOLEAN,
     fastConnectRefused           NULL OPTIONAL,
     serviceControl               SEQUENCE OF ServiceControlSession OPTIONAL,
     circuitInfo                  CircuitInfo OPTIONAL,
     featureSet                   FeatureSet OPTIONAL,
     destinationInfo              EndpointType OPTIONAL,
     h245SecurityMode             H245Security OPTIONAL
}

ConferenceList ::= SEQUENCE
{
     conferenceID                 ConferenceIdentifier OPTIONAL,
     conferenceAlias              AliasAddress OPTIONAL,
     nonStandardData              NonStandardParameter OPTIONAL,
     ...
}
```

```
FacilityReason ::= CHOICE
{
     routeCallToGatekeeper   NULL,     -- call must use gatekeeper model
                                       -- gatekeeper is alternativeAddress
     callForwarded           NULL,
     routeCallToMC           NULL,
     undefinedReason         NULL,
     ...,
     conferenceListChoice    NULL,
     startH245               NULL,     -- recipient should connect to h245Address
     noH245                  NULL,     -- endpoint does not support H.245
     newTokens               NULL,
     featureSetUpdate        NULL,
     forwardedElements       NULL,
     transportedInformation  NULL
}

Progress-UUIE ::= SEQUENCE
{
     protocolIdentifier      ProtocolIdentifier,
     destinationInfo         EndpointType,
     h245Address             TransportAddress OPTIONAL,
     callIdentifier          CallIdentifier,
     h245SecurityMode        H245Security OPTIONAL,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     fastStart               SEQUENCE OF OCTET STRING OPTIONAL,
     ...,
     multipleCalls           BOOLEAN,
     maintainConnection      BOOLEAN,
     fastConnectRefused      NULL OPTIONAL
}

TransportAddress ::= CHOICE
{
     ipAddress SEQUENCE
     {
          ip             OCTET STRING (SIZE(4)),
          port           INTEGER(0..65535)
     },
     ipSourceRoute       SEQUENCE
     {
          ip             OCTET STRING (SIZE(4)),
          port           INTEGER(0..65535),
          route          SEQUENCE OF OCTET STRING (SIZE(4)),
          routing        CHOICE
          {
               strict    NULL,
               loose     NULL,
               ...
          },
          ...
     },
     ipxAddress     SEQUENCE
     {
          node           OCTET STRING (SIZE(6)),
          netnum         OCTET STRING (SIZE(4)),
          port           OCTET STRING (SIZE(2))
     },
     ip6Address     SEQUENCE
     {
          ip             OCTET STRING (SIZE(16)),
```

```
          port           INTEGER(0..65535),
          ...
     },
     netBios             OCTET STRING (SIZE(16)),
     nsap                OCTET STRING (SIZE(1..20)),
     nonStandardAddress NonStandardParameter,
     ...
}

Status-UUIE ::= SEQUENCE
{
     protocolIdentifier ProtocolIdentifier,
     callIdentifier     CallIdentifier,
     tokens             SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens       SEQUENCE OF CryptoH323Token OPTIONAL,
     ...
}

StatusInquiry-UUIE ::= SEQUENCE
{
     protocolIdentifier ProtocolIdentifier,
     callIdentifier     CallIdentifier,
     tokens             SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens       SEQUENCE OF CryptoH323Token OPTIONAL,
     ...
}

SetupAcknowledge-UUIE ::= SEQUENCE
{
     protocolIdentifier ProtocolIdentifier,
     callIdentifier     CallIdentifier,
     tokens             SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens       SEQUENCE OF CryptoH323Token OPTIONAL,
     ...
}

Notify-UUIE ::= SEQUENCE
{
     protocolIdentifier ProtocolIdentifier,
     callIdentifier     CallIdentifier,
     tokens             SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens       SEQUENCE OF CryptoH323Token OPTIONAL,
     ...
}

-- Beginning of common message elements section

EndpointType ::= SEQUENCE
{
     nonStandardData    NonStandardParameter OPTIONAL,
     vendor             VendorIdentifier OPTIONAL,
     gatekeeper         GatekeeperInfo OPTIONAL,
     gateway            GatewayInfo OPTIONAL,
     mcu                McuInfo OPTIONAL,  -- mc must be set as well
     terminal           TerminalInfo OPTIONAL,
     mc                 BOOLEAN,           -- shall not be set by itself
     undefinedNode      BOOLEAN,
     ...,
     set           BIT STRING (SIZE(32)) OPTIONAL,
                         -- shall not be used with mc, gatekeeper
                         -- code points for the various SET devices
                         -- are defined in the respective SET Annexes
```

```
    supportedTunnelledProtocols  SEQUENCE OF TunnelledProtocol OPTIONAL
                            -- list of supported tunnelled protocols
}

GatewayInfo ::= SEQUENCE
{
    protocol                SEQUENCE OF SupportedProtocols OPTIONAL,
    nonStandardData         NonStandardParameter OPTIONAL,
    ...
}

SupportedProtocols ::= CHOICE
{
    nonStandardData         NonStandardParameter,
    h310                    H310Caps,
    h320                    H320Caps,
    h321                    H321Caps,
    h322                    H322Caps,
    h323                    H323Caps,
    h324                    H324Caps,
    voice                   VoiceCaps,
    t120-only               T120OnlyCaps,
    ...,
    nonStandardProtocol     NonStandardProtocol,
    t38FaxAnnexbOnly        T38FaxAnnexbOnlyCaps,
    sip                     SIPCaps
}

H310Caps ::= SEQUENCE
{
    nonStandardData         NonStandardParameter OPTIONAL,
    ...,
    dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
    supportedPrefixes       SEQUENCE OF SupportedPrefix
}

H320Caps ::= SEQUENCE
{
    nonStandardData         NonStandardParameter OPTIONAL,
    ...,
    dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
    supportedPrefixes       SEQUENCE OF SupportedPrefix
}

H321Caps ::= SEQUENCE
{
    nonStandardData         NonStandardParameter OPTIONAL,
    ...,
    dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
    supportedPrefixes       SEQUENCE OF SupportedPrefix
}

H322Caps ::= SEQUENCE
{
    nonStandardData         NonStandardParameter OPTIONAL,
    ...,
    dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
    supportedPrefixes       SEQUENCE OF SupportedPrefix
}
```

```
H323Caps ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix
}

H324Caps ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix
}

VoiceCaps ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix
}

T120OnlyCaps ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix
}

NonStandardProtocol ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix,
     ...
}

T38FaxAnnexbOnlyCaps ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix,
     t38FaxProtocol          DataProtocolCapability,
     t38FaxProfile           T38FaxProfile,
     ...
}

SIPCaps ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     dataRatesSupported      SEQUENCE OF DataRate OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix OPTIONAL,
     ...
}

McuInfo ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     protocol                SEQUENCE OF SupportedProtocols OPTIONAL
}
```

```
TerminalInfo ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     ...
}

GatekeeperInfo ::= SEQUENCE
{
     nonStandardData         NonStandardParameter OPTIONAL,
     ...
}

VendorIdentifier ::= SEQUENCE
{
     vendor         H221NonStandard,
     productId      OCTET STRING (SIZE(1..256)) OPTIONAL,     -- per vendor
     versionId      OCTET STRING (SIZE(1..256)) OPTIONAL,     -- per product
     ...,
     enterpriseNumber   OBJECT IDENTIFIER OPTIONAL
}

H221NonStandard ::= SEQUENCE
{    t35CountryCode     INTEGER(0..255),
     t35Extension       INTEGER(0..255),
     manufacturerCode   INTEGER(0..65535),
     ...
}

TunnelledProtocol ::= SEQUENCE
{
     id CHOICE
     {
     tunnelledProtocolObjectID             OBJECT IDENTIFIER,
          tunnelledProtocolAlternateID     TunnelledProtocolAlternateIdentifier,
          ...
     },
     subIdentifier                         IA5String (SIZE (1..64)) OPTIONAL,
     ...
}

TunnelledProtocolAlternateIdentifier ::= SEQUENCE
{
     protocolType            IA5String (SIZE (1..64)),
     protocolVariant         IA5String (SIZE (1..64)) OPTIONAL,
     ...
}

NonStandardParameter ::= SEQUENCE
{
     nonStandardIdentifier   NonStandardIdentifier,
     data                    OCTET STRING
}

NonStandardIdentifier        ::= CHOICE
{
     object                  OBJECT IDENTIFIER,
     h221NonStandard         H221NonStandard,
     ...
}
```

```
AliasAddress ::= CHOICE
{
     dialledDigits IA5String (SIZE (1..128)) (FROM ("0123456789#*,")),
     h323-ID       BMPString (SIZE (1..256)), -- Basic ISO/IEC 10646-1 (Unicode)
     ...,
     url-ID        IA5String (SIZE(1..512)),  -- URL style address
     transportID   TransportAddress,
     email-ID      IA5String (SIZE(1..512)),  -- rfc822-compliant email address
     partyNumber   PartyNumber,
     mobileUIM     MobileUIM
}

AddressPattern ::= CHOICE
{
wildcard  AliasAddress,
range          SEQUENCE
{
startOfRange   PartyNumber,
endOfRange     PartyNumber
},
...
}

PartyNumber ::= CHOICE
{
     e164Number                   PublicPartyNumber,
                                       -- the numbering plan is according to
                                       -- ITU-T Recs E.163 and E.164.
     dataPartyNumber              NumberDigits,
                                       -- not used, value reserved.
     telexPartyNumber             NumberDigits,
                                       -- not used, value reserved.
     privateNumber                PrivatePartyNumber,
                                       -- the numbering plan is according to
                                       -- ISO/IEC 11571.
     nationalStandardPartyNumber  NumberDigits,
                                       -- not used, value reserved.
     ...
}

PublicPartyNumber ::= SEQUENCE
{
     publicTypeOfNumber      PublicTypeOfNumber,
     publicNumberDigits      NumberDigits
}

PrivatePartyNumber ::= SEQUENCE
{
     privateTypeOfNumber     PrivateTypeOfNumber,
     privateNumberDigits     NumberDigits
}

NumberDigits ::= IA5String (SIZE (1..128)) (FROM ("0123456789#*,"))

PublicTypeOfNumber ::= CHOICE
{
     unknown                 NULL,
                                       -- if used number digits carry prefix
                                       -- indicating type
                                       -- of number according to national
                                       -- recommendations.
     internationalNumber     NULL,
     nationalNumber          NULL,
```

```
     networkSpecificNumber   NULL,
                                        -- not used, value reserved
     subscriberNumber        NULL,
     abbreviatedNumber       NULL,
                                        -- valid only for called party number at
                                        -- the outgoing access, network
                                        -- substitutes appropriate number.
...
}

PrivateTypeOfNumber ::= CHOICE
{
     unknown                 NULL,
     level2RegionalNumber    NULL,
     level1RegionalNumber    NULL,
     pISNSpecificNumber      NULL,
     localNumber             NULL,
     abbreviatedNumber       NULL,
     ...
}

MobileUIM ::= CHOICE
{
     ansi-41-uim ANSI-41-UIM,     -- Americas standards Wireless Networks
     gsm-uim GSM-UIM,             -- European standards Wireless Networks
     ...
}

TBCD-STRING ::= IA5String (FROM ("0123456789#*abc"))

ANSI-41-UIM ::= SEQUENCE
{
     imsi               TBCD-STRING (SIZE (3..16)) OPTIONAL,
     min                TBCD-STRING (SIZE (3..16)) OPTIONAL,
     mdn                TBCD-STRING (SIZE (3..16)) OPTIONAL,
     msisdn             TBCD-STRING (SIZE (3..16)) OPTIONAL,
     esn                TBCD-STRING (SIZE (16)) OPTIONAL,
     mscid              TBCD-STRING (SIZE (3..16)) OPTIONAL,
     system-id CHOICE
     {
          sid           TBCD-STRING (SIZE (1..4)),
          mid           TBCD-STRING (SIZE (1..4)),
          ...
     },
     systemMyTypeCode   OCTET STRING (SIZE (1)) OPTIONAL,
     systemAccessType   OCTET STRING (SIZE (1)) OPTIONAL,
     qualificationInformationCode OCTET STRING (SIZE (1)) OPTIONAL,
     sesn               TBCD-STRING (SIZE (16)) OPTIONAL,
     soc                TBCD-STRING (SIZE (3..16)) OPTIONAL,
     ...
     -- IMSI refers to International Mobile Station Identification
     -- MIN refers to Mobile Identification Number
     -- MDN refers to Mobile Directory Number
     -- MSISDN refers to Mobile Station ISDN number
     -- ESN Refers to Electronic Serial Number
     -- MSCID refers to Mobile Switching Center number + Market ID or System ID
     -- SID refers to System Identification and MID refers to Market
     -- Identification
     -- SystemMyTypeCode refers to vendor identification number
     -- SystemAccessType refers to the system access type like power down
     -- registration or call
     -- origination or Short Message response etc.
     -- Qualification Information Code refers to the validity
```

```
    -- SESN Refers to SIM Electronic Serial Number for Security purposes of
    -- User
    -- Identification
    -- SOC refers to System Operator Code
}

GSM-UIM ::= SEQUENCE
{
    imsi               TBCD-STRING (SIZE (3..16)) OPTIONAL,
    tmsi               OCTET STRING (SIZE (1..4)) OPTIONAL,
    msisdn             TBCD-STRING (SIZE (3..16)) OPTIONAL,
    imei               TBCD-STRING (SIZE (15..16)) OPTIONAL,
    hplmn              TBCD-STRING (SIZE (1..4)) OPTIONAL,
    vplmn              TBCD-STRING (SIZE (1..4)) OPTIONAL,
    -- IMSI refers to International Mobile Station Identification
    -- MSISDN refers to Mobile Station ISDN number
    -- IMEI Refers to International Mobile Equipment Identification
    -- VPLMN or HPLMN refers to Visiting or Home Public Land Mobile Network
    -- number
    ...
}

ExtendedAliasAddress ::= SEQUENCE
{
    address                 AliasAddress,
    presentationIndicator   PresentationIndicator OPTIONAL,
    screeningIndicator      ScreeningIndicator OPTIONAL,
    ...
}

Endpoint ::= SEQUENCE
{
    nonStandardData             NonStandardParameter OPTIONAL,
    aliasAddress                SEQUENCE OF AliasAddress OPTIONAL,
    callSignalAddress           SEQUENCE OF TransportAddress OPTIONAL,
    rasAddress                  SEQUENCE OF TransportAddress OPTIONAL,
    endpointType                EndpointType OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    priority                    INTEGER(0..127) OPTIONAL,
    remoteExtensionAddress      SEQUENCE OF AliasAddress OPTIONAL,
    destExtraCallInfo           SEQUENCE OF AliasAddress OPTIONAL,
    ...,
    alternateTransportAddresses AlternateTransportAddresses OPTIONAL,
    circuitInfo                 CircuitInfo   OPTIONAL,
    featureSet                  FeatureSet    OPTIONAL
}

AlternateTransportAddresses ::= SEQUENCE
{
    annexE             SEQUENCE OF TransportAddress OPTIONAL,
    ...,
    sctp               SEQUENCE OF TransportAddress OPTIONAL
}

UseSpecifiedTransport ::= CHOICE
{
    tcp                NULL,
    annexE             NULL,
    ...,
    sctp               NULL
}
```

```
AlternateGK ::= SEQUENCE
{
     rasAddress              TransportAddress,
     gatekeeperIdentifier    GatekeeperIdentifier  OPTIONAL,
     needToRegister          BOOLEAN,
     priority                INTEGER (0..127),
     ...
}

AltGKInfo ::=SEQUENCE
{
     alternateGatekeeper     SEQUENCE OF AlternateGK,
     altGKisPermanent        BOOLEAN,
     ...
}

SecurityServiceMode ::= CHOICE
{
     nonStandard        NonStandardParameter,
     none               NULL,
     default            NULL,
     ...                -- can be extended with other specific modes
}

SecurityCapabilities ::= SEQUENCE
{
     nonStandard             NonStandardParameter OPTIONAL,
     encryption              SecurityServiceMode,
     authenticaton           SecurityServiceMode,
     integrity               SecurityServiceMode,
     ...
}

SecurityErrors     ::=  CHOICE
{
     securityWrongSyncTime       NULL,     -- either time server
                                           -- problem or network delay
     securityReplay              NULL,     -- replay attack encountered
     securityWrongGeneralID      NULL,     -- wrong general ID
     securityWrongSendersID      NULL,     -- wrong senders ID
     securityIntegrityFailed     NULL,     -- integrity check failed
     securityWrongOID            NULL,     -- wrong token OIDs or crypto alg
                                             OIDs
     securityDHmismatch          NULL,     -- mismatch of DH parameters
     securityCertificateExpired  NULL,     -- certificate has expired
     securityCertificateDateInvalid   NULL,     -- certificate is not yet valid
     securityCertificateRevoked  NULL,     -- certificate was found revoked
     securityCertificateNotReadable   NULL,     -- decoding error
     securityCertificateSignatureInvalid   NULL,       -- wrong signature in the
                                                       -- certificate
     securityCertificateMissing  NULL,     -- no certificate available
     securityCertificateIncomplete NULL,   -- missing expected certificate
                                           -- extensions
     securityUnsupportedCertificateAlgOID  NULL, -- crypto algs not understood
     securityUnknownCA           NULL,     -- CA/root certificate could not
                                           -- be found
...
}

SecurityErrors2    ::=  CHOICE
{
     securityWrongSyncTime   NULL, -- either time server problem or network
                                   delay
     securityReplay          NULL, -- replay attack encountered
```

```
    securityWrongGeneralID  NULL, -- wrong general ID
    securityWrongSendersID  NULL, -- wrong senders ID
    securityIntegrityFailed NULL, -- integrity check failed
    securityWrongOID        NULL, -- wrong token OIDs or crypto alg OIDs
    ...
}

H245Security ::= CHOICE
{
    nonStandard             NonStandardParameter,
    noSecurity              NULL,
    tls                     SecurityCapabilities,
    ipsec                   SecurityCapabilities,
    ...
}


QseriesOptions ::= SEQUENCE
{
    q932Full       BOOLEAN, -- if true, indicates full support for Q.932
    q951Full       BOOLEAN, -- if true, indicates full support for Q.951
    q952Full       BOOLEAN, -- if true, indicates full support for Q.952
    q953Full       BOOLEAN, -- if true, indicates full support for Q.953
    q955Full       BOOLEAN, -- if true, indicates full support for Q.955
    q956Full       BOOLEAN, -- if true, indicates full support for Q.956
    q957Full       BOOLEAN, -- if true, indicates full support for Q.957
    q954Info       Q954Details,
    ...
}

Q954Details ::= SEQUENCE
{
    conferenceCalling       BOOLEAN,
    threePartyService       BOOLEAN,
    ...
}

GloballyUniqueID        ::= OCTET STRING (SIZE(16))
ConferenceIdentifier    ::= GloballyUniqueID
RequestSeqNum           ::= INTEGER (1..65535)
GatekeeperIdentifier    ::= BMPString (SIZE(1..128))
BandWidth               ::= INTEGER (0..4294967295)   -- in 100s of bits
CallReferenceValue      ::= INTEGER (0..65535)
EndpointIdentifier      ::= BMPString (SIZE(1..128))
ProtocolIdentifier      ::= OBJECT IDENTIFIER
TimeToLive              ::= INTEGER (1..4294967295)   -- in seconds
H248PackagesDescriptor  ::= OCTET STRING  -- This octet string contains ASN.1
                                          -- PER encoded H.248
                                          -- PackagesDescriptor

H248SignalsDescriptor   ::= OCTET STRING  -- This octet string contains
                                          -- ASN.1 PER encoded H.248
                                          -- SignalsDescriptor.

FeatureDescriptor       ::= GenericData

CallIdentifier ::= SEQUENCE
{
    guid           GloballyUniqueID,
    ...
}
```

```
EncryptIntAlg ::= CHOICE
{    -- core encryption algorithms for RAS message integrity
     nonStandard        NonStandardParameter,
     isoAlgorithm       OBJECT IDENTIFIER, -- defined in ISO/IEC 9979
     ...
}
NonIsoIntegrityMechanism ::= CHOICE
{    -- HMAC mechanism used, no truncation, tagging may be necessary!
     hMAC-MD5           NULL,
     hMAC-iso10118-2-s  EncryptIntAlg,     -- according to ISO/IEC 10118-2 using
                                           -- EncryptIntAlg as core block
                                           -- encryption algorithm (short MAC)
     hMAC-iso10118-2-l  EncryptIntAlg,     -- according to ISO/IEC 10118-2 using
                                           -- EncryptIntAlg as core block
                                           -- encryption algorithm (long MAC)
     hMAC-iso10118-3    OBJECT IDENTIFIER, -- according to ISO/IEC 10118-3 using
                                           -- OID as hash function (OID is SHA-1,
                                           -- RIPE-MD160,
                                           -- RIPE-MD128)
     ...
}

IntegrityMechanism ::= CHOICE
{    -- for RAS message integrity
     nonStandard   NonStandardParameter,
     digSig        NULL,              -- indicates to apply a digital signature
     iso9797       OBJECT IDENTIFIER, -- according to ISO/IEC 9797 using OID as
                                      -- core encryption algorithm (X-CBC MAC)
     nonIsoIM      NonIsoIntegrityMechanism,
     ...
}

ICV ::= SEQUENCE
{
     algorithmOID  OBJECT IDENTIFIER,      -- the algorithm used to compute the
                                           -- signature
     icv           BIT STRING              -- the computed cryptographic
                                           -- integrity check value or signature
}

FastStartToken ::= ClearToken (WITH COMPONENTS {..., timeStamp PRESENT, dhkey
PRESENT, generalID PRESENT
                                           -- set to "alias" -- })
EncodedFastStartToken ::= TYPE-IDENTIFIER.&Type (FastStartToken)
CryptoH323Token::= CHOICE
{
     cryptoEPPwdHash SEQUENCE
     {
          alias         AliasAddress,      -- alias of entity generating hash
          timeStamp     TimeStamp,         -- timestamp used in hash
          token         HASHED    { EncodedPwdCertToken -- generalID set to
                                                        -- "alias" -- }
     },
     cryptoGKPwdHash  SEQUENCE
     {
          gatekeeperId  GatekeeperIdentifier,   -- GatekeeperID of GK generating
                                                -- hash
          timeStamp     TimeStamp,              -- timestamp used in hash
          token         HASHED    { EncodedPwdCertToken  -- generalID set to
                                                         -- Gatekeeperid -- }
     },
     cryptoEPPwdEncr    ENCRYPTED { EncodedPwdCertToken -- generalID set to
                                                         -- Gatekeeperid --},
```

```
    cryptoGKPwdEncr     ENCRYPTED { EncodedPwdCertToken -- generalID set to
                                                        -- Gatekeeperid --},
    cryptoEPCert        SIGNED { EncodedPwdCertToken -- generalID set to
                                                    -- Gatekeeperid -- },
    cryptoGKCert        SIGNED { EncodedPwdCertToken -- generalID set to alias -- },
    cryptoFastStart     SIGNED { EncodedFastStartToken },
    nestedcryptoToken   CryptoToken,
    ...
}


DataRate ::= SEQUENCE
{
    nonStandardData         NonStandardParameter OPTIONAL,
    channelRate             BandWidth,
    channelMultiplier       INTEGER (1..256) OPTIONAL,
    ...
}

CallLinkage ::= SEQUENCE
{
    globalCallId            GloballyUniqueID  OPTIONAL,
    threadId                GloballyUniqueID  OPTIONAL,
    ...
}

SupportedPrefix ::= SEQUENCE
{
    nonStandardData         NonStandardParameter OPTIONAL,
    prefix                  AliasAddress,
    ...
}

CapacityReportingCapability ::= SEQUENCE
{
    canReportCallCapacity       BOOLEAN,
    ...
}

CapacityReportingSpecification ::= SEQUENCE
{
    when SEQUENCE
    {
        callStart     NULL OPTIONAL,
        callEnd       NULL OPTIONAL,
        ...
    },
    ...
}

CallCapacity ::= SEQUENCE
{
    maximumCallCapacity         CallCapacityInfo OPTIONAL,
    currentCallCapacity         CallCapacityInfo OPTIONAL,
    ...
}

CallCapacityInfo ::= SEQUENCE
{
    voiceGwCallsAvailable               SEQUENCE OF CallsAvailable OPTIONAL,
    h310GwCallsAvailable                SEQUENCE OF CallsAvailable OPTIONAL,
    h320GwCallsAvailable                SEQUENCE OF CallsAvailable OPTIONAL,
    h321GwCallsAvailable                SEQUENCE OF CallsAvailable OPTIONAL,
    h322GwCallsAvailable                SEQUENCE OF CallsAvailable OPTIONAL,
```

```
    h323GwCallsAvailable                SEQUENCE OF CallsAvailable OPTIONAL,
    h324GwCallsAvailable                SEQUENCE OF CallsAvailable OPTIONAL,
    t120OnlyGwCallsAvailable            SEQUENCE OF CallsAvailable OPTIONAL,
    t38FaxAnnexbOnlyGwCallsAvailable    SEQUENCE OF CallsAvailable OPTIONAL,
    terminalCallsAvailable              SEQUENCE OF CallsAvailable OPTIONAL,
    mcuCallsAvailable                   SEQUENCE OF CallsAvailable OPTIONAL,
    ...,
    sipGwCallsAvailable                 SEQUENCE OF CallsAvailable OPTIONAL
}

CallsAvailable ::= SEQUENCE
{
    calls         INTEGER (0..4294967295),
    group         IA5String (SIZE (1..128)) OPTIONAL,
    ...,
    carrier       CarrierInfo OPTIONAL
}

CircuitInfo ::= SEQUENCE
{
    sourceCircuitID             CircuitIdentifier OPTIONAL,
    destinationCircuitID        CircuitIdentifier OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL,
    ...
}

CircuitIdentifier ::= SEQUENCE
{
    cic           CicInfo OPTIONAL,  group     GroupID OPTIONAL,
    ...,
    carrier       CarrierInfo OPTIONAL
}

CicInfo ::= SEQUENCE
{
    cic           SEQUENCE OF OCTET STRING (SIZE (2..4)),
    pointCode     OCTET STRING (SIZE (2..5)),
    ...
}

GroupID ::= SEQUENCE
{
    member        SEQUENCE OF INTEGER (0..65535) OPTIONAL,
    group         IA5String (SIZE (1..128)),
    ...
}

CarrierInfo ::= SEQUENCE
{
    carrierIdentificationCode   OCTET STRING (SIZE (3..4)) OPTIONAL,
    carrierName                 IA5String (SIZE (1..128)) OPTIONAL,
    ...
}

ServiceControlDescriptor ::= CHOICE
{
    url                         IA5String (SIZE(0..512)),  -- indicates a URL-
                                                           -- referenced
                                                           -- protocol/resource
    signal                      H248SignalsDescriptor,
    nonStandard                 NonStandardParameter,
    callCreditServiceControl    CallCreditServiceControl,
    ...
}
```

```
ServiceControlSession ::= SEQUENCE
{
     sessionId      INTEGER (0..255),
     contents       ServiceControlDescriptor OPTIONAL,
     reason CHOICE
     {
          open           NULL,
          refresh        NULL,
          close          NULL,
          ...
     },
     ...
}

RasUsageInfoTypes ::= SEQUENCE
{
     nonStandardUsageTypes        SEQUENCE OF NonStandardParameter,
     startTime                    NULL OPTIONAL,
     endTime                      NULL OPTIONAL,
     terminationCause             NULL OPTIONAL,
     ...
}

RasUsageSpecification ::= SEQUENCE
{
     when SEQUENCE
     {
          start                   NULL OPTIONAL,
          end                     NULL OPTIONAL,
          inIrr                   NULL OPTIONAL,
          ...
     },
     callStartingPoint SEQUENCE
     {
          alerting           NULL OPTIONAL,
          connect            NULL OPTIONAL,
          ...
     } OPTIONAL,
     required                RasUsageInfoTypes,
     ...
}

RasUsageInformation ::= SEQUENCE
{
     nonStandardUsageFields       SEQUENCE OF NonStandardParameter,
     alertingTime                 TimeStamp OPTIONAL,
     connectTime                  TimeStamp OPTIONAL,
     endTime                      TimeStamp OPTIONAL,
     ...
}

CallTerminationCause ::= CHOICE
{
     releaseCompleteReason        ReleaseCompleteReason,
     releaseCompleteCauseIE       OCTET STRING (SIZE(2..32)),
     ...
}
```

```
BandwidthDetails ::= SEQUENCE
{
     sender              BOOLEAN,               -- TRUE=sender, FALSE=receiver
     multicast           BOOLEAN,               -- TRUE if stream is multicast
     bandwidth           BandWidth,             -- Bandwidth used for stream
     rtcpAddresses       TransportChannelInfo,  -- RTCP addresses for media stream
     ...
}

CallCreditCapability ::= SEQUENCE
{
     canDisplayAmountString       BOOLEAN OPTIONAL,
     canEnforceDurationLimit      BOOLEAN OPTIONAL,
     ...
}

CallCreditServiceControl ::= SEQUENCE
{
     amountString            BMPString (SIZE (1..512)) OPTIONAL,   -- (Unicode)
     billingMode CHOICE
     {
          credit             NULL,
          debit              NULL,
          ...
     } OPTIONAL,
     callDurationLimit       INTEGER (1..4294967295) OPTIONAL,    -- in seconds
     enforceCallDurationLimit    BOOLEAN OPTIONAL,
     callStartingPoint CHOICE
     {
          alerting           NULL,
          connect            NULL,
          ...
     } OPTIONAL,
     ...
}

GenericData ::= SEQUENCE
{
     id                  GenericIdentifier,
     parameters          SEQUENCE (SIZE (1..512)) OF EnumeratedParameter
OPTIONAL,
     ...
}

GenericIdentifier ::= CHOICE
{
     standard            INTEGER(0..16383,...),
     oid                 OBJECT IDENTIFIER,
     nonStandard         GloballyUniqueID,
     ...
}

EnumeratedParameter ::= SEQUENCE
{
     id                  GenericIdentifier,
     content             Content OPTIONAL,
     ...
}

Content ::= CHOICE
{
     raw                 OCTET STRING,
     text                IA5String,
     unicode             BMPString,
```

```
    bool                BOOLEAN,
    number8             INTEGER (0..255),
    number16            INTEGER (0..65535),
    number32            INTEGER (0..4294967295),
    id                  GenericIdentifier,
    alias               AliasAddress,
    transport           TransportAddress,
    compound            SEQUENCE (SIZE (1..512)) OF EnumeratedParameter,
    nested              SEQUENCE (SIZE (1..16)) OF GenericData,
    ...
}

FeatureSet ::= SEQUENCE
{
    replacementFeatureSet   BOOLEAN,
    neededFeatures          SEQUENCE OF FeatureDescriptor OPTIONAL,
    desiredFeatures         SEQUENCE OF FeatureDescriptor OPTIONAL,
    supportedFeatures       SEQUENCE OF FeatureDescriptor OPTIONAL,
    ...
}

TransportChannelInfo ::= SEQUENCE
{
    sendAddress             TransportAddress OPTIONAL,
    recvAddress             TransportAddress OPTIONAL,
    ...
}

RTPSession ::= SEQUENCE
{
    rtpAddress                  TransportChannelInfo,
    rtcpAddress                 TransportChannelInfo,
    cname                       PrintableString,
    ssrc                        INTEGER (1..4294967295),
    sessionId                   INTEGER (1..255),
    associatedSessionIds        SEQUENCE OF INTEGER (1..255),
    ...,
    multicast                   NULL OPTIONAL,
    bandwidth                   BandWidth OPTIONAL
}

RasMessage ::= CHOICE
{
    gatekeeperRequest           GatekeeperRequest,
    gatekeeperConfirm           GatekeeperConfirm,
    gatekeeperReject            GatekeeperReject,
    registrationRequest         RegistrationRequest,
    registrationConfirm         RegistrationConfirm,
    registrationReject          RegistrationReject,
    unregistrationRequest       UnregistrationRequest,
    unregistrationConfirm       UnregistrationConfirm,
    unregistrationReject        UnregistrationReject,
    admissionRequest            AdmissionRequest,
    admissionConfirm            AdmissionConfirm,
    admissionReject             AdmissionReject,
    bandwidthRequest            BandwidthRequest,
    bandwidthConfirm            BandwidthConfirm,
    bandwidthReject             BandwidthReject,
    disengageRequest            DisengageRequest,
    disengageConfirm            DisengageConfirm,
    disengageReject             DisengageReject,
    locationRequest             LocationRequest,
    locationConfirm             LocationConfirm,
    locationReject              LocationReject,
```

```
     infoRequest                  InfoRequest,
     infoRequestResponse          InfoRequestResponse,
     nonStandardMessage           NonStandardMessage,
     unknownMessageResponse       UnknownMessageResponse,
     ...,
     requestInProgress            RequestInProgress,
     resourcesAvailableIndicate   ResourcesAvailableIndicate,
     resourcesAvailableConfirm    ResourcesAvailableConfirm,
     infoRequestAck               InfoRequestAck,
     infoRequestNak               InfoRequestNak,
     serviceControlIndication     ServiceControlIndication,
     serviceControlResponse       ServiceControlResponse,
     admissionConfirmSequence     SEQUENCE OF AdmissionConfirm
}

GatekeeperRequest ::= SEQUENCE --(GRQ)
{

     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,
     genericData                  SEQUENCE OF GenericData OPTIONAL
}

GatekeeperConfirm ::= SEQUENCE --(GCF)
{
     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
}

GatekeeperReject ::= SEQUENCE --(GRJ)
{
     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,     -- permission failure, not a resource
                                          -- failure
    invalidRevision             NULL,
    undefinedReason             NULL,
    ...,
    securityDenial              NULL,
    genericDataReason           NULL,
    neededFeatureNotSupported   NULL,
    securityError               SecurityErrors}

RegistrationRequest ::= SEQUENCE --(RRQ)
{
    requestSeqNum               RequestSeqNum,
    protocolIdentifier          ProtocolIdentifier,
    nonStandardData             NonStandardParameter OPTIONAL,
    discoveryComplete           BOOLEAN,
    callSignalAddress           SEQUENCE OF TransportAddress,
    rasAddress                  SEQUENCE OF TransportAddress,
    terminalType                EndpointType,
    terminalAlias               SEQUENCE OF AliasAddress OPTIONAL,
    gatekeeperIdentifier        GatekeeperIdentifier  OPTIONAL,
    endpointVendor              VendorIdentifier,
    ...,
    alternateEndpoints          SEQUENCE OF Endpoint OPTIONAL,
    timeToLive                  TimeToLive OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue         ICV OPTIONAL,
    keepAlive                   BOOLEAN,
    endpointIdentifier          EndpointIdentifier OPTIONAL,
    willSupplyUUIEs             BOOLEAN,
    maintainConnection          BOOLEAN,
    alternateTransportAddresses AlternateTransportAddresses OPTIONAL,
    additiveRegistration        NULL OPTIONAL,
    terminalAliasPattern        SEQUENCE OF AddressPattern OPTIONAL,
    supportsAltGK               NULL OPTIONAL,
    usageReportingCapability    RasUsageInfoTypes OPTIONAL,
    multipleCalls               BOOLEAN OPTIONAL,
    supportedH248Packages       SEQUENCE OF H248PackagesDescriptor OPTIONAL,
    callCreditCapability        CallCreditCapability OPTIONAL,
    capacityReportingCapability CapacityReportingCapability OPTIONAL,
    capacity                    CallCapacity OPTIONAL,
    featureSet                  FeatureSet OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL,
    restart                     NULL     OPTIONAL,
    supportsACFSequences        NULL     OPTIONAL
}
```

```
RegistrationConfirm ::= SEQUENCE --(RCF)
{
     requestSeqNum                          RequestSeqNum,
     protocolIdentifier                     ProtocolIdentifier,
     nonStandardData                        NonStandardParameter OPTIONAL,
     callSignalAddress                      SEQUENCE OF TransportAddress,
     terminalAlias                          SEQUENCE OF AliasAddress OPTIONAL,
     gatekeeperIdentifier                   GatekeeperIdentifier  OPTIONAL,
     endpointIdentifier                     EndpointIdentifier,
     ...,
     alternateGatekeeper                    SEQUENCE OF AlternateGK OPTIONAL,
     timeToLive                             TimeToLive OPTIONAL,
     tokens                                 SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                           SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue                    ICV OPTIONAL,
     willRespondToIRR                       BOOLEAN,
     preGrantedARQ                          SEQUENCE
     {
          makeCall                          BOOLEAN,
          useGKCallSignalAddressToMakeCall  BOOLEAN,
          answerCall                        BOOLEAN,
          useGKCallSignalAddressToAnswer    BOOLEAN,
          ...,
          irrFrequencyInCall      INTEGER (1..65535) OPTIONAL, -- in seconds;
                                                               -- not present
                                                               -- if GK does
                                                               -- not want IRRs
          totalBandwidthRestriction   BandWidth OPTIONAL,      -- total limit
                                                               -- for all
                                                               -- concurrent
                                                                  calls
          alternateTransportAddresses      AlternateTransportAddresses OPTIONAL,
          useSpecifiedTransport            UseSpecifiedTransport OPTIONAL
     } OPTIONAL,
     maintainConnection                BOOLEAN,
     serviceControl                    SEQUENCE OF ServiceControlSession
OPTIONAL,
     supportsAdditiveRegistration      NULL OPTIONAL,
     terminalAliasPattern              SEQUENCE OF AddressPattern OPTIONAL,
     supportedPrefixes                 SEQUENCE OF SupportedPrefix OPTIONAL,
     usageSpec                         SEQUENCE OF RasUsageSpecification
OPTIONAL,
     featureServerAlias                AliasAddress OPTIONAL,
     capacityReportingSpec             CapacityReportingSpecification OPTIONAL,
     featureSet                        FeatureSet OPTIONAL,
     genericData                       SEQUENCE OF GenericData OPTIONAL
}

RegistrationReject ::= SEQUENCE --(RRJ)
{
     requestSeqNum                RequestSeqNum,
     protocolIdentifier           ProtocolIdentifier,
     nonStandardData              NonStandardParameter OPTIONAL,
     rejectReason                 RegistrationRejectReason,
     gatekeeperIdentifier         GatekeeperIdentifier  OPTIONAL,
     ...,
     altGKInfo                    AltGKInfo OPTIONAL,
     tokens                       SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                 SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue          ICV OPTIONAL,
     featureSet                   FeatureSet OPTIONAL,
     genericData                  SEQUENCE OF GenericData OPTIONAL
}
```

```
RegistrationRejectReason ::= CHOICE
{
     discoveryRequired            NULL,
     invalidRevision              NULL,
     invalidCallSignalAddress     NULL,
     invalidRASAddress            NULL,     -- supplied address is invalid
     duplicateAlias               SEQUENCE OF AliasAddress,
                                            -- alias registered to another
                                            -- endpoint
     invalidTerminalType          NULL,
     undefinedReason              NULL,
     transportNotSupported        NULL,     -- one or more of the transports
     ...,
     transportQOSNotSupported     NULL,     -- endpoint QoS not supported
     resourceUnavailable          NULL,     -- gatekeeper resources exhausted
     invalidAlias                 NULL,     -- alias not consistent with
                                            -- gatekeeper rules
     securityDenial               NULL,
     fullRegistrationRequired     NULL,     -- registration permission has
                                               expired
     additiveRegistrationNotSupported NULL,
     invalidTerminalAliases           SEQUENCE
     {
          terminalAlias           SEQUENCE OF AliasAddress OPTIONAL,
          terminalAliasPattern    SEQUENCE OF AddressPattern OPTIONAL,
          supportedPrefixes       SEQUENCE OF SupportedPrefix OPTIONAL,
          ...
     },
     genericDataReason            NULL,
     neededFeatureNotSupported    NULL,
     securityError                SecurityErrors
}

UnregistrationRequest ::= SEQUENCE --(URQ)
{
     requestSeqNum           RequestSeqNum,
     callSignalAddress       SEQUENCE OF TransportAddress,
     endpointAlias           SEQUENCE OF AliasAddress OPTIONAL,
     nonStandardData         NonStandardParameter OPTIONAL,
     endpointIdentifier      EndpointIdentifier OPTIONAL,
     ...,
     alternateEndpoints      SEQUENCE OF Endpoint OPTIONAL,
     gatekeeperIdentifier    GatekeeperIdentifier OPTIONAL,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     reason                  UnregRequestReason OPTIONAL,
     endpointAliasPattern    SEQUENCE OF AddressPattern OPTIONAL,
     supportedPrefixes       SEQUENCE OF SupportedPrefix OPTIONAL,
     alternateGatekeeper     SEQUENCE OF AlternateGK OPTIONAL,
     genericData             SEQUENCE OF GenericData OPTIONAL
}

UnregRequestReason ::= CHOICE
{
     reregistrationRequired  NULL,
     ttlExpired              NULL,
     securityDenial          NULL,
     undefinedReason         NULL,
     ...,
     maintenance             NULL,
     securityError           SecurityErrors2
}
```

```
UnregistrationConfirm ::= SEQUENCE --(UCF)
{
     requestSeqNum           RequestSeqNum,
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     genericData             SEQUENCE OF GenericData OPTIONAL
}

UnregistrationReject ::= SEQUENCE --(URJ)
{

     requestSeqNum           RequestSeqNum,
     rejectReason            UnregRejectReason,
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     altGKInfo               AltGKInfo OPTIONAL,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     genericData             SEQUENCE OF GenericData OPTIONAL
}

UnregRejectReason ::= CHOICE
{
     notCurrentlyRegistered  NULL,
     callInProgress          NULL,
     undefinedReason         NULL,
     ...,
     permissionDenied        NULL,     -- requesting user not allowed to
                                       -- unregister specified user
     securityDenial          NULL,
     securityError           SecurityErrors2
}

AdmissionRequest ::= SEQUENCE --(ARQ)
{
     requestSeqNum               RequestSeqNum,
     callType                    CallType,
     callModel                   CallModel OPTIONAL,
     endpointIdentifier          EndpointIdentifier,
     destinationInfo             SEQUENCE OF AliasAddress OPTIONAL,
     destCallSignalAddress       TransportAddress OPTIONAL,
     destExtraCallInfo           SEQUENCE OF AliasAddress OPTIONAL,
     srcInfo                     SEQUENCE OF AliasAddress,
     srcCallSignalAddress        TransportAddress OPTIONAL,
     bandWidth                   BandWidth,
     callReferenceValue          CallReferenceValue,
     nonStandardData             NonStandardParameter OPTIONAL,
     callServices                QseriesOptions  OPTIONAL,
     conferenceID                ConferenceIdentifier,
     activeMC                    BOOLEAN,
     answerCall                  BOOLEAN,  -- answering a call
     ...,
     canMapAlias                 BOOLEAN,  -- can handle alias address
     callIdentifier              CallIdentifier,
     srcAlternatives             SEQUENCE OF Endpoint OPTIONAL,
     destAlternatives            SEQUENCE OF Endpoint OPTIONAL,
     gatekeeperIdentifier        GatekeeperIdentifier OPTIONAL,
     tokens                      SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue         ICV OPTIONAL,
```

```
    transportQOS                TransportQOS OPTIONAL,
    willSupplyUUIEs             BOOLEAN,
    callLinkage                 CallLinkage OPTIONAL,
    gatewayDataRate             DataRate OPTIONAL,
    capacity                    CallCapacity OPTIONAL,
    circuitInfo                 CircuitInfo OPTIONAL,
    desiredProtocols            SEQUENCE OF SupportedProtocols OPTIONAL,
    desiredTunnelledProtocol    TunnelledProtocol OPTIONAL,
    featureSet                  FeatureSet OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL,
    canMapSrcAlias              BOOLEAN
}

CallType ::= CHOICE
{
    pointToPoint       NULL,          -- Point-to-point
    oneToN             NULL,          -- no interaction (FFS)
    nToOne             NULL,          -- no interaction (FFS)
    nToN               NULL,          -- interactive (multipoint)
    ...
}

CallModel ::= CHOICE
{
    direct             NULL,
    gatekeeperRouted   NULL,
    ...
}

TransportQOS ::= CHOICE
{
    endpointControlled      NULL,
    gatekeeperControlled    NULL,
    noControl               NULL,
    ...
}

AdmissionConfirm ::= SEQUENCE --(ACF)
{
    requestSeqNum               RequestSeqNum,
    bandWidth                   BandWidth,
    callModel                   CallModel,
    destCallSignalAddress       TransportAddress,
    irrFrequency                INTEGER (1..65535) OPTIONAL,
    nonStandardData             NonStandardParameter OPTIONAL,
    ...,
    destinationInfo             SEQUENCE OF AliasAddress OPTIONAL,
    destExtraCallInfo           SEQUENCE OF AliasAddress OPTIONAL,
    destinationType             EndpointType OPTIONAL,
    remoteExtensionAddress      SEQUENCE OF AliasAddress OPTIONAL,
    alternateEndpoints          SEQUENCE OF Endpoint OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue         ICV OPTIONAL,
    transportQOS                TransportQOS OPTIONAL,
    willRespondToIRR            BOOLEAN,
    uuiesRequested              UUIEsRequested,
    language                    SEQUENCE OF IA5String (SIZE (1..32)) OPTIONAL,
    alternateTransportAddresses AlternateTransportAddresses OPTIONAL,
    useSpecifiedTransport       UseSpecifiedTransport OPTIONAL,
    circuitInfo                 CircuitInfo OPTIONAL,
    usageSpec                   SEQUENCE OF RasUsageSpecification OPTIONAL,
    supportedProtocols          SEQUENCE OF SupportedProtocols OPTIONAL,
    serviceControl              SEQUENCE OF ServiceControlSession OPTIONAL,
```

```
    multipleCalls               BOOLEAN OPTIONAL,
    featureSet                  FeatureSet OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL,
    modifiedSrcInfo             SEQUENCE OF AliasAddress OPTIONAL
}

UUIEsRequested ::= SEQUENCE
{
    setup                   BOOLEAN,
    callProceeding          BOOLEAN,
    connect                 BOOLEAN,
    alerting                BOOLEAN,
    information             BOOLEAN,
    releaseComplete         BOOLEAN,
    facility                BOOLEAN,
    progress                BOOLEAN,
    empty                   BOOLEAN,
    ...,
    status                  BOOLEAN,
    statusInquiry           BOOLEAN,
    setupAcknowledge        BOOLEAN,
    notify                  BOOLEAN
}

AdmissionReject ::= SEQUENCE --(ARJ)
{
    requestSeqNum           RequestSeqNum,
    rejectReason            AdmissionRejectReason,
    nonStandardData         NonStandardParameter OPTIONAL,
    ...,
    altGKInfo               AltGKInfo OPTIONAL,
    tokens                  SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
    callSignalAddress       SEQUENCE OF TransportAddress OPTIONAL,
    integrityCheckValue     ICV OPTIONAL,
    serviceControl          SEQUENCE OF ServiceControlSession OPTIONAL,
    featureSet              FeatureSet OPTIONAL,
    genericData             SEQUENCE OF GenericData OPTIONAL
}

AdmissionRejectReason ::= CHOICE
{
    calledPartyNotRegistered    NULL,     -- cannot translate address
    invalidPermission           NULL,     -- permission has expired
    requestDenied               NULL,     -- no bandwidth available
    undefinedReason             NULL,
    callerNotRegistered         NULL,
    routeCallToGatekeeper       NULL,
    invalidEndpointIdentifier   NULL,
    resourceUnavailable         NULL,
    ...,
    securityDenial              NULL,
    qosControlNotSupported      NULL,
    incompleteAddress           NULL,
    aliasesInconsistent         NULL,     -- multiple aliases in request
                                          -- identify distinct people
    routeCallToSCN              SEQUENCE OF PartyNumber,
    exceedsCallCapacity         NULL,     -- destination does not have the
                                          -- capacity for this call
    collectDestination          NULL,
    collectPIN                  NULL,
    genericDataReason           NULL,
    neededFeatureNotSupported   NULL,
    securityError               SecurityErrors2,
```

```
    securityDHmismatch          NULL,     -- mismatch of DH parameters
    noRouteToDestination        NULL,     -- destination unreachable
    unallocatedNumber           NULL      -- destination number unassigned
}

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
}

BandwidthConfirm ::= SEQUENCE --(BCF)
{
    requestSeqNum               RequestSeqNum,
    bandWidth                   BandWidth,
    nonStandardData             NonStandardParameter OPTIONAL,
    ...,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue         ICV OPTIONAL,
    capacity                    CallCapacity OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL
}

BandwidthReject ::= SEQUENCE --(BRJ)
{
    requestSeqNum               RequestSeqNum,
    rejectReason                BandRejectReason,
    allowedBandWidth            BandWidth,
    nonStandardData             NonStandardParameter OPTIONAL,
    ...,
    altGKInfo                   AltGKInfo OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue         ICV OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL
}

BandRejectReason ::= CHOICE
{
    notBound                    NULL,     -- discovery permission has aged
    invalidConferenceID         NULL,     -- possible revision
    invalidPermission           NULL,     -- true permission violation
    insufficientResources       NULL,
    invalidRevision             NULL,
    undefinedReason             NULL,
    ...,
```

```
     securityDenial              NULL,
     securityError               SecurityErrors2}

LocationRequest ::= SEQUENCE --(LRQ)
{
     requestSeqNum               RequestSeqNum,
     endpointIdentifier          EndpointIdentifier OPTIONAL,
     destinationInfo             SEQUENCE OF AliasAddress,
     nonStandardData             NonStandardParameter OPTIONAL,
     replyAddress                TransportAddress,
     ...,
     sourceInfo                  SEQUENCE OF AliasAddress OPTIONAL,
     canMapAlias                 BOOLEAN, -- can handle alias address
     gatekeeperIdentifier        GatekeeperIdentifier OPTIONAL,
     tokens                      SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue         ICV OPTIONAL,
     desiredProtocols            SEQUENCE OF SupportedProtocols OPTIONAL,
     desiredTunnelledProtocol    TunnelledProtocol OPTIONAL,
     featureSet                  FeatureSet OPTIONAL,
     genericData                 SEQUENCE OF GenericData OPTIONAL,
     hopCount                    INTEGER (1..255) OPTIONAL,
     circuitInfo                 CircuitInfo OPTIONAL,
     callIdentifier              CallIdentifier OPTIONAL,
     bandWidth                   BandWidth OPTIONAL,
     sourceEndpointInfo          SEQUENCE OF AliasAddress OPTIONAL,
     canMapSrcAlias              BOOLEAN
}

LocationConfirm ::= SEQUENCE --(LCF)
{
     requestSeqNum               RequestSeqNum,
     callSignalAddress           TransportAddress,
     rasAddress                  TransportAddress,
     nonStandardData             NonStandardParameter OPTIONAL,
     ...,
     destinationInfo             SEQUENCE OF AliasAddress OPTIONAL,
     destExtraCallInfo           SEQUENCE OF AliasAddress OPTIONAL,
     destinationType             EndpointType OPTIONAL,
     remoteExtensionAddress      SEQUENCE OF AliasAddress OPTIONAL,
     alternateEndpoints          SEQUENCE OF Endpoint OPTIONAL,
     tokens                      SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue         ICV OPTIONAL,
     alternateTransportAddresses AlternateTransportAddresses OPTIONAL,
     supportedProtocols          SEQUENCE OF SupportedProtocols OPTIONAL,
     multipleCalls               BOOLEAN OPTIONAL,
     featureSet                  FeatureSet OPTIONAL,
     genericData                 SEQUENCE OF GenericData OPTIONAL,
     circuitInfo                 CircuitInfo OPTIONAL,
     serviceControl              SEQUENCE OF ServiceControlSession OPTIONAL,
     modifiedSrcInfo             SEQUENCE OF AliasAddress OPTIONAL,
     bandWidth                   BandWidth OPTIONAL
}

LocationReject ::= SEQUENCE --(LRJ)
{
     requestSeqNum          RequestSeqNum,
     rejectReason           LocationRejectReason,
     nonStandardData        NonStandardParameter OPTIONAL,
     ...,
     altGKInfo              AltGKInfo OPTIONAL,
     tokens                 SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens           SEQUENCE OF CryptoH323Token OPTIONAL,
```

```
    integrityCheckValue     ICV OPTIONAL,
    featureSet              FeatureSet OPTIONAL,
    genericData             SEQUENCE OF GenericData OPTIONAL,
    serviceControl          SEQUENCE OF ServiceControlSession OPTIONAL
}

LocationRejectReason ::= CHOICE
{
    notRegistered           NULL,
    invalidPermission       NULL,     -- exclusion by administrator or feature
    requestDenied           NULL,     -- cannot find location
    undefinedReason         NULL,
    ...,
    securityDenial              NULL,
    aliasesInconsistent         NULL,     -- multiple aliases in request
                                          -- identify distinct people
    routeCalltoSCN              SEQUENCE OF PartyNumber,
    resourceUnavailable         NULL,
    genericDataReason           NULL,
    neededFeatureNotSupported   NULL,
    hopCountExceeded            NULL,
    incompleteAddress           NULL,
    securityError               SecurityErrors2,
    securityDHmismatch          NULL,     -- mismatch of DH parameters
    noRouteToDestination        NULL,     -- destination unreachable
    unallocatedNumber           NULL      -- destination number unassigned
}

DisengageRequest ::= SEQUENCE --(DRQ)
{
    requestSeqNum           RequestSeqNum,
    endpointIdentifier      EndpointIdentifier,
    conferenceID            ConferenceIdentifier,
    callReferenceValue      CallReferenceValue,
    disengageReason         DisengageReason,
    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,
    circuitInfo             CircuitInfo OPTIONAL,
    usageInformation        RasUsageInformation OPTIONAL,
    terminationCause        CallTerminationCause OPTIONAL,
    serviceControl          SEQUENCE OF ServiceControlSession OPTIONAL,
    genericData             SEQUENCE OF GenericData OPTIONAL
}

DisengageReason ::= CHOICE
{
    forcedDrop              NULL,     -- gatekeeper is forcing the drop
    normalDrop              NULL,     -- associated with normal drop
    undefinedReason         NULL,
    ...
}
```

```
DisengageConfirm ::= SEQUENCE --(DCF)
{
     requestSeqNum           RequestSeqNum,
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     capacity                CallCapacity OPTIONAL,
     circuitInfo             CircuitInfo OPTIONAL,
     usageInformation        RasUsageInformation OPTIONAL,
     genericData             SEQUENCE OF GenericData OPTIONAL
}

DisengageReject ::= SEQUENCE --(DRJ)
{
     requestSeqNum           RequestSeqNum,
     rejectReason            DisengageRejectReason,
     nonStandardData         NonStandardParameter OPTIONAL,
     ...,
     altGKInfo               AltGKInfo OPTIONAL,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     genericData             SEQUENCE OF GenericData OPTIONAL
}

DisengageRejectReason ::= CHOICE
{
     notRegistered           NULL,     -- not registered with gatekeeper
     requestToDropOther      NULL,     -- cannot request drop for others
     ...,
     securityDenial          NULL,
     securityError           SecurityErrors2
}

InfoRequest ::= SEQUENCE --(IRQ)
{
     requestSeqNum           RequestSeqNum,
     callReferenceValue      CallReferenceValue,
     nonStandardData         NonStandardParameter OPTIONAL,
     replyAddress            TransportAddress OPTIONAL,
     ...,
     callIdentifier          CallIdentifier,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     uuiesRequested          UUIEsRequested OPTIONAL,
     callLinkage             CallLinkage OPTIONAL,
     usageInfoRequested           RasUsageInfoTypes OPTIONAL,
     segmentedResponseSupported  NULL OPTIONAL,
     nextSegmentRequested         INTEGER (0..65535) OPTIONAL,
     capacityInfoRequested        NULL OPTIONAL,
     genericData                  SEQUENCE OF GenericData OPTIONAL
}

InfoRequestResponse ::= SEQUENCE --(IRR)
{

     nonStandardData         NonStandardParameter OPTIONAL,
     requestSeqNum           RequestSeqNum,
     endpointType            EndpointType,
     endpointIdentifier      EndpointIdentifier,
     rasAddress              TransportAddress,
```

```
    callSignalAddress       SEQUENCE OF TransportAddress,
    endpointAlias           SEQUENCE OF AliasAddress OPTIONAL,
    perCallInfo             SEQUENCE OF SEQUENCE
    {
        nonStandardData         NonStandardParameter OPTIONAL,
        callReferenceValue      CallReferenceValue,
        conferenceID            ConferenceIdentifier,
        originator              BOOLEAN OPTIONAL,
        audio                   SEQUENCE OF RTPSession OPTIONAL,
        video                   SEQUENCE OF RTPSession OPTIONAL,
        data                    SEQUENCE OF TransportChannelInfo OPTIONAL,
        h245                    TransportChannelInfo,
        callSignalling          TransportChannelInfo,
        callType                CallType,
        bandWidth               BandWidth,
        callModel               CallModel,
        ...,
        callIdentifier          CallIdentifier,
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        substituteConfIDs       SEQUENCE OF ConferenceIdentifier,
        pdu                     SEQUENCE OF SEQUENCE
        {
            h323pdu       H323-UU-PDU,
            sent      BOOLEAN       -- TRUE is sent, FALSE is received
        } OPTIONAL,
        callLinkage             CallLinkage OPTIONAL,
        usageInformation        RasUsageInformation OPTIONAL,
        circuitInfo             CircuitInfo OPTIONAL
    } OPTIONAL,
    ...,
    tokens                  SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue     ICV OPTIONAL,
    needResponse            BOOLEAN,
    capacity                CallCapacity OPTIONAL,
    irrStatus               InfoRequestResponseStatus OPTIONAL,
    unsolicited             BOOLEAN,
    genericData             SEQUENCE OF GenericData OPTIONAL
}

InfoRequestResponseStatus ::= CHOICE
{
    complete            NULL,
    incomplete          NULL,
    segment             INTEGER (0..65535),
    invalidCall         NULL,
    ...
}

InfoRequestAck ::= SEQUENCE --(IACK)
{
    requestSeqNum               RequestSeqNum,
    nonStandardData             NonStandardParameter OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue         ICV OPTIONAL,
    ...
}
```

```
InfoRequestNak ::= SEQUENCE --(INAK)
{
     requestSeqNum               RequestSeqNum,
     nonStandardData             NonStandardParameter OPTIONAL,
     nakReason                   InfoRequestNakReason,
     altGKInfo                   AltGKInfo OPTIONAL,
     tokens                      SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue         ICV OPTIONAL,
     ...
}

InfoRequestNakReason ::= CHOICE
{
     notRegistered      NULL,     -- not registered with gatekeeper
     securityDenial     NULL,
     undefinedReason    NULL,
     ...,
     securityError      SecurityErrors2

}

NonStandardMessage ::= SEQUENCE
{
     requestSeqNum           RequestSeqNum,
     nonStandardData         NonStandardParameter,
     ...,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     featureSet              FeatureSet OPTIONAL,
     genericData             SEQUENCE OF GenericData OPTIONAL
}

UnknownMessageResponse ::= SEQUENCE   -- (XRS)
{
     requestSeqNum           RequestSeqNum,
     ...,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     messageNotUnderstood    OCTET STRING
}

RequestInProgress ::= SEQUENCE        -- (RIP)
{
     requestSeqNum           RequestSeqNum,
     nonStandardData         NonStandardParameter      OPTIONAL,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
     integrityCheckValue     ICV OPTIONAL,
     delay                   INTEGER(1..65535),
     ...
}

ResourcesAvailableIndicate ::= SEQUENCE --(RAI)
{
     requestSeqNum           RequestSeqNum,
     protocolIdentifier      ProtocolIdentifier,
     nonStandardData         NonStandardParameter OPTIONAL,
     endpointIdentifier      EndpointIdentifier,
     protocols               SEQUENCE OF SupportedProtocols,
     almostOutOfResources    BOOLEAN,
     tokens                  SEQUENCE OF ClearToken OPTIONAL,
```

```
    cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue     ICV OPTIONAL,
    ...,
    capacity                CallCapacity OPTIONAL,
    genericData             SEQUENCE OF GenericData OPTIONAL
}

ResourcesAvailableConfirm ::= SEQUENCE --(RAC)
{
    requestSeqNum           RequestSeqNum,
    protocolIdentifier      ProtocolIdentifier,
    nonStandardData         NonStandardParameter OPTIONAL,
    tokens                  SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue     ICV OPTIONAL,
    ...,
    genericData             SEQUENCE OF GenericData OPTIONAL
}

ServiceControlIndication ::= SEQUENCE --(SCI)
{
    requestSeqNum           RequestSeqNum,
    nonStandardData         NonStandardParameter OPTIONAL,
    serviceControl          SEQUENCE OF ServiceControlSession,
    endpointIdentifier      EndpointIdentifier OPTIONAL,
    callSpecific SEQUENCE
    {
        callIdentifier      CallIdentifier,
        conferenceID        ConferenceIdentifier,
        answeredCall        BOOLEAN,
        ...
    } OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue         ICV OPTIONAL,
    featureSet                  FeatureSet OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL,
    ...
}

ServiceControlResponse ::= SEQUENCE --(SCR)
{
    requestSeqNum                   RequestSeqNum,
    result                          CHOICE
    {
        started                     NULL,
        failed                      NULL,
        stopped                     NULL,
        notAvailable                NULL,
        neededFeatureNotSupported   NULL,
        ...
    } OPTIONAL,
    nonStandardData             NonStandardParameter OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue         ICV OPTIONAL,
    featureSet                  FeatureSet OPTIONAL,
    genericData                 SEQUENCE OF GenericData OPTIONAL,
    ...
}


END     -- of ASN.1
```

Anexo I

Paquetización de vídeo H.263+

En IETF RFC 2429 se especifica un formato de cabida útil del RTP para trenes de bits de vídeo H.263 que contienen las nuevas características "H.263+" adoptadas en la versión 2 (1998) de la Rec. UIT-T H.263 (que incluye las características que utilizan PLUSTYPE o el anexo I/H.263 a anexo T/H.263).

Es necesario que los trenes de bits H.263 que no utilizan las nuevas características de la versión 2 de la Rec. UIT-T H.263 tengan la capacidad de soportar el formato de cabida útil H.263 de la norma RFC 2190 como se especifica en el anexo E, por razones de compatibilidad con implementaciones previas. Sin embargo, el nuevo formato de cabida útil especificado en RFC 2429 debiera utilizarse aún para trenes de bits que no contienen las nuevas características de la versión 2 siempre que el formato de cabida útil más nuevo posea las capacidades de los terminales de recepción.

Apéndice I

RTP/RTCP

El material informativo a que se hace referencia puede encontrarse en:

– SCHULZRINNE (H.), CASNER (S.), FREDERICK (R.) and JACOBSON (V.): RFC 3550, RTP: A Transport Protocol for Real-Time Applications, *Internet Engineering Task Force*, 2003.

Apéndice II

Perfil RTP

El material informativo a que se hace referencia figura en:

– SCHULZRINNE (H.) CASNER (S.): RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control, *Internet Engineering Task Force*, 2003.

Apéndice III

Paquetización H.261

El material informativo a que se hace referencia figura en:

– TURLETTI (T.), HUITEMA (C.): RFC 2032, RTP Payload Format for H.261 Video Streams, *Internet Engineering Task Force*, 1996.

Apéndice IV

Funcionamiento de H.225.0 en distintas pilas de protocolos de la red de paquetes

En este apéndice figuran detalles adicionales relativos al funcionamiento de H.225.0 en distintas pilas reales de protocolos de la red de paquetes. Las redes de paquetes utilizadas en esta Recomendación proporcionarán modos de funcionamiento fiables y no fiables, incluido un medio para distinguir fronteras de paquetes.

IV.1 TCP/IP/UDP

Adviértase que UDP puede fragmentar y reensamblar grandes paquetes de vídeo, pero un fracaso en la ejecución de la paquetización de MB puede conducir a la pérdida de un GOB completo.

La multidifusión IP debe utilizarse para la distribución GRQ en oposición a la difusión de capa de acceso a medios.

<table>
<tr><th>Aplicaciones de entrega no fiable</th><th>Señalización de llamada y canal H.245</th></tr>
<tr><td rowspan="2">UDP</td><td>TPKT</td></tr>
<tr><td>TCP</td></tr>
<tr><td colspan="2">IP</td></tr>
<tr><td colspan="2">Capa de enlace</td></tr>
<tr><td colspan="2">Capa física</td></tr>
</table>

Un TPKT es un formato de paquete como se define en IETF RFC 1006. Se utiliza para delimitar mensajes particulares (PDU) dentro del tren TCP, que proporciona un tren continuo de octetos sin límites explícitos. Un TPKT consta de un campo de número de versión de un octeto seguido de un campo reservado de un octeto, seguido de un campo de longitud de dos octetos, seguido de los datos reales. El campo número de versión contendrá el valor "3", el campo reservado contendrá el valor "0", el campo de longitud contendrá la longitud de todo el paquete incluido los campos número de versión, reservado y de longitud con una palabra "big-endian" (los octetos de la izquierda son los más significativos) de 16 bits.

IV.1.1 Descubrimiento del controlador de acceso

IV.1.1.1 Descubrimiento utilizando dirección multidifusión o puerto conocido

Tras el descubrimiento del controlador de acceso y los procedimientos de registro descritos en la cláusula 7/H.323, los puntos extremos deben utilizar la siguiente dirección multidifusión o puerto conocido cuando intenten descubrir el controlador de acceso apropiado para su configuración de red:

– Dirección UDP para comunicación multidifusión con controladores de acceso: 224.0.1.41

– Puerto UDP para comunicación multidifusión con controladores de acceso: 1718

– Puerto UDP para comunicación RAS unidifusión donde no existe "otro acuerdo": 1719

Cabe señalar que "otro acuerdo" puede incluir el registro de un punto extremo con un controlador de acceso.

Se señala que las implementaciones deberán tener en cuenta el alcance de la multidifusión a fin de no sobrecargar Internet con mensajes de descubrimiento.

Suponiendo que un controlador de acceso tiene una dirección IP por ejemplo de 134.134.12.1, puede tener lugar la señalización siguiente:

– LRQ o GRQ llega a 134.134.12.1: puerto 1719;

– LRQ o GRQ llega a 134.134.12.1: puerto 1718 (se señala que esto puede ocurrir con los controladores de acceso de la versión 1);

– LRQ o GRQ llega a 224.0.1.41: puerto 1718.

El controlador de acceso puede transmitir un mensaje LRQ a las siguientes direcciones:

– 224.0.1.41: puerto 1718 (multidifusión a todos los controladores de acceso);

– X.X.X.X: puerto 1719 (a un determinado controlador de acceso).

El puerto 1719 sólo se debe utilizar cuando se envía una petición unidifusión. Esto permite al receptor conocer si debe enviar un rechazo (xRJ) al emisor (debe hacerlo en todos los casos).

El puerto 1718 sólo se debe utilizar cuando se envía una petición multidifusión. El receptor debe enviar la respuesta adecuada dependiendo del mensaje. Para LRQ que no requiere rechazo, el receptor no debe responder las peticiones multidifusión. Para GRQ se debe enviar un GRJ dirigido a la fuente de la GRQ.

IV.1.1.2 Descubrimiento utilizando DNS (informativo)

IV.1.1.2.1 Un URL para controladores de acceso

En primer lugar, obsérvese que un controlador de acceso se identifica mediante una dirección de transporte y un gatekeeperIdentifier (identificador de controlador de acceso), que es una cadena. Un controlador de acceso es un recurso particular en Internet, y por ello es lógico especificarlo en un localizador de recurso uniforme (URL, *uniform resource locator*). El protocolo formulado por el controlador de acceso es RAS, por lo que el URL para un controlador de acceso puede venir dado por:

ras://gkID@domainname

gkID (ID de controlador de acceso) es el gatekeeperIdentifier, y domainname (nombre de dominio) es un nombre del sistema de nombres de dominio (DNS, *domain name system*) que identifica el dominio del controlador de acceso. Se señala que no necesariamente es éste un nombre de dominio totalmente cualificado (FQDN, *fully qualified domain name*) con un registro A; no es preciso que este nombre de dominio tenga una interfaz de transporte física con un número IP registrado en el DNS. No obstante, si es un FQDN, es razonable insistir en que su número IP es el del controlador de acceso al que se refiere el URL. En este caso, se puede añadir un número de puerto opcional al URL:

ras://gkID@domainname:port_no.

Si no se proporciona ningún número de puerto, el valor conocido de 1719 se toma como un valor por defecto.

El caso más interesante es cuando no se trata de un FQDN, y el nombre de dominio no designa, por tanto, una dirección de transporte indicada en el DNS. El nombre de dominio puede referirse entonces a una pura "zona de autoridad del controlador de acceso". En la próxima cláusula se explica cómo localizar el controlador de acceso en este caso.

IV.1.1.2.2 Localización del URL

El URL no resuelve el problema de localizar el controlador de acceso, sólo proporciona un formato normalizado de la información que hay que hallar. El problema consiste en cómo producir una dirección de transporte y un gatekeeperidentifier para la señalización RAS dado el nombre de dominio de un controlador de acceso.

Si el controlador de acceso tiene un identificador conforme a IETF RFC 822, es fácil extraer un nombre de dominio a partir del identificador de un controlador de acceso conforme a IETF RFC 822. De hecho, puede ser conveniente proporcionar a los puntos extremos identificadores conformes a IETF RFC 822 y luego estipular que la parte nombre de dominio del identificador se refiere al dominio del controlador de acceso.

IV.1.1.2.2.1 Indagación de registro de recursos SRV

La primera solución tiene en cuenta el hecho de que el controlador de acceso es básicamente un servicio de sistema, y que la dirección de transporte de un servicio de sistema nominado se puede extraer del DNS mediante la indagación de un nuevo tipo de registro de recurso DNS, denominado "registro de localización de servicio" (SRV, *service location record*). Dado un nombre de dominio, se efectuará una indagación de registro SRV de la dirección de transporte del servicio RAS para ese dominio. El propio nombre de dominio, o el que se devuelve en la respuesta SRV, se utiliza como gatekeeperidentifier. El registro SRV y su uso se definen en IETF RFC 2782.

IV.1.1.2.2.2 Indagación de registro TXT

Todas las implementaciones DNS actuales soportan el registro de recurso TXT. Se trata, básicamente, de algún texto libre que puede ser devuelto para cada nombre de dominio. Es posible almacenar muchos recursos TXT para un solo dominio. La norma estipula que se devuelvan todos los registros TXT cuando se efectúe una indagación sobre ellos.

Es posible utilizar indagaciones TXT si fallan las indagaciones SRV. Se supone que para extraer un nombre de dominio se utiliza el mismo convenio que se propuso anteriormente. Para gatekeeperIdentifiers pueden utilizarse cadenas conformes a IETF RFC 822 (nombres de correo electrónico "-like") o cadenas conformes a IETF RFC 1768 (URL). En cualquiera de los dos casos se utiliza el nombre de dominio para efectuar una indagación TXT de DNS sobre el nombre de dominio. Los registros de recursos devueltos son líneas de texto libre, y el terminal buscará entonces líneas en la respuesta de la forma:

ras [< gk id>@]<domain name >[:<portno>] [<priority>]

El campo **<gk id>** es un ID de controlador de acceso opcional que está separado del nombre de dominio. Si este campo está ausente, se supone que el propio dominio es entonces el ID de controlador de acceso.

El campo **<domain name>** puede ser el nombre del registro A que contiene la dirección IP del controlador de acceso, o bien una dirección IP bruta en forma de puntos. No es necesario que el nombre de dominio esté totalmente cualificado; si no lo está, el subdominio en el que se localizó el registro TXT se añadirá a él para formar el nombre de registro A totalmente cualificado.

El campo opcional **[:<portno>]** puede utilizarse para especificar un número de puerto distinto del puerto RAS normalizado.

El campo opcional **[<priority>]** especifica el orden en que se debe acceder a los controladores de acceso enumerados para el descubrimiento o las indagaciones LRQ si hay más de un registro TXT ras. Los números más bajos tienen mayor prioridad.

Obsérvese que, si el campo **<gk id>** está ausente, este formato supone que los ID de controlador de acceso son en realidad nombres de dominio legales. No obstante, si es necesario que un solo sistema central soporte múltiples controladores de acceso lógicos, cada uno con un ID distinto, el formato lo soportará. Esto es así porque los registros A separados pueden contener la misma dirección IP.

Se utilizan espacios en blanco como delimitadores entre **ras** y **gk id**, si están presentes, o **domain name**, y entre **portno** y **priority**. Los espacios en blanco están formados por cualquier número de espacios o tabuladores.

Ejemplos de registros TXT de controlador de acceso válidos:

– ras gk1
– ras gk1.company.com
– ras gk1:1500 3
– ras 172.11.22.33:1500 2

El cliente servidor analiza las líneas y a partir de ellas obtiene la dirección de transporte del controlador de acceso dentro de ese dominio a la que puede enviar mensajes RAS.

Puesto que el DNS requiere un servidor para devolver todos los registros TXT asociados con un nombre de dominio, el cliente puede seleccionar y procesar únicamente los registros que le son útiles. Permite también al DNS devolver una lista ordenada de controladores de acceso que pueden servir como alternativas y reservas, tal como se define en la Rec. UIT-T H.323.

Se señala que el servidor devuelto en esa indagación podría ser una dirección de transporte real en notación decimal de puntos, o un FQDN que necesita una indagación de registro A en DNS para determinar la dirección de transporte. La ventaja de utilizar un FQDN es que habitualmente se ocultan los números IP reales. La ventaja de utilizar números IP consiste en que se evita una segunda indagación en DNS, acortando así el tiempo previo al establecimiento de la comunicación.

IV.1.1.2.3 Procesamiento de los ID de correo electrónico por el controlador de acceso durante los mensajes ARQ y LRQ

Cuando el campo **destinationInfo (información de destino)** de un mensaje ARQ o LRQ contiene una dirección de alias **email-ID (identificador de correo electrónico)**, el controlador de acceso debe verificar primero la base de datos de su registro en relación con el alias. Si no puede resolverlo, el controlador de acceso debe analizar el alias para recuperar su porción de dominio. Si no se proporciona ningún dominio, el controlador de acceso puede generar un dominio por defecto. El dominio se utiliza entonces para localizar uno o más controladores de acceso, utilizando los procedimientos indicados en IV.1.1.2.2. El controlador de acceso puede indagar a todos los controladores de acceso así localizados con un intercambio de mensajes LRQ/LCF/LRJ.

Obsérvese que más de un controlador de acceso puede tener registros TXT correspondientes en un solo dominio DNS. En consecuencia, un solo dominio DNS puede "contener" más de una zona H.323. Por ello, incluso si un controlador de acceso no puede resolver un ID de correo electrónico cuya porción de dominio es uno de sus dominios por defecto, puede indagar todavía otras zonas en el mismo dominio DNS.

Si el controlador de acceso es presentado con un alias no registrado que es un **h323-id** y el ID puede ser interpretado como una porción de usuario legal de un nombre IETF RFC 822, el controlador de acceso puede interpretar el alias como si fuera un ID de correo electrónico en su dominio por defecto e intentar localizar el alias en algún otro controlador de acceso. Del mismo modo, el controlador de acceso puede quitar el nombre de dominio de un ID de correo electrónico procedente de un mensaje LRQ entrante para que pueda ser localizado como un h323-ID.

IV.1.2 Comunicaciones de punto extremo a punto extremo

Los puntos extremos que deseen recibir llamadas de puntos extremos que caen fuera de la zona de su controlador de acceso deben utilizar el siguiente puerto por el canal de señalización de llamada:

– Puerto de señalización de llamada TCP de punto extremo 1720

Aunque está permitido utilizar valores dinámicos para que estos puertos permitan múltiples puntos extremos en un único dispositivo, debe entenderse que esto impedirá la interoperación con puntos extremos que quedan fuera de la zona del controlador de acceso, excepto vía de una pasarela en la zona.

IV.2 SPX/IPX

Adviértase que dado que no hay ningún reensamblado de red de paquetes grandes, es esencial el uso de fragmentación de MB.

Aplicaciones de entrega no fiable	Canal H.245 canal de señalización de llamada
PXP	SPX
IPX	
Capa de enlace	
Capa física	

IV.2.1 Descubrimiento del controlador de acceso

En terminología IPX, un "zócalo" es el equivalente de un "puerto" en IP y un "identificador TSAP" en esta Recomendación y en la Rec. UIT-T H.323.

En las redes basadas en IPX, los controladores de acceso deben anunciar el "tipo de servicio de controlador de acceso" definido más adelante para permitir a los puntos extremos localizarlos en una red. Análogamente, los puntos extremos deben solicitar al "tipo de servicio de controlador de acceso" que encuentre la ubicación del controlador de acceso más próximo.

– Tipo de servicio de controlador de acceso En estudio

NOTA – El tipo de servicio se denomina zócalo SAP en alguna documentación IPX.

IV.2.2 Comunicación de punto extremo a punto extremo

Los puntos extremos que desean recibir llamadas de puntos extremos que caen fuera de la zona de su controlador de acceso, deben utilizar los siguientes zócalos para señalización de llamada.

– Puerto de señalización de llamada IPX de punto extremo En estudio

Aunque se permite utilizar valores dinámicos para que estos zócalos permitan múltiples puntos extremos en un solo dispositivo, debe entenderse que esto evitará la interoperación con puntos extremos que caen fuera de la zona del controlador de acceso, salvo vía una pasarela en la zona.

IV.3 SCTP

La pila de protocolos H.323 por SCTP es como sigue:

Aplicaciones de entrega no fiable	Señalización de llamada con control de llamada tunelizado
UDP	SCTP
IP	
Capa de enlace	
Capa física	

Cada mensaje de señalización de llamada H.225.0 se transferirá en un bloque DATOS SCTP distinto. No se añadirán encabezamientos (es decir, no habrá TPKT). Deberá especificarse el orden de entrega.

IV.3.1 Trenes

Todos los mensajes de la misma llamada utilizarán el mismo tren SCTP. La implementación puede utilizar distintos trenes para diferentes llamadas.

IV.3.2 Identificadores de protocolos de cabida útil

Puede utilizarse SCTP con un identificador de protocolo de cabida útil indefinido (0) o con 13, que es el número asignado a H.323 por la IANA.

Apéndice V

Utilización de ASN.1 en esta Recomendación

En este apéndice se recapitulan los convenios ASN.1 que se han utilizado en esta Recomendación. En las futuras revisiones de esta Recomendación sólo deberán utilizarse estas construcciones. Únicamente en circunstancias excepcionales se considerarán construcciones ASN.1 adicionales.

V.1 Rotulado (tagging)

Todos los rótulos (tags) en esta Recomendación son AUTOMATIC TAGS.

V.2 Tipos

Los siguientes tipos pueden aparecer en las definiciones ASN.1 de esta Recomendación.

BIT STRING	IA5String	OCTET STRING
BMPString	INTEGER	SEQUENCE
BOOLEAN	NULL	SEQUENCE OF
CHOICE	NumericString	SET
GeneralString	OBJECT IDENTIFIER	SET OF

V.3 Constricciones y gamas

Esta Recomendación utiliza constricciones de tamaño ("SIZE") para cadenas, SET OF y SEQUENCE OF, constricciones de gama de valores para enteros, y alfabetos permitidos ("FROM").

V.4 Extensibilidad

Esta Recomendación utiliza el marcador de extensión (elipsis "...").

Apéndice VI

Identificadores H.225.0 de protocolos de señalización tunelizados

La presente Recomendación soporta la tunelización de protocolos de señalización de llamada no H.323, como se describe en 10.4/H.323. La serie de anexos M/H.323 a la Recomendación (M.1/H.323, M.2/H.323, etc.) define la tunelización de protocolos específicos. Un protocolo tunelizado en esta Recomendación se identifica mediante información en la estructura ASN.1 **TunnelledProtocol (protocolo tunelizado)** definida en 7.6 y en el anexo H. El presente apéndice contiene una lista de identificadores de **TunnelledProtocol** que han sido atribuidos a protocolos tunelizados específicos.

Los protocolos tunelizados que se definen como propios de esta Recomendación se muestran en los cuadros VI.1 y VI.2. Se señala que la tunelización no se limita a los protocolos indicados en esos cuadros.

Cuadro VI.1/H.225.0 – Protocolos tunelizados identificados por el tunnelledProtocolObjectID

Especificación de tunelización	Especificación de protocolo	tunnelledProtocolObjectID	subIdentifier
M.1/H.323	ISO/CEI 11572 y 11582	{iso (1) identified-organization (3) icd-ecma (0012) private-isdn-signalling-domain (9)}	(Ninguno)
M.2/H.323	Rec. UIT-T Q.763 (1988)	{itu-t (0) recommendation (0) q (17) 763}	"1988"
M.2/H.323	Rec. UIT-T Q.763 (1993)	{itu-t (0) recommendation (0) q (17) 763}	"1993"

Cuadro VI.2/H.225.0 – Protocolos tunelizados identificados por el TunnelledProtocolAlternateIdentifier

Especificación de tunelización	Especificación de protocolo	protocolType	protocolVariant	subIdentifier
M.2/H.323	ANSI T1.113-1988	"isup"	"ANSI T1.113-1988"	"1988"
M.2/H.323	ETS 300 121	"isup"	"ETS 300 121"	"121"
M.2/H.323	ETS 300 356	"isup"	"ETS 300 356"	"356"
M.2/H.323	BELLCORE GR-317	"isup"	"BELLCORE GR-317"	"317"
M.2/H.323	JT-Q761-4(1987-1992)	"isup"	"JT-Q761-4(1987-1992)"	"87"
M.2/H.323	JT-Q761-4(1993)	"isup"	"JT-Q761-4(1993)"	"93"

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2004