UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.510

(03/2002)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Procedimientos de movilidad y de colaboración – Movilidad para los sistemas y servicios multimedios de la serie H

Movilidad para sistemas y servicios multimedios H.323

Recomendación UIT-T H.510

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

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

Recomendación UIT-T H.510

Movilidad para sistemas y servicios multimedios H.323

Resumen

Esta Recomendación tiene por finalidad definir servicios y procedimientos para el soporte de la movilidad en los sistemas multimedios H.323.

Orígenes

La Recomendación UIT-T H.510, preparada por la Comisión de Estudio 16 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 29 de marzo de 2002.

Palabras clave

H.323, movilidad del terminal, movilidad del usuario, sistemas multimedios.

PREFACIO

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

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

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

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

NOTA

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Recomendación UIT-T H.510

Movilidad para sistemas y servicios multimedios H.323

1 Alcance

Esta Recomendación trata los aspectos de movilidad relativos a los sistemas H.323 por encima de la capa de transporte. La presente Recomendación H.510 aplica nuevas funciones definidas para soportar la gestión de la movilidad para sistemas H.323.

Trata principalmente el soporte de la movilidad de los terminales, aunque también trata el soporte de la movilidad de usuario en el contexto de H.323. Esta versión de la presente Recomendación no abarca los procedimientos de traspaso en los cuales se pueden mantener llamadas activas durante cambios de ubicación.

El interfuncionamiento con otras redes para el soporte de la movilidad a través de redes de diferentes tipos está fuera del ámbito de la presente Recomendación.

2 Referencias

2.1 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.

[1] Recomendación UIT-T H.323 (2000), *Sistemas de comunicación multimedios basados en paquetes*.

[2] Recomendación UIT-T H.225.0 (2000), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.

[3] Recomendación UIT-T H.225.0 Anexo G (1999), *Comunicación entre dominios administrativos*.

[4] Recomendación UIT-T H.501 (2002), *Protocolo para la gestión de movilidad y comunicación intradominio e interdominio en sistemas multimedios*.

[5] Recomendación UIT-T H.530 (2002), *Procedimientos de seguridad simétricos para H.510 (movilidad para los sistemas y servicios multimedios H.323)*.

2.2 Referencias informativas

– IETF RFC 2486 (1999), *The Network Access Identifier*.

3 Definiciones

A los efectos de esta Recomendación se aplicarán las definiciones dadas en la Rec. UIT-T H.323, con las siguientes adiciones:

3.1 dominio administrativo: Se define como en H.225.0 anexo G. Un dominio administrativo está constituido por una o más zonas.

3.2 identidad de usuario llamable: Identidad de usuario que puede ser utilizada por un usuario llamante para hacer una llamada al usuario identificado por esta identidad de usuario. Puede ser anunciada, por ejemplo en una guía telefónica, como la identidad mediante la cual un usuario puede ser alcanzado.

3.3 punto de conexión H.323: Punto de conexión de una red que permite al terminal H.323 registrarse (inscribirse) en un controlador de acceso o comunicar directamente con otro terminal.

3.4 dominio de base: El dominio administrativo que está relacionado con el usuario móvil por un contrato de abono. El dominio de base contiene datos específicos del usuario que incluyen la ubicación, autenticación, e información de perfil de servicio relacionadas con el usuario móvil.

3.5 controlador de acceso de base (GK de base): Controlador de acceso en el dominio de base de un usuario.

3.6 proveedor de servicio de base: Proveedor de servicio o administrador a cargo del dominio de base de un usuario, lo que implica que el usuario está relacionado con el proveedor de servicio de base por un contrato de abono.

3.7 ubicación: Punto de conexión de la red a través del cual el usuario/terminal tiene acceso al sistema H.323 en ese momento.

3.8 terminal móvil H.323: Terminal que puede cambiar el punto de conexión H.323.

3.9 gestión de la movilidad: Conjunto de funciones que se necesitan para proporcionar la movilidad del usuario, del terminal y del servicio.

3.10 punto de conexión de red: Interfaz de red utilizado por un punto extremo para acceder al sistema H.323. Cada punto de conexión de red está asociado con una dirección de red (por ejemplo, una dirección IP) mediante la cual los paquetes enviados al punto extremo llegan al punto extremo.

3.11 en línea: Estado de un usuario o terminal móvil que ha "iniciado una sesión", es decir que está registrado actualmente en un controlador de acceso, por oposición a estar **ausente** o haber "terminado una sesión".

3.12 identidad de usuario primaria: Identidad de usuario atribuida permanentemente a un usuario en el momento del abono y que se mantiene durante todo el tiempo que dura el abono. Cada usuario tiene una identidad de usuario primaria, y sólo una.

3.13 movilidad del servicio: Aptitud de un usuario para utilizar el servicio particular (a que se ha abonado) cualquiera que sea la ubicación del usuario y del terminal empleado para ese fin.

3.14 dominio sirviente: Dominio administrativo (visitado o de base) que está sirviendo a un usuario/terminal móvil en línea.

3.15 controlador de acceso sirviente: Controlador de acceso (visitado o de base) en el que un usuario/terminal móvil en línea está registrado en ese momento.

3.16 identidad de usuario temporal: Identidad de usuario atribuida provisionalmente a un usuario y que está prevista para ser utilizada en lugar de la identidad de usuario primaria, por ejemplo por razones de seguridad.

3.17 identidad de terminal: Código o cadena de caracteres que identifica unívocamente a un terminal.

NOTA – Una posible utilización es para autenticar el terminal durante el registro del usuario. La autenticación del terminal permite verificar si el usuario está o no autorizado para utilizar el terminal (por ejemplo, si el terminal móvil H.323 ha sido "puesto en lista negra" por el proveedor de servicio de base – por ejemplo si ha sido robado – el usuario móvil no puede registrarse en la red H.323 con ese terminal).

3.18 movilidad del terminal: Aptitud de un terminal para cambiar su ubicación (es decir, el punto de conexión de red y el punto de conexión H.323) al mismo tiempo que conserva su capacidad de comunicar.

3.19 movilidad discreta del terminal (terminal en desplazamiento): Aptitud de un terminal para realizar cambios discretos de ubicación, es decir cambiar su ubicación cuando no haya trenes de medios activos.

3.20 movilidad continua del terminal (traspaso): Aptitud de un terminal para cambiar su ubicación cuando hay trenes de medios activos. Se dice que el traspaso se efectúa *sin contratiempo* cuando como resultado del cambio de ubicación del terminal no se produce un retardo o pérdida de datos que serían percibidos por el usuario como una degradación de la calidad de servicio (se señala que el hecho de que los traspasos se efectúen sin contratiempo puede depender de muchos factores, tales como el tipo de servicio y la robustez de la presentación del servicio respecto a la pérdida de datos en el terminal).

3.21 usuario: Persona o entidad autorizada para utilizar servicios de comunicación H.323.

3.22 identidad de usuario: Código o cadena de caracteres que identifica unívocamente a un usuario a través de una infraestructura multiusuario, multiservicio.

3.23 movilidad del usuario (movilidad personal): Aptitud de un usuario para mantener la misma identidad de usuario cualquiera que sea el terminal utilizado y su punto de conexión de red. Los terminales utilizados pueden ser de tipos diferentes.

3.24 movilidad discreta del usuario (usuario en desplazamiento): Aptitud de un usuario para cambiar su ubicación o sus terminales cuando no haya trenes de medios activos.

3.25 movilidad continua del usuario (movilidad de la sesión): Aptitud de un usuario para cambiar su ubicación o sus terminales cuando hay trenes de medios activos.

NOTA – En la red con conmutación de circuitos se ofrece una prestación similar mediante el servicio suplementario portabilidad del terminal.

3.26 perfil de servicio de usuario: Información específica del usuario que indica los servicios a que está abonado un usuario y los datos de configuración personales para los respectivos servicios.

3.27 dominio visitado: Dominio administrativo que no es el dominio de base y está sirviendo a un usuario móvil.

3.28 controlador de acceso visitado (GK visitado): Controlador de acceso en un dominio visitado.

4 Símbolos y abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

A Dirección (como un tipo de registro/indagación DNS) (*address*)

AuF Función de autenticación (*authentication function*)

BE Elemento de frontera (*border element*)

DHCP Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)

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

e164 Tipo de dirección "número de teléfono" (según Rec. UIT-T E.164)

EP Punto extremo (*endpoint*)

GK Controlador de acceso (*gatekeeper*)

HLF Función ubicación de base (*home location function*)

IMSI Identidad internacional de abonado del servicio móvil (*international mobile subscriber identity*)

IP Protocolo Internet (*Internet protocol*)

MT Terminal móvil (*mobile terminal*)

NAI Identificador de acceso a red (*network access identifier*)

NPoA Punto de conexión de red (*network point of attachment*)

RAS Protocolo de registro, admisión y estado (*registration, admission and status*) (Rec. UIT-T H.225.0)

En esta Recomendación se utilizan los siguientes mensajes RAS:

ACF Confirmación de admisión (*admissionConfirm*)

ARJ Rechazo de admisión (*admissionReject*)

ARQ Petición de admisión (*admissionRequest*)

GCF Confirmación de controlador de acceso (*gatekeeperConfirm*)

GRJ Rechazo de controlador de acceso (*gatekeeperReject*)

GRQ Petición de controlador de acceso (*gatekeeperRequest*)

LCF Confirmación de localización (*locationConfirm*)

LRQ Petición de localización (*locationRequest*)

RCF Confirmación de registro (*registrationConfirm*)

RIP Petición en curso (*requestInProgress*)

RRJ Rechazo de registro (*registrationReject*)

RRQ Petición de registro (*registrationRequest*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

SRV Servicio (como un tipo de registro/indagación DNS) (*service*)

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

TXT Texto (como un tipo de registro/indagación DNS) (*text*)

UCF Confirmación de desregistro (*unregistrationConfirm*)

UIM Módulo de identificación de usuario (*user identification module*)

URL Localizador de recurso universal (*universal resource locator*)

URQ Petición de desregistro (*unregistrationRequest*)

VLF Función ubicación del visitante (*visitor location function*)

5 Descripción del servicio de movilidad H.323

En las siguientes cláusulas se definen los servicios proporcionados por el sistema H.323 para ofrecer movilidad del terminal y movilidad del usuario. Se trata de descripciones del servicio global desde el punto de vista del usuario y no se describen los aspectos de la interfaz de usuario.

5.1 Descripción general

5.1.1 Movilidad del usuario H.323

Esta Recomendación trata el soporte de usuarios móviles pertenecientes a una red H.323.

NOTA – La movilidad del usuario en general se describe en otras Recomendaciones.

En una red que soporta la movilidad del usuario hay una asociación dinámica entre usuarios y terminales móviles. Cualquier usuario móvil puede registrarse en cualquier terminal con acceso a la red, dentro de los límites de los permisos aplicables. El registro permite al usuario móvil obtener los servicios permitidos por el perfil de servicio de usuario aplicable en el terminal que se está utilizando en ese momento. Un cambio de ubicación tiene por resultado un nuevo registro del usuario móvil y el correspondiente desregistro de la ubicación anterior (si existía).

Un usuario móvil siempre pertenece a un dominio administrativo, y sólo a uno, el dominio de base de ese usuario. La movilidad del usuario puede estar limitada al dominio de base, o puede permitirse a través de múltiples dominios administrativos según acuerdos de servicio entre esos dominios y el dominio de base del usuario.

El perfil de servicio de usuario aplicable a un usuario móvil depende de la ubicación actual y de los acuerdos de servicio antes mencionados. Una vez registrado debidamente, un usuario móvil podrá iniciar y/o recibir llamadas en la ubicación actual. Sin embargo, pueden ser aplicables restricciones relativas a la utilización de los recursos permitidos, la calidad de servicio disponible, etc.

Con respecto a la Rec. UIT-T H.323 y en lo tocante a la movilidad interdominio hay que considerar dos aspectos:

a) un usuario móvil se registra en un terminal H.323. El usuario es tratado como un usuario H.323 nativo sin tener en cuenta que su dominio de base sea o no un sistema H.323. En este último caso, el dominio de base redirigirá a una pasarela de ingreso H.323 las llamadas destinadas al usuario móvil.

b) Un usuario móvil cuyo dominio de base es un sistema H.323 transita a otra red. En este caso el dominio de base H.323 redirigirá a una pasarela de egreso H.323 las llamadas destinadas al usuario móvil.

5.1.2 Movilidad del terminal H.323

Por movilidad de un terminal H.323 ha de entenderse que un terminal H.323 puede cambiar su ubicación, es decir, su punto de conexión de red, y conservar su aptitud para comunicar. En esta Recomendación la movilidad del terminal se formula atendiendo a la movilidad de un usuario que en un momento dado está asociado al terminal. Sólo en aquellos casos en que existan consideraciones especiales que sean aplicables específicamente a terminales y no a usuarios se tratará separadamente la movilidad del terminal.

Es posible que ningún usuario esté registrado en un determinado terminal. Los servicios que serán posibles en un terminal sin que un usuario esté registrado dependerán de la implementación. Para proveer servicios en un terminal en que no haya ningún usuario móvil registrado, dicho terminal puede ser asociado con un usuario "por defecto" inscrito "por administración". De esta forma no es necesario atender los terminales directamente y pueden tratarse con referencia a su usuario por defecto.

5.1.3 Movilidad del servicio

En el contexto de esta Recomendación, la movilidad del servicio está limitada a aplicar el perfil de servicio de usuario móvil cuando se hace o se recibe una llamada.

NOTA – Otros aspectos de la movilidad del servicio se describirán en otras Recomendaciones.

5.2 Requisitos H.323

5.2.1 Requisitos de la movilidad de usuario H.323

La movilidad de usuario H.323 implica los siguientes servicios:

1) **Identificación y autenticación del usuario móvil**: permiten a un dominio sirviente validar la identificación del usuario móvil.

2) **Autenticación del dominio sirviente**: permite a un usuario móvil verificar la autenticidad del dominio sirviente para asegurarse de que el dominio es efectivamente aquél de que se esperan los servicios.

3) **Registro/desregistro del usuario móvil**: permite al usuario móvil asociarse con cualquier terminal H.323 alámbrico o inalámbrico para hacer o recibir llamadas. Esto puede efectuarse de forma permanente (sin ningún desregistro) o temporal (con desregistro una vez terminado un periodo de registro).

   NOTA – Un registro permanente podría activarse "por administración" sin que interviniera ningún usuario real. Esto puede tener muchas aplicaciones útiles, tales como la prestación de servicio en terminales públicos, o la administración de un terminal "por defecto" en el escritorio personal de un usuario.

4) **Tratamiento de llamada de un usuario móvil**: permite a un usuario móvil hacer y/o recibir llamadas, generalmente después del registro, basándose en su identidad de usuario en cualquier terminal H.323 adecuado. Esta aptitud sólo puede estar limitada por las capacidades del terminal y de la red, y quizás por las restricciones impuestas por los acuerdos de nivel de servicio (SLA, *service level agreements*) entre proveedores de servicio de los dominios administrativos que intervienen. Este servicio consta de dos partes (que pueden ser soportadas independientemente una de la otra), a saber, el tratamiento de llamada entrante y el tratamiento de llamada saliente:

   - *Tratamiento de llamada entrante de usuario móvil*, que dirige las llamadas entrantes para un usuario móvil hacia un terminal H.323 en que dicho usuario se ha registrado, independientemente de la ubicación del terminal y del dominio sirviente en que se ha registrado el usuario móvil.
   - *Tratamiento de llamada saliente de usuario móvil*, que detecta una llamada saliente de un usuario móvil y la establece aplicando el perfil de servicio de usuario, independientemente de la ubicación del usuario dentro de la red H.323. La identidad del usuario será presentada a cualquier parte de destino como la identificación normal del originador de la llamada, independientemente de la ubicación del terminal y del dominio sirviente en el que está registrado el usuario móvil.

5.2.2 Requisitos de la movilidad de terminal H.323

La movilidad de terminal H.323 implica los siguientes servicios:

1) **Autenticación de un terminal móvil H.323**: permite la verificación de la autenticidad de un terminal móvil H.323 en el contexto de la *asociación* que tiene con un usuario móvil (previamente establecida mediante registro). La autenticación del terminal se utiliza para verificar que el terminal puede realmente actuar a nombre del usuario que está registrado en dicho terminal en ese momento.

   NOTA – La información para determinar qué terminal concreto se utiliza sólo es útil para fines secundarios, por ejemplo para cotejarla con una lista negra de terminales robados, o para localizar un terminal, más bien que un usuario.

2) **Autenticación del dominio sirviente**: permite a un terminal móvil H.323 verificar la autenticidad del dominio sirviente (al entrar en dicho dominio) a nombre del usuario móvil que se ha registrado en el terminal.

3) **Registro/desregistro del terminal móvil H.323**: permite a un terminal móvil H.323 renovar el registro del usuario móvil actualmente asociado con dicho terminal cuando cambia la ubicación y anular el registro, por ejemplo cuando es apagado.

4) **Transferencia de perfiles de servicio de usuario**: permite transferir el perfil de servicio de usuario (o una parte del mismo) al dominio sirviente (es decir, al controlador de acceso responsable o posiblemente al terminal propiamente dicho).

5) **Tratamiento de llamada de terminal móvil H.323**: está totalmente abarcado por el tratamiento de llamada de usuario móvil pues se supone que un usuario necesita estar asociado con el terminal para los fines del tratamiento de llamada (puede ser un usuario por defecto).

6) **Traspaso de terminal móvil H.323**: permite a un terminal móvil H.323 mantener una llamada mientras se desplaza de una ubicación a otra. Esta prestación queda en estudio.

5.2.3 Requisitos de la identificación de movilidad

5.2.3.1 Identificación del usuario móvil

Un usuario puede tener múltiples identidades diferentes previstas para fines diferentes. Puede haber al menos tres utilizaciones distintas de la identidad de usuario:

- La más evidente es la utilización por un usuario llamante que desea llamar a un usuario llamado. Un número e164 es un ejemplo de este tipo de identidad, que será denominada aquí **identidad de usuario llamable**.
- Otra finalidad de la identidad de usuario es identificar un usuario permanentemente ante el proveedor de servicio de base por toda la duración del abono del usuario. Esta identidad, denominada aquí **identidad de usuario primaria**, es la identidad clave con respecto a la cual se establece la correspondencia de todas las demás identidades de usuario. Este tipo de identificador hace posible que un usuario tenga varias identidades de usuario llamables, o cambiar las entidades de usuario llamables mientras se mantiene la misma identidad de usuario primaria (y por lo tanto el mismo abono) con el proveedor de servicio de base.
- Una tercera utilización en algunos sistemas, en los que puede ser conveniente transmitir la identidad de usuario primaria con la menor frecuencia posible, es identificar un usuario localmente atribuyéndole una identidad de usuario no permanente durante cierto periodo de tiempo o mientras el usuario está ubicado en cierta parte de la red. Este tipo de identidad de usuario se denomina **identidad de usuario temporal** y se utiliza en lugar de la identidad de usuario primaria, normalmente por razones de seguridad.

Es posible que una misma identidad de usuario funcione como una identidad de usuario llamable y como la identidad de usuario primaria, pero debe ser posible utilizar identidades de usuario diferentes para estos fines. Si una identidad de usuario se utiliza tanto para la identidad de usuario primaria como para una identidad de usuario llamable, no debe haber necesidad de utilizar una identidad de usuario temporal para el usuario.

A los efectos de esta Recomendación se deben cumplir los siguientes requisitos:

- El usuario (no el terminal) se identifica mediante una AliasAddress de acuerdo con la Rec. UIT-T H.225.0. El usuario puede tener varias direcciones de alias únicas tales como una dirección de correo electrónico de tipo email-ID, un URL de tipo URL-ID, un número de teléfono de tipo e164, un módulo de identificación de usuario (UIM, *user identification module*) que incluya por ejemplo una identidad de abonado móvil internacional (IMSI, *international mobile subscriber identity*), etc.
- Todos los tipos de identidad de usuario – identidad de usuario llamable, identidad de usuario primaria e identidad de usuario temporal – serán direcciones de alias.

- Las identidades de usuario serán únicas dentro de la porción de un sistema H.323 en la que podrán utilizarse. Esto significa que la identidad de usuario primaria y cualesquiera identidades de usuario llamables que puedan utilizarse a nivel mundial tienen que ser únicas a nivel mundial. No obstante, puede haber identidades de usuario llamables que se utilicen localmente, tales como los números abreviados. Las identidades de usuario temporales pueden también tener significado solamente local.

5.2.3.2 Identificación del terminal móvil

Aunque es posible que para fines de encaminamiento de llamadas y de gestión de la movilidad la identidad del terminal utilizado por un usuario móvil no ofrezca interés, en algunos caso puede necesitarse también identificar el terminal, por ejemplo para prohibir la utilización de terminales robados o no provistos de licencia.

A los efectos de esta Recomendación se cumplirán los siguientes requisitos:

- El terminal (soporte lógico y/o soporte físico) puede tener una firma, por ejemplo de tipo h323-ID, que es generada por el vendedor del terminal dentro del proceso de fabricación. La firma será única y nunca cambiará en todo el tiempo de vida del terminal.
- Los terminales se identifican para fines de encaminamiento por su dirección en la capa de red y en ciertas ocasiones por su dirección en la capa de enlace de datos.

5.2.3.3 Identificación del dominio administrativo

La identificación del dominio administrativo tiene dos finalidades. En primer lugar, es necesaria para identificar el dominio administrativo de base de un usuario a efectos de actualizar la información de ubicación del usuario y para obtener la ubicación actual cuando se llama al usuario. En segundo lugar, el usuario podría preferir unos dominios administrativos a otros, por ejemplo porque el servicio sea más barato o porque existan acuerdos de servicio entre el proveedor de servicio de base y otros proveedores de servicio.

El dominio administrativo de base se identifica sea por un identificador de dominio administrativo explícito, sea porque su identidad se deduce de la identidad de usuario (por ejemplo en caso de números e164 jerárquicos o direcciones de alias de tipo identificador de correo electrónico).

A los efectos de esta Recomendación se deben cumplir los siguientes requisitos:

- Cada dominio administrativo será identificable por una identidad de dominio administrativo.
- Será posible deducir la identidad del dominio de base a partir de todas las identidades del usuario utilizadas a nivel mundial. Las identidades de usuario utilizadas localmente no tienen que contener la información sobre el dominio de base.

5.2.3.4 Identificación de la zona

La identificación de la zona (es decir del controlador de acceso) puede ser necesaria si el usuario prefiere ciertas zonas (del mismo dominio administrativo) a otras. En este caso, la identidad de la zona y del controlador de acceso deben conocerse antes de que el usuario (y el terminal) se inscriban en la zona.

A los efectos de esta Recomendación se deben cumplir los siguientes requisitos:

- Será posible configurar una o más zonas o controladores de acceso como las zonas de base o los GK de base de un usuario. La información sobre la zona de base y los GK de base debe incluirse en el perfil de servicio del usuario.
- El terminal móvil H.323 podrá identificar al controlador de acceso respondiéndole durante el procedimiento de descubrimiento del controlador de acceso, y tomar decisiones sobre la zona en la que desea registrarse sobre la base de esa información y del perfil de servicio de usuario.

5.3 Procedimientos requerido para la gestión de la movilidad

Para la gestión de la movilidad H.323 deben estar soportados los siguientes procedimientos:

- Mecanismo de descubrimiento de controlador de acceso para identificar y elegir el dominio administrativo deseado o la zona preferida.
- Actualización de la ubicación cuando el usuario/terminal móvil se registra o desregistra, o cambia el punto de conexión de red.

  NOTA – El término "desregistro" se utiliza para designar el procedimiento a nivel de usuario de terminar el estado en línea. En los procedimientos de protocolo H.510 que se indican a continuación se utiliza asimismo el término "desregistro" conforme a la terminología H.323/H.225.0.
- Autenticación mutual del terminal/usuario y de la red.
- Compartición del perfil de servicio de usuario entre el dominio de base y el GK (visitado), si es necesario.
- Autorización de peticiones de servicio (por ejemplo para una llamada saliente) atendiendo al perfil de servicio de usuario.
- Localización del terminal/usuario móvil para llamadas entrantes.

5.4 Procedimientos requeridos para proveer y configurar entidades móviles H.323

Estos procesos están fuera del ámbito de la presente Recomendación.

6 Arquitectura para la movilidad H.323

6.1 Modelo de arquitectura

La figura 1 presenta la arquitectura funcional y puntos de referencia para la gestión de la movilidad en sistemas H.323, sobre la base de la arquitectura funcional de H.225.0 anexo G. Otras entidades funcionales (VLF, HLF, AuF) están combinadas con elementos H.323 existentes – controladores de acceso, elementos de frontera – o representan elementos externos con respecto a la actual H.323. En este último caso, mostrado en la figura 1, pueden considerarse como servicios de extremo de fondo, en cuyo caso los enlaces entre ellas y entidades H.323 existentes representan ejemplares del punto de referencia D. Las líneas gruesas indican los enlaces que están dentro del ámbito de esta Recomendación.

Los puntos de referencia entre elementos dentro del grupo de servicios de extremo de fondo, los cuales no forman parte de la actual arquitectura H.323, están fuera del ámbito de esta Recomendación. Esto se indica por el uso de líneas discontinuas para la representación de los enlaces.

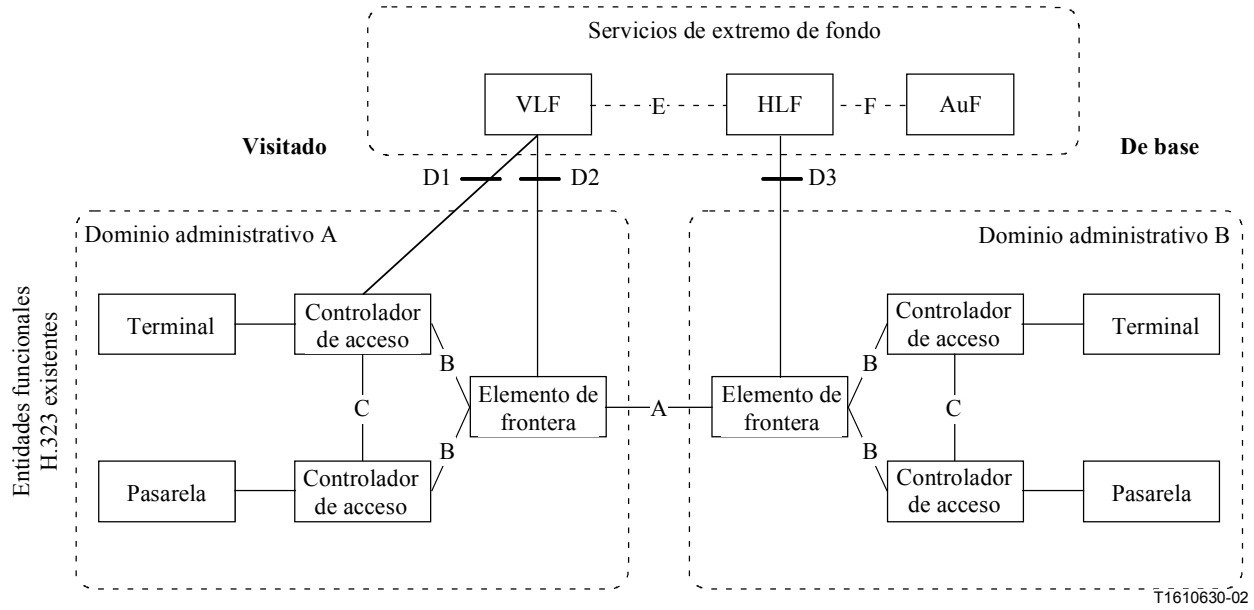


Figura 1/H.510 – Diagrama de arquitectura funcional con puntos de referencia

6.2 Entidades funcionales

6.2.1 Entidades especificas de la movilidad

Las funciones HLF, VLF y AUF se definen en otras Recomendaciones. A efectos de la presente Recomendación, pueden describirse como sigue:

- La HLF representa el banco de datos de base que almacena los datos (de abono) permanentes de un usuario/terminal móvil así como la ubicación actual (mediante un puntero hacia una VLF) si el usuario/terminal está en línea. Esta entidad funcional siempre está asociada con el dominio de base.
- La VLF representa un banco de datos para el almacenamiento temporal de datos relacionados con un usuario/terminal visitante, incluyendo un puntero hacia el controlador de acceso en el que el usuario/terminal está registrado en cada momento y un puntero hacia HLF. Esta entidad funcional está asociada con el dominio sirviente (de base o visitado).
- La AuF se encarga de la autenticación de un usuario/terminal móvil ante el dominio sirviente (de base o visitado). Siempre está asociada con la HLF del usuario (terminal móvil, y por tanto con el dominio de base.

Una VLF puede estar asociada con un controlador de acceso o con múltiples controladores de acceso siempre que todos los controladores de acceso pertenezcan al mismo dominio administrativo, es decir, que el límite superior del área de servicio de una VLF sea el dominio administrativo. Lo mismo es aplicable a la HLF/AuF aunque puede haber un menor número de HLF/AuF que de VLF.

6.2.2 Terminal móvil H.323

Además de la funcionalidad terminal H.323 normalizado, un terminal H.323 móvil soporta:

– la asociación con cualquier usuario móvil autorizado;

– la adopción de un perfil de servicio de usuario móvil;

– el cambio dinámico de la red y/o del punto de conexión H.323.

NOTA – En este contexto, "dinámico" significa que el sistema H.323 trata automáticamente las actualizaciones de ubicación sin necesidad de una intervención administrativa. No significa que las llamadas existentes se mantengan cuando se producen cambios de ubicación (es decir, el traspaso no está soportado en esta versión de la Recomendación).

6.2.3 Controlador de acceso y elemento de frontera

Un terminal móvil H.323 está controlado por un GK de base cuando se desplaza dentro del dominio de base, y en otro caso por el GK visitado. En este último caso la comunicación puede implicar asimismo elementos de frontera en ambos dominios administrativos, el de base y el visitado.

El GK contiene también la información necesaria para tratar las llamadas iniciadas o recibidas por el terminal móvil registrado en dicho controlador de acceso (por ejemplo información de servicio suplementario recibida de la HLF, pero para algunos servicios suplementarios el GK puede necesitar obtener información adicional de la HLF).

Los controladores de acceso y los elementos de frontera tienen que soportar la comunicación con las entidades funcionales indicadas en 6.2.1 a menos que estas funciones estén integradas con el controlador de acceso o el elemento de frontera. Para más detalle, véase 6.3.

6.3 Puntos de referencia

Esta Recomendación trata las siguientes relaciones lógicas de señalización entre:

1) GK y BE a través del punto de referencia B.
2) GK y VLF a través del punto de referencia D1.
3) VLF y HLF a través del punto de referencia E (fuera del ámbito de esta Recomendación).
4) HLF y AuF a través del punto de referencia F (fuera del ámbito de esta Recomendación).
5) VLF y BE a través del punto de referencia D2 y entre HLF y BE a través del punto de referencia D3.
6) Dos BE a través del punto de referencia A.

Los protocolos de señalización para la gestión de la movilidad a través de las interfaces existentes en la Rec. UIT-T H.323 son los protocolos definidos en las Recomendaciones UIT-T H.225.0 (RAS, Q.931), H.245 y H.501.

Puesto que las entidades funcionales HLF, VLF y AuF pueden coexistir, en un mismo elemento de red, con un controlador de acceso o con un elemento de frontera, los puntos de referencia pueden ser internos a estos elementos de red. La figura 2 ilustra un ejemplo de esta situación con dos elementos de red compuestos: un BE situado con el controlador de acceso y la VLF (designado por controlador de acceso/VLF/BE) y la HLF así como la AuF con otro elemento de frontera (designado por elemento de frontera/HLF/AuF).

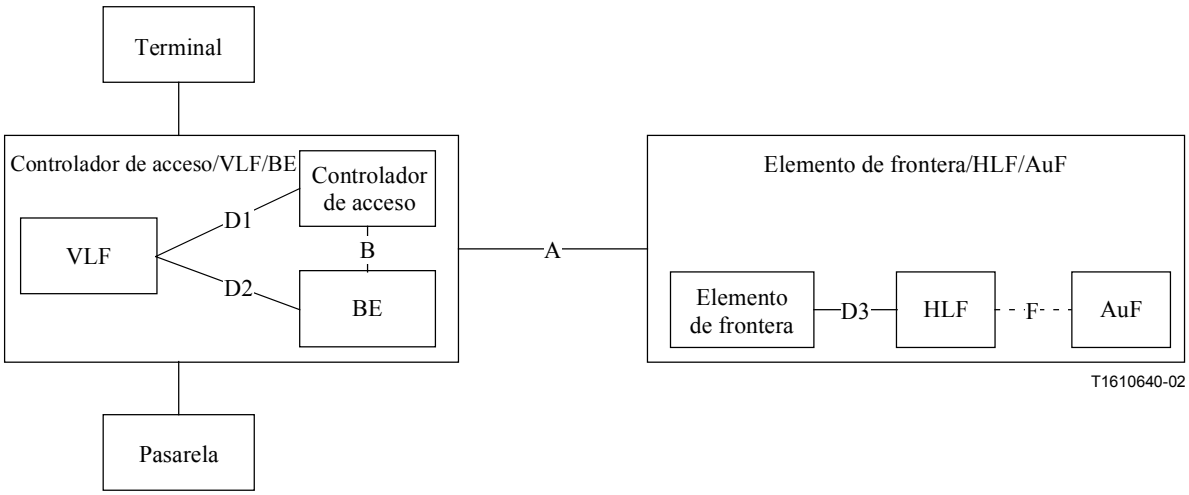


Figura 2/H.510 – Ejemplo de elementos de red compuestos

7 Procedimientos de gestión de la movilidad

7.1 Consideraciones generales sobre los procedimientos de gestión de la movilidad

Esta cláusula describe los procedimientos para proporcionar las funciones de gestión de la movilidad en sistemas H.323. Los procedimientos se presentan en forma de diagramas de flujo de información (o diagramas de secuencia de mensajes) con explicaciones adicionales.

Los procedimientos de gestión de la movilidad tienen tres partes principales:

- **Procedimientos de anuncio de espacio de dirección HLF**: procedimientos que deben aplicarse antes de que los usuarios asociados con una HLF puedan ser contactados. Estos procedimientos se aplican entre las HLF y los BE/GK para anunciar las identidades de usuario para las cuales la ubicación de usuarios con estas identidades se puede determinar contactando la HLF.
- **Procedimientos de actualización de la ubicación**: procedimientos que es necesario aplicar cuando un usuario móvil, que utiliza un terminal H.323, cambia el punto de conexión H.323 (la zona) o el punto de conexión de red (la dirección de red), o cuando el usuario accede al sistema por primera vez después de un periodo de ausencia (es decir, cuando no hay información de ubicación actual sobre el usuario almacenada en la HLF asociada). Estos procedimientos incluyen el descubrimiento de controlador de acceso y los procedimientos de registro y desregistro.

  NOTA – Cómo el terminal descubre que ha cambiado el punto de conexión de red es una cuestión de implementación que está fuera del ámbito de esta Recomendación. Por ejemplo, la pila IP en el terminal informa a la aplicación del terminal sobre el cambio de la dirección IP.
- **Procedimientos de gestión de la movilidad relacionados con la llamada**: procedimientos que deben aplicarse cuando se establece una comunicación hacia o desde un usuario móvil utilizando un terminal H.323. Estos procedimientos de gestión de la movilidad incluyen el intercambio de la información necesaria para localizar al usuario a que se está llamando.

Los procedimientos de gestión de la movilidad no prevén el caso de la movilidad continua del terminal, es decir, los traspasos. Los procedimientos de traspaso no forman parte de la versión 1 de esta Recomendación.

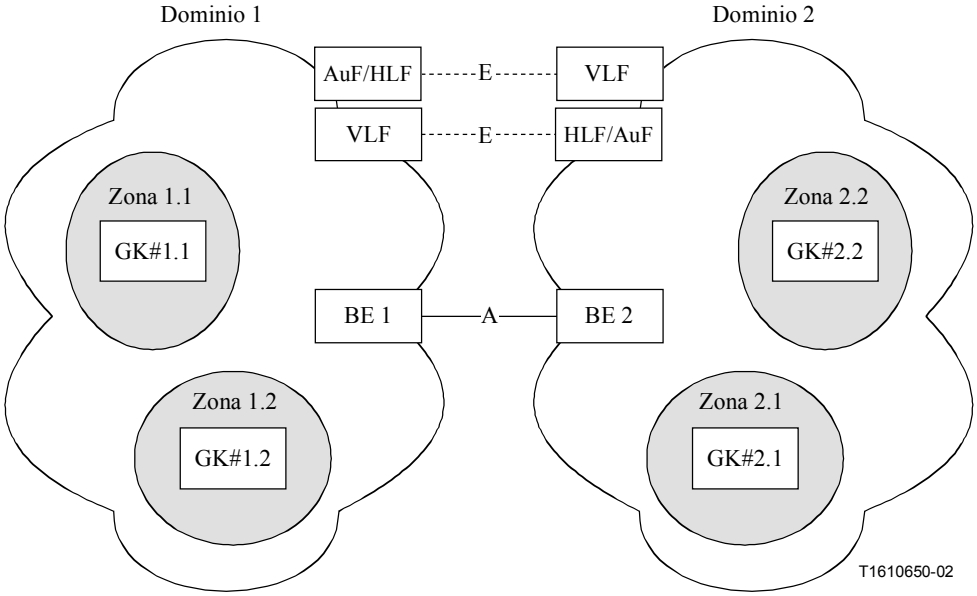
7.2 Ejemplo de escenarios para procedimientos de gestión de la movilidad

Para ilustrar las diversas posibilidades de cambios de ubicación, la figura 3 muestra un ejemplo de dos dominios, cada uno de los cuales comprende dos zonas:

Pueden distinguirse los siguientes escenarios de cambio de ubicación:

1) Intrazona dentro del dominio de base, por ejemplo un usuario/terminal perteneciente al dominio 1 cambia su ubicación actual dentro de la zona 1.1 a otra ubicación dentro de la misma zona.
2) Intrazona dentro del dominio visitado, por ejemplo un usuario/terminal perteneciente al dominio 1 cambia su ubicación actual dentro de la zona 2.1 a otra ubicación dentro de la misma zona.
3) Interzona dentro del dominio de base, por ejemplo un usuario/terminal perteneciente al dominio 1 cambia su ubicación actual dentro de la zona 1.1 a otra ubicación dentro de la zona 1.2.
4) Intrazona dentro del dominio visitado, por ejemplo un usuario/terminal perteneciente al dominio 1 cambia su ubicación actual dentro de la zona 2.1 a otra ubicación dentro de la zona 2.2.
5) Interdominio, por ejemplo un usuario/terminal perteneciente al dominio 1 cambia su ubicación actual de la zona 1.1 a la zona 2.2.

Los procedimientos descritos en las cláusulas siguientes tienen en cuenta el escenario 5), que es el más general. Los otros escenarios pueden obtenerse a partir del escenario 5) omitiendo ciertos pasos en el procedimiento.



NOTA – Por razones de simplicidad, no se han representado enlaces dentro de los dominios; para esos enlaces, véase la figura 1.

Figura 3/H.510 – Modelo de escenarios

7.3 Procedimientos de anuncio de espacio de dirección HLF

7.3.1 Disposición estática

En una disposición estática, los GK y BE están configurados con las direcciones de las HLF que contactarán para resolver identidades de usuario llamables o primarias. La gama de las posibles identidades de usuario y las HLF asociadas se ponen en conocimiento del GK o BE mediante

configuración o administración. La HLF adecuada se selecciona atendiendo al contenido de la entidad de usuario presente.

Los procedimientos para configurar o actualizar los GK y BE en una disposición estática están fuera del ámbito de esta Recomendación.

7.3.2 Disposición dinámica

En una disposición dinámica, los GK y BE obtienen dinámicamente el conocimiento sobre las identidades de usuario y las HLF asociadas, por medio de un protocolo. Las HLF utilizarán los procedimientos y mensajes descritos en la Rec. UIT-T H.501 para anunciar las identidades de usuario contenidas en su base de datos, es decir, su espacio de dirección, a los GK y BE.

Los GK y BE enviarán mensajes **DescriptorIDRequest** y **DescriptorRequest** a las HLF para obtener información sobre el espacio de dirección de las HLF, y las HLF responderán a estas indagaciones con mensajes **DescriptorIDConfirmation** y **DescriptorConfirmation**, respectivamente, para anunciar sus espacios de dirección. Las HLF deben también enviar mensajes **DescriptorUpdate** a los GK/BE cuando se produzca un cambio en su espacio de dirección. Los GK/BE y las HLF pueden establecer una relación de servicio utilizando mensajes **ServiceRequest** y **ServiceConfirmation** descritos en la Rec. UIT-T H.501, previamente a cualquier otra comunicación con cada uno de los demás.

Gracias a la información obtenida con estos mensajes, los GK y BE pueden deducir, de las identidades de los usuarios móviles, la HLF adecuada para contactar cada usuario móvil.

7.3.3 Patrones de dirección

Según la Rec. UIT-T H.501, los descriptores pueden contener direcciones de alias en los formatos de correo electrónico y de número de parte (en forma de un número e164 internacional, por defecto). Por acuerdo entre los dominios que intervienen pueden estar soportados otros formatos de direcciones de alias, por ejemplo los formatos de un plan de numeración privado. Los formatos de identidades de usuario móvil (como IMSI) requerirán, de todas formas, un acuerdo de este tipo.

Los GK, BE y HLF conformes a esta Recomendación soportarán identidades de usuario en forma de direcciones de alias, como se especifica en la Rec. UIT-T H.225.0 (tipo ASN.1 *AliasAddress*), de los siguientes formatos:

- **Identidades de usuario llamables**: una dirección de correo electrónico (tipo *AliasAddress.email-ID*) o un número e164 (internacional) (tipo *AliasAddress.partyNumber.e164Number*), o facultativamente un número de parte privado (calificado completamente) (tipo *AliasAddress.partyNumber.privateNumber*).
- **Identidades de usuario primarias**: una de las identidades de usuario llamables, o un Identificador de acceso a la red (NAI, véase RFC 2486), o una identidad de usuario móvil mundial (tipo *AliasAddress.mobileUIM*), que contiene por ejemplo un IMSI. El NAI es de tipo *AliasAddress.email-ID* incluso si no representa una dirección de correo electrónico llamable.

Otros formatos e identificadores quedan en estudio.

Los procedimientos no distinguen entre identidades de usuario llamables y primarias. Tales procedimientos quedan en estudio.

7.4 Procedimientos de actualización de ubicación

Se aplican procedimientos de actualización cuando:

– un terminal móvil H.323 (re)inicia una operación;

– un terminal móvil H.323 se desplaza a una nueva ubicación;

– un usuario móvil comienza una sesión con (*logs onto*) un determinado terminal móvil H.323.

Los procedimientos de actualización de ubicación utilizan procedimientos RAS H.225.0: descubrimiento de controlador de acceso, registro y desregistro.

7.4.1 Descubrimiento de controlador de acceso

7.4.1.1 Consideraciones generales

Desde el punto de vista del sistema H.323, el procedimiento de descubrimiento de controlador de acceso es el primer procedimiento que aplica el terminal móvil H.323 cuando se necesita una actualización de ubicación. La única excepción es una actualización de ubicación intrazona, en la que se puede omitir el descubrimiento de controlador de acceso ya que el terminal móvil H.323 permanece registrado en el mismo controlador de acceso en que estaba registrado antes.

Un terminal móvil H.323 iniciará el procedimiento de descubrimiento de controlador de acceso cuando se presenta uno o más de los siguientes eventos o situaciones:

- El terminal móvil H.323 ha ganado acceso a la red subyacente a través de un nuevo punto de conexión de red. Por ejemplo, el terminal ha obtenido una dirección IP de un servidor DHCP. Esta situación incluye el arranque del terminal móvil H.323 así como el caso en que el terminal móvil H.323 cambia su NPoA en el curso de la operación.
- El terminal móvil H.323 ha perdido la conexión con el controlador de acceso en el que estaba previamente registrado. la pérdida puede haberse producido paulatinamente cuando el controlador de acceso envía un mensaje URQ al terminal móvil H.323, o bruscamente por ejemplo por fallo del enlace en el trayecto de comunicación entre el terminal móvil H.323 y el controlador de acceso.
- Una petición de registro fracasa por el motivo *discoveryRequired*.

Hay varios métodos para ejecutar el procedimiento de descubrimiento de controlador de acceso, los cuales dependen de las capacidades de la red subyacente (por ejemplo, de que la red soporte o no la multidifusión) y de la parte del sistema H.323 a que se gane acceso. A continuación se indican los métodos que pueden ser utilizados por los terminales móviles H.323. Un terminal móvil H.323 puede aplicar uno, varios o todos estos métodos, con el orden de preferencia configurado en el terminal móvil H.323:

1) Mensaje GRQ multidifusión.
2) Mensaje GRQ unidifusión a un controlador de acceso, cuya dirección ha sido previamente introducida en una memoria cache o almacenada de otra forma.
3) Interrogación SRV en el gk_domain (IV.1.1/H.225.0).
4) Interrogación del registro TXT en el gk_domain (IV.1.1/H.225.0).
5) Interrogación del registro "A" en el gk_domain.
6) Descubrimiento manual (7.2.1/H.323).

Los métodos 3 a 5 utilizan el sistema de nombres de dominio (DNS, *domain name system*). El descubrimiento manual está fuera del ámbito de esta Recomendación.

7.4.1.2 Descubrimiento de un controlador de acceso sirviente

El controlador de acceso sirviente será un controlador de acceso de base mientras un terminal móvil H.323 se desplaza dentro de su dominio de base; en otro caso será un controlador de acceso visitado. Todos los métodos indicados en 7.4.1.1 retornarán la dirección o direcciones de uno o más controladores de acceso, si tiene éxito.

Si la dirección del controlador de acceso se encontró utilizando uno de los métodos 3 a 5, el terminal móvil H.323 enviará un mensaje GRQ (unidifusión) a ese controlador de acceso. Si la

dirección del controlador de acceso se encontró utilizando el método 1 ó 2, el terminal móvil H.323 intentará registrarse en uno de los controladores de acceso, como se describe en 7.4.2.

Si un controlador de acceso recibe un mensaje GRQ (unidifusión) ejecutará una de estas dos acciones:

1) Enviará un GCF si llega a ser el controlador de acceso sirviente y permitirá que el terminal se inscriba.

2) Enviará un GRJ con o sin una lista de otros controladores de acceso.

Según la respuesta que reciba del controlador de acceso, el terminal ejecutará una de estas tres acciones:

1) Si el controlador de acceso respondió con un GCF, el terminal móvil H.323 intentará inscribirse en el controlador de acceso como se describe en 7.4.2.

2) Si el controlador de acceso respondió con un GRJ, el terminal móvil H.323 recorrerá la lista en sentido descendente y comenzará enviando un GRQ al controlador de acceso de más alto nivel de prioridad.

3) Si el controlador de acceso respondió con un GRJ pero no incluyó una lista con otros controladores de acceso, el terminal móvil H.323 deberá utilizar la lista de otros controladores de acceso que pueda haber recibido anteriormente. Si el terminal móvil H.323 no tiene ninguna lista de otros controladores de acceso, no podrá descubrir un controlador de acceso para inscribirse.

7.4.2 Registro

Un terminal móvil H.323 aplicará el procedimiento de registro si ha ocurrido alguno de los siguientes eventos. El terminal deberá disponer ya de la información sobre el controlador de acceso al que le va a enviar la petición de registro.

- El terminal (re)aparece en una zona (por ejemplo, tras la energización). En este caso el descubrimiento del controlador de acceso debe efectuarse antes de comenzar el registro. Véase 7.4.1.
- Un nuevo usuario comienza a utilizar el terminal. Si el terminal ya está registrado no es necesario el descubrimiento del controlador de acceso. Si todavía está registrado un usuario anterior y el terminal acepta el nuevo usuario, el nuevo registro reemplaza al anterior, y el controlador de acceso efectúa el desregistro del anterior usuario (véase 7.4.3).
- El terminal se ha desplazado a otro NPoA diferente de aquél en que estaba registrado. Se requerirá el descubrimiento del controlador de acceso (véase 7.4.1) antes del registro, a menos que se sepa que el nuevo NPoA pertenece a la zona del anterior controlador de acceso (cambio de ubicación intrazona).
- Siempre que un terminal se desplaza a una nueva zona sin que esté participando en una llamada (aunque no cambie el NPoA).
- Cuando ha quedado sin efecto el anterior registro (por ejemplo, por haber expirado el tiempo de vida del registro). Esto puede detectarlo por ejemplo el controlador de acceso que ha respondido a un ARQ con un ARJ que indica que el terminal móvil no está registrado. Si se conoce otro controlador de acceso (por ejemplo, por un mensaje ARJ), se puede intentar el registro en este otro controlador de acceso; de no ser así, hay que realizar primero el descubrimiento del controlador de acceso (véase 7.4.1).
- Como una indicación de "mantenerse vivo" (registro ligero, véase la Rec. UIT-T H.225.0), para prolongar el tiempo de vida del registro actual.

7.4.3 Desregistro

El procedimiento de desregistro tiene por objeto suprimir el registro de un usuario o de un terminal móvil H.323 en un controlador de acceso. Si el terminal también tiene su propia dirección de alias, por ejemplo un ID de terminal, su registro también se suprime cuando se efectúa el desregistro de un usuario. Si un terminal móvil H.323 es desregistrado, el usuario que está usando el terminal en ese momento queda también desregistrado. Un terminal móvil H.323 debe efectuar un desregistro si ocurre uno o más de estos eventos o situaciones:

- Se cierra la aplicación del terminal móvil H.323.
- Un usuario que está utilizando el terminal desea desregistrarse del sistema H.323.
- El terminal móvil H.323 va a suprimir su conexión a través del actual NPoA con el controlador de acceso en el que está registrado pero no se conectará inmediatamente con algún controlador de acceso a través de otro NPoA.

  Si el terminal móvil H.323 cambia su ubicación de tal manera que se conectará con el sistema H.323 a través de un nuevo NPoA inmediatamente después de desconectarse del antiguo NPoA, el terminal móvil H.323 no tiene necesidad de desregistrar porque el desregistro se efectuará implícitamente dentro del procedimiento de actualización de la ubicación.
- El controlador de acceso, la VLF o la HLF solicitan el desregistro de un usuario del terminal móvil H.323, por ejemplo si expira el tiempo de vida del registro.

7.4.4 Flujos de información para los procedimientos de actualización de ubicación

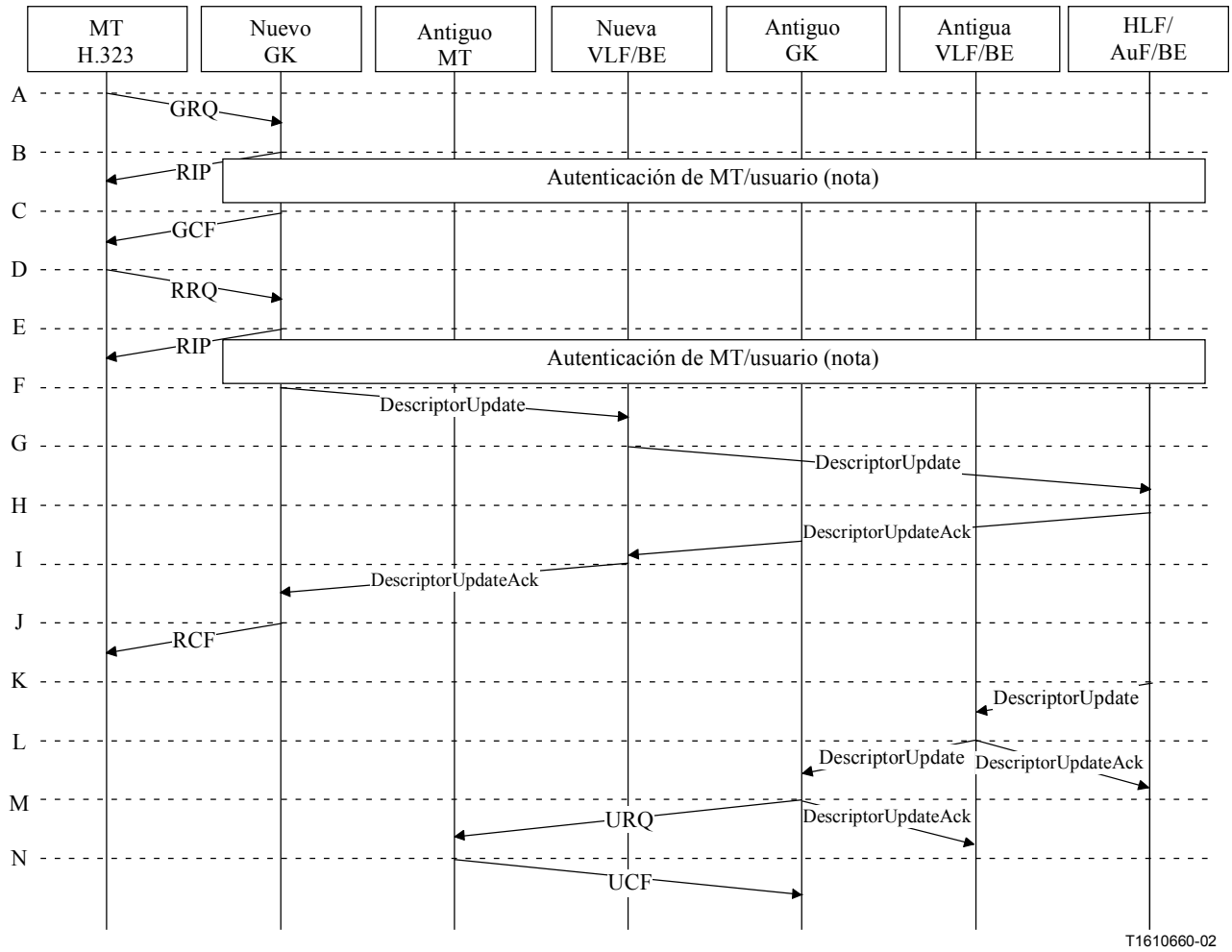
La figura 4 muestra el flujo de información completo para el procedimiento de actualización de ubicación. Se aplica el flujo completo cuando el terminal móvil H.323 cambia su ubicación de un dominio visitado a otro. En este caso, el antiguo controlador de acceso y la antigua VLF mantienen información sobre el usuario que está utilizando ese terminal.

En los siguientes casos sólo se aplican partes del flujo completo, como se indica en la descripción detallada que se presenta a continuación en la figura 4:

– El terminal móvil H.323 cambia su ubicación (por ejemplo el NPoA) dentro de la misma zona (no es necesario el descubrimiento del controlador de acceso y no cambia la información en la VLF y/o HLF).

– El terminal móvil H.323 cambia de zona dentro del mismo dominio visitado (la VLF antigua y la nueva son las mismas, la información en la HLF no cambia).

– El terminal móvil H.323 (o un usuario móvil) se registra por primera vez después de haberse desregistrado anteriormente (no es necesario suprimir la anterior información de ubicación en la antigua VLF y/o GK).



NOTA – La autenticación se efectuará una sola vez, en el paso B o en el paso E.

Figura 4/H.510 – Flujo de información en el procedimiento de actualización de ubicación

A continuación se explica el significado de los pasos indicados en la figura 4.

Los pasos A-C no se necesitan cuando se cambia la ubicación (el NPoA) dentro de la misma zona, o en el caso de registro para mantener vivo.

A: Se cumplieron las condiciones para iniciar los procedimientos de actualización de ubicación con descubrimiento de controlador de acceso, por lo que el terminal móvil H.323 envía un mensaje GRQ al controlador de acceso. El mensaje GRQ incluirá en el campo *endpointAlias* todas las identidades de usuario (incluso la identidad de usuario primaria) que pueden utilizarse para identificar al usuario.

B: Por lo general, la autenticación se efectúa una sola vez en el curso de la actualización de la ubicación, es decir, se aplica el paso B o el paso E. Si el controlador de acceso autentica al usuario en este punto, efectuará la autenticación como se especifica en la Rec. UIT-T H.530. Se puede retornar al terminal móvil H.323 un mensaje RIP como una indicación de un posible retardo en la respuesta a GRQ.

Si el controlador de acceso no acepta esta petición del usuario, enviará un GRJ al terminal móvil H.323.

C: El controlador de acceso retorna GCF al terminal móvil H.323 para indicarle que aceptará el registro. Si se efectuó el paso B, el mensaje GCF contendrá la información de autenticación que utilizará el terminal móvil para el RRQ siguiente.

D: El terminal móvil H.323 envía un mensaje de petición de registro (RRQ) al controlador de acceso (ya conocido). A menos que se trate de un registro para mantener vivo, el mensaje

RRQ incluirá en el campo *terminalAlias* todas las identidades de usuario (incluso la identidad de usuario primaria) que pueden utilizarse para identificar al usuario y fueron indicadas por el usuario.

E: Por lo general, la autenticación se efectúa una sola vez en el curso de la actualización de la ubicación, es decir, se aplica el paso B o el paso E. Si el controlador de acceso autentica al usuario en este punto, efectuará la autenticación como se especifica en la Rec. UIT-T H.530. Se puede retornar al terminal móvil H.323 un mensaje RIP como una indicación de un posible retardo en la respuesta a RRQ.

Si el controlador de acceso no acepta esta petición del usuario, enviará un RRJ al terminal móvil H.323.

F: Si el terminal móvil H.323 y el usuario que lo está utilizando ya están registrados, el controlador de acceso actualiza el registro y continúa en el paso J. Se da este caso si el terminal móvil H.323 cambia el NPoA dentro de la zona o si se renueva el anterior registro (por ejemplo como un mecanismo periódico de mantener vivo.

Si el controlador de acceso observa que el usuario no está ya registrado, envía un mensaje **DescriptorUpdate** a la VLF/BE con la que está asociado (tras una autenticación exitosa).

El mensaje **DescriptorUpdate** incluirá la dirección TSAP del controlador de acceso como una *aliasAddress* en el campo *sender* del mensaje y el campo *updateInfo* que contiene un descriptor con un nuevo *descriptorID* en el campo *descriptorInfo* y el *updateType* fijado a *added*. En el campo *templates*, cada *descriptor* incluirá como patrones específicos todas las identidades de usuario (incluso la identidad de usuario primaria) que habrán de ser registradas, junto con *sendSetup* como el *messageType* del campo *routeInfo*. El descriptor puede también incluir el *gatekeeperID* del GK que envió el mensaje **DescriptorUpdate**. El controlador de acceso también almacena la dirección del NPoA a través del cual el terminal móvil H.323 se conecta al controlador de acceso.

G: Al recibir el mensaje **DescriptorUpdate**, la VLF/BE cotejará cada *descriptor* con los ya almacenados en anteriores actualizaciones de la ubicación. Si el usuario ya estaba registrado en la VLF/BE, la VLF/BE actuará como se describe en el paso I más adelante. En este caso la VLF/BE antigua y la nueva son las mismas. Además, la VLF/BE enviará un mensaje **DescriptorUpdate** al antiguo controlador de acceso, como se describirá en el paso L.

La VLF/BE cambiará el campo *messageType* por *sendAccessRequest* y el campo *sender* por la dirección TSAP de la propia VLF/BE. Si el *gatekeeperID* estaba presente en el *descriptor* enviado por el GK, la VLF/BE puede suprimirlo del mensaje, antes de hacerlo seguir. Por último, la VLF/BE deduce la dirección TSAP de la HLF/BE del usuario a partir de la identidad de usuario primaria contenida en el *descriptor*, y envía el mensaje **DescriptorUpdate** a la HLF/BE.

H: La HLF/BE almacena la dirección TSAP de la VLF/BE como información de ubicación sobre el usuario indicado por la identidad de usuario primaria en el mensaje **DescriptorUpdate** y envía un mensaje **DescriptorUpdateAck** como respuesta a la VLF/BE.

I: La VLF/BE almacena todas la identidades de usuario que recibe, la dirección TSAP de la HLF/BE del usuario, y la dirección TSAP del controlador de acceso, que recibió en el paso G, como la información de ubicación sobre ese usuario, y envía un mensaje **DescriptorUpdateAck** al controlador de acceso.

J: El controlador de acceso almacena el NPoA así como todas las identidades de usuario que recibió del terminal móvil H.323 en el mensaje RRQ en el paso D. El controlador de acceso enviará un mensaje RCF al terminal móvil H.323 para indicar que la actualización de la ubicación tuvo éxito.

Los pasos K a M sólo se ejecutan si en la HLF/BE y en el GK (precedente) y en la VLF/BE (si existía) se disponía de la previa información de ubicación sobre el usuario antes de ejecutar el paso G.

K: La HLF/BE puede ejecutar este paso inmediatamente después del paso H, para asegurar una actualización oportuna de la información de ubicación a través de la red. La HLF/BE enviará un mensaje **DescriptorUpdate** a la antigua VLF/BE. El mensaje incluirá la dirección TSAP de la propia HLF/BE en el campo *sender* y *updateInfo* que contiene un *descriptor* con el *descriptorID* del registro original y todas las identidades de usuario registradas, del usuario, como patrones específicos, *nonExistent* como el *messageType* del campo *routeInfo* y el *updateType* fijado a *deleted*.

L: La VLF/BE suprimirá la anterior información de ubicación indicada por el *descriptor* (es decir, la dirección TSAP del antiguo controlador de acceso y todas las identidades de usuario almacenadas) y enviará un mensaje **DescriptorUpdate**, como se describió en el paso K, al antiguo controlador de acceso (con el campo *sender* fijado a la dirección TSAP de la propia VLF/BE). La VLF/BE también responderá a la HLF/BE con un mensaje **DescriptorUpdateAck**.

M: El antiguo controlador de acceso suprimirá la información de ubicación (es decir, la relativa al NPoA) así como otras informaciones de registro que ha estado manteniendo sobre el usuario indicado por el *descriptorID* o el *descriptor*, y responderá a la VLF/BE con un mensaje **DescriptorUpdateAck**. Deberá también enviar un mensaje URQ al anterior terminal móvil H.323.

N: El anterior terminal móvil H.323 responde al URQ con UCF y suprime sus datos de registro, si existen.

La siguiente lista contiene un resumen del contenido de los mensaje que ofrecen interés para esta Recomendación (en el caso de mensajes o campos de mensajes no indicados aquí, el mensaje o campo de mensaje deberá utilizarse como se indica en las Recomendaciones UIT-T H.323, H.225.0 o H.501):

GRQ

Campo	Descripción
endpointAlias	Todas las identidades de usuario disponibles del usuario que se va a registrar (puede ser el usuario por defecto)

RRQ

Campo	Descripción
terminalAlias	Todas las identidades de usuario disponibles del usuario que se va a registrar

DescriptorUpdate

Campo	Descripción
sender	La dirección TSAP de la entidad que envía el mensaje.
updateInfo	
descriptorInfo	
descriptor	
descriptorInfo	
descriptorID	nuevo identificador asignado a este registro (si updateType = added) identificador asignado en el momento del registro (si updateType = deleted)
templates	
pattern	uno para cada identidad de usuario disponible
specific	la identidad de usuario a registrar
routeInfo	
sendSetup	si enviado de GK a VLF/BE
sendAccessRequest	si enviado de VLF/BE a HLF/BE
nonExistent	si enviado de HLF/BE a VLF/BE/de VLF/BE a GK
gatekeeperID	Facultativamente el ID del GK que envió el mensaje
updateType	
added	en el sentido GK→VLF/BE, VLF/BE→HLF/BE
deleted	en el sentido HLF/BE→VLF/BE, VLF/BE→GK

7.4.5 Desregistro

Un terminal móvil H.323 o un usuario móvil se desregistra siguiendo una petición explícita del usuario, o a petición del GK, VLF o HLF. Como resultado del desregistro se suprime la información de ubicación en la HLF, VLF y GK. En situaciones irregulares, por ejemplo pérdida de la conexión o expiración del tiempo de vida del registro, el GK, VLF o HLF puede también suprimir la información de ubicación sin seguir un procedimiento completo de desregistro.

Las figuras 5 a 8 ilustran el procedimiento de desregistro en los tres casos antes mencionados.

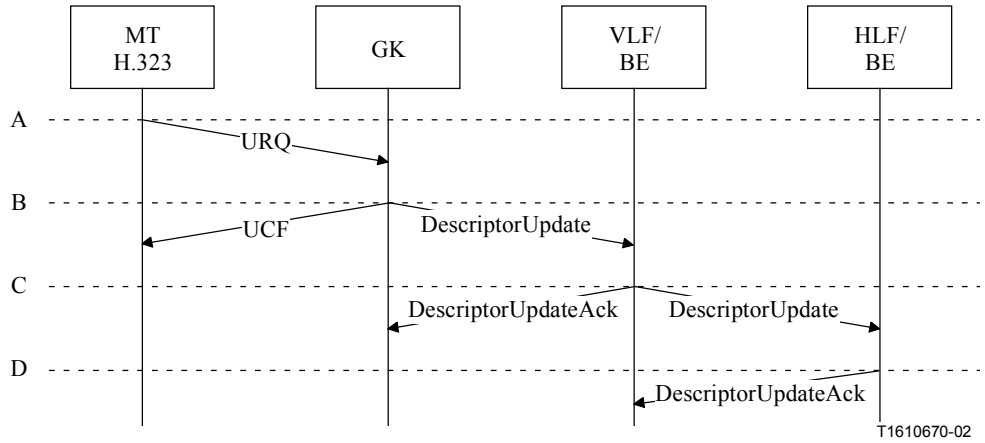


Figura 5/H.510 – Desregistro iniciado por el terminal móvil H.323

La figura 5 ilustra el procedimiento de desregistro iniciado por el terminal móvil H.323. A continuación se presenta una descripción más detallada:

A: El terminal móvil H.323 envía un mensaje URQ al controlador de acceso en el que está registrado. En caso de que el desregistro no sea aplicable por haberse dejado en estudio esta cuestión, el mensaje URQ incluirá todas las identidades registradas para ese usuario en el campo *endpointAlias*. Si el terminal móvil H.323 debe también ser desregistrado, no se deberá incluir ninguna dirección de alias.

B: El controlador de acceso procesará el mensaje URQ en la forma normal, es decir, suprimirá la dirección o direcciones de alias que fueron indicadas en el URQ, y enviará un mensaje **DescriptorUpdate** a la VLF/BE con que está asociado. El mensaje incluirá la dirección TSAP del controlador de acceso en el campo *sender*, el *descriptorID* anteriormente asignado cuando se registró ese usuario, todas las identidades de usuario como patrones específicos y el *updateType* fijado a *deleted*. Si el terminal móvil H.323 se desregistra a sí mismo (es decir, no se limita al desregistro de su usuario actual), el controlador de acceso también suprimirá la información de ubicación (es decir, la relativa al NPoA) utilizada por ese terminal. El controlador de acceso enviará un mensaje UCF al terminal móvil H.323 confirmando el desregistro.

C: La VLF/BE suprimirá la información de ubicación (es decir, la dirección TSAP del controlador de acceso y todas las entidades de usuario registradas) indicada por el *descriptor*, cambiará el campo *sender* del mensaje **DescriptorUpdate** por la dirección TSAP de la VLF/BE y reenviará el mensaje **DescriptorUpdate** a la HLF/BE del usuario. La VLF/BE responderá también al controlador de acceso con un mensaje **DescriptorUpdateAck**.

D: La HLF/BE suprimirá la información de ubicación (es decir, la dirección TSAP de la VLF/BE) que ha almacenado sobre el usuario, indicada por el *descriptor*. La HLF/BE también responderá a la VLF/BE con un mensaje **DescriptorUpdateAck**.

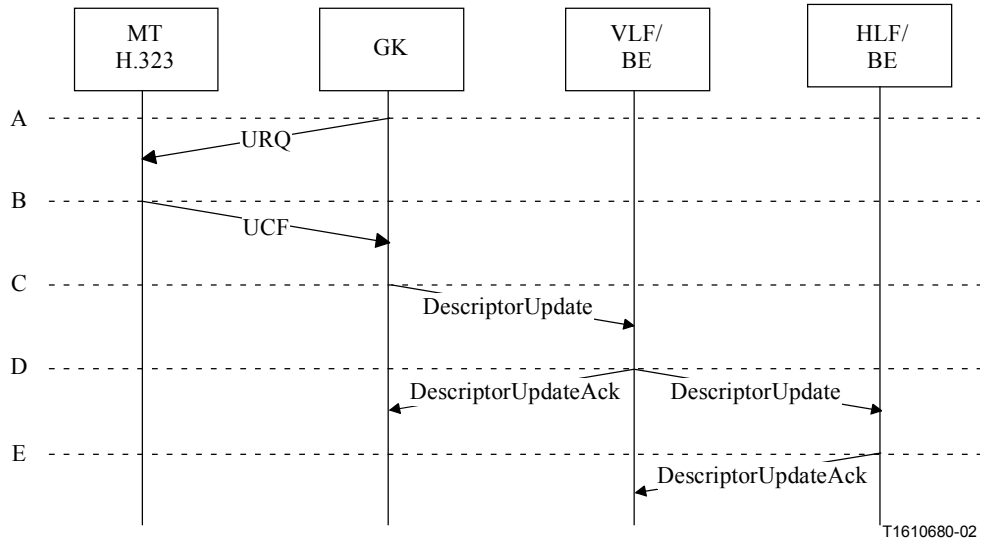


Figura 6/H.510 – Desregistro iniciado por el controlador de acceso

La figura 6 ilustra el procedimiento de desregistro iniciado por el controlador de acceso. A continuación se presenta una descripción más detallada:

A: El controlador de acceso envía un mensaje URQ al terminal móvil H.323 del cual un usuario habrá de ser desregistrado. El mensaje incluirá todas las entidades de usuario registradas en el campo *endpointAlias* si el único que se desregistra es el usuario. Si también se ha de desregistrar el terminal móvil H.323, no se deberá incluir ninguna dirección de alias.

B: El terminal móvil H.323 envía un mensaje UCF al controlador de acceso confirmando el desregistro. El controlador de acceso suprime la información de desregistro relativa al usuario, y si el propio terminal móvil H.323 se desregistra, suprime también el NPoA.

Los pasos C, D, y E son respectivamente iguales a los pasos B, C, D del caso anterior.

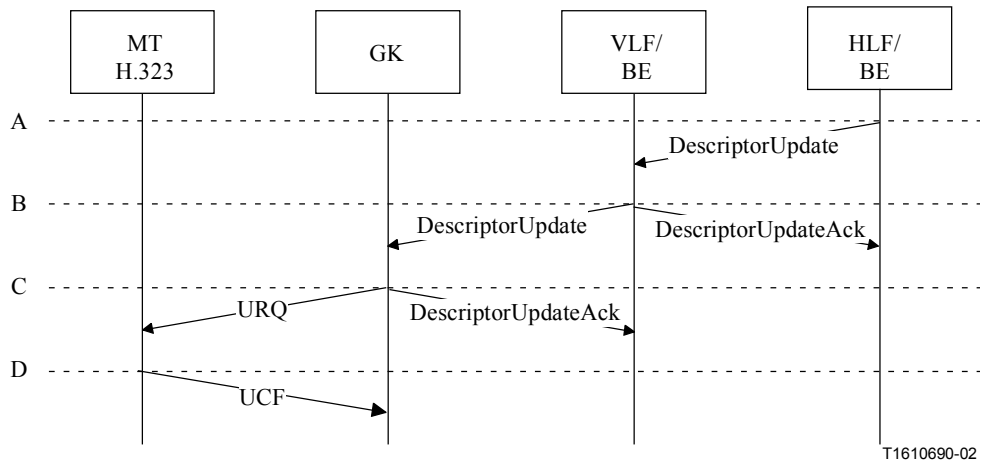


Figura 7/H.510 – Desregistro iniciado por la HLF

La figura 7 ilustra el procedimiento de desregistro iniciado por la HLF. A continuación se presenta una descripción más detallada:

A: La HLF/BE suprime la información de ubicación (es decir, la dirección TSAP de la VLF/BE) que tiene almacenada con relación al usuario y envía un mensaje **DescriptorUpdate** a la VLF/BE que en ese momento mantiene la información de ubicación sobre el usuario. El mensaje incluirá la dirección TSAP de la HLF/BE en el campo *sender*, el *descriptorID* asignado a ese usuario cuando se registró, todas las identidades de usuario registradas como patrones específicos, y el *updateType* fijado a *deleted*.

B: La VLF/BE suprimirá la información de ubicación (es decir, la dirección TSAP del controlador de acceso y todas las identidades de usuario registradas) indicada por el *descriptor*, cambiará el campo *sender* del mensaje **DescriptorUpdate** por la dirección TSAP de la propia VLF/BE y reenviará el mensaje **DescriptorUpdate** al controlador de acceso indicado por la dirección del controlador de acceso que estaba almacenada como la información de ubicación relativa al usuario. La VLF/BE también responderá a la HLF/BE con un mensaje **DescriptorUpdateAck**.

C: El controlador de acceso suprimirá la dirección o direcciones de alias almacenadas para el usuario indicadas por el *descriptor* y enviará un mensaje URQ al terminal móvil H.323. El mensaje URQ incluirá todas las identidades de usuario registradas del usuario que se desregistra. El controlador de acceso también responderá a la VLF/BE con un mensaje **DescriptorUpdateAck**.

D: El terminal móvil H.323 enviará un mensaje UCF al controlador de acceso confirmando el desregistro.

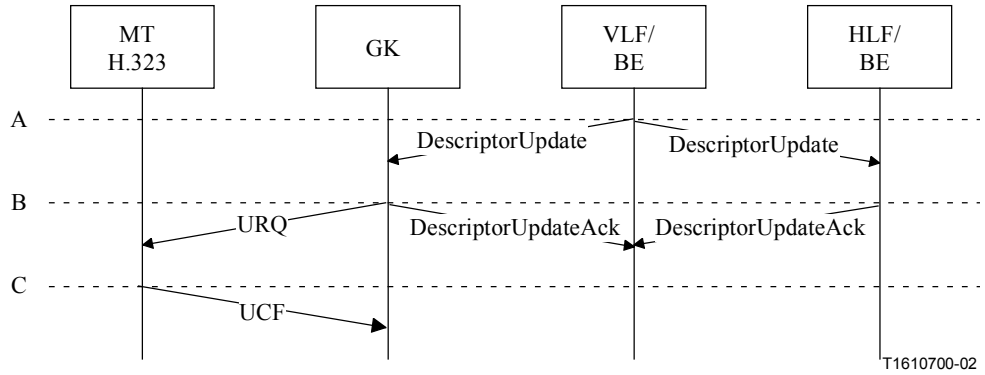


Figura 8/H.510 – Desregistro iniciado por la VLF

La figura 8 ilustra el procedimiento de desregistro iniciado por la VLF. A continuación se presenta una descripción más detallada del procedimiento:

A: La VLF/BE suprime la información de ubicación (es decir, la dirección TSAP del controlador de acceso y todas las identidades de usuario registradas) que tiene almacenada en relación con el usuario, y envía un mensaje **DescriptorUpdate** a la HLF/BE asociada con el usuario y al controlador de acceso en el que el usuario está registrado en ese momento. El mensaje incluirá la dirección TSAP de la VLF/BE en el campo *sender*, el *descriptorID* asignado a ese usuario cuando se registró, todas las identidades de usuario registradas como patrones específicos y el *updateType* fijado a *deleted*.

B: La HLF/BE suprimirá la información de ubicación (es decir, la dirección TSAP de la VLF/BE) relacionada con el usuario indicada por el *descriptor* y responderá a la VLF/BE con un mensaje **DescriptorUpdateAck**.

El controlador de acceso suprimirá la dirección o direcciones de alias almacenadas para el usuario indicadas por el *descriptor* y enviará un mensaje URQ al terminal móvil H.323. El mensaje URQ incluirá todas las identidades de usuario registradas del usuario que se desregistra. El controlador de acceso también responderá a la VLF/BE con un mensaje **DescriptorUpdateAck**.

C: El terminal móvil H.323 enviará un mensaje UCF al controlador de acceso confirmando el desregistro.

La siguiente lista contiene un resumen del contenido de los mensajes que ofrecen interés para esta Recomendación (en el caso de mensajes o campos de mensajes no indicados aquí, el mensaje o campo de mensaje deberá utilizarse como se indica en las Recomendaciones UIT-T H.323, H.225.0 o H.501):

DescriptorUpdate

Campo	Descripción
sender	La dirección TSAP del emisor del mensaje.
updateInfo	
descriptorInfo	
descriptor	
descriptorInfo	
descriptorID	identificador asignado en el momento del registro
templates	
pattern	uno para cada identidad de usuario registrada
specific	identidad de usuario
routeInfo	
nonExistent	
gatekeeperID	Facultativamente el ID del GK que envió el mensaje.
updateType	
deleted	

7.5 Procedimientos de gestión de la movilidad en la fase de establecimiento de comunicación

7.5.1 Principios generales

Esta cláusula describe los flujos de información para los procedimientos de gestión de la movilidad que intervienen en la fase de establecimiento de comunicación. Para el establecimiento de comunicación se aplicarán los procedimientos H.323 normales, es decir, el protocolo RAS y la señalización de control de llamada H.225.0, y H.501. A continuación se indican otros requisitos que también deben cumplirse.

Se distinguen dos casos: llamadas que terminan en un terminal móvil H.323 (tratamiento de llamada entrante), y llamadas originadas por un terminal móvil H.323 (tratamiento de llamada saliente). Una llamada de un terminal móvil H.323 a otro terminal móvil H.323 es una combinación de ambos casos.

En el caso del tratamiento de llamada entrante, el primer requisito específico de la movilidad es la aptitud para encontrar la ubicación actual del terminal/usuario móvil. Esto se describe en 7.5.2.

En el caso del tratamiento de llamada saliente, la movilidad puede ser soportada por procedimientos H.323 normales. Todo otro requisito específico de la movilidad queda en estudio.

7.5.2 Procedimientos de gestión de la movilidad en la fase de establecimiento de comunicación en el caso de llamadas entrantes

Puesto que en las llamadas intrazona el controlador de acceso conoce la ubicación (el NPoA) del terminal móvil/usuario móvil H.323 llamado así como cualesquiera *aliasAddresses* asociadas con el usuario llamado (indicadas cuando el usuario móvil se registró en el controlador de acceso), no hay que cumplir requisitos adicionales específicos de la movilidad en comparación con el caso del abonado no móvil en H.323.

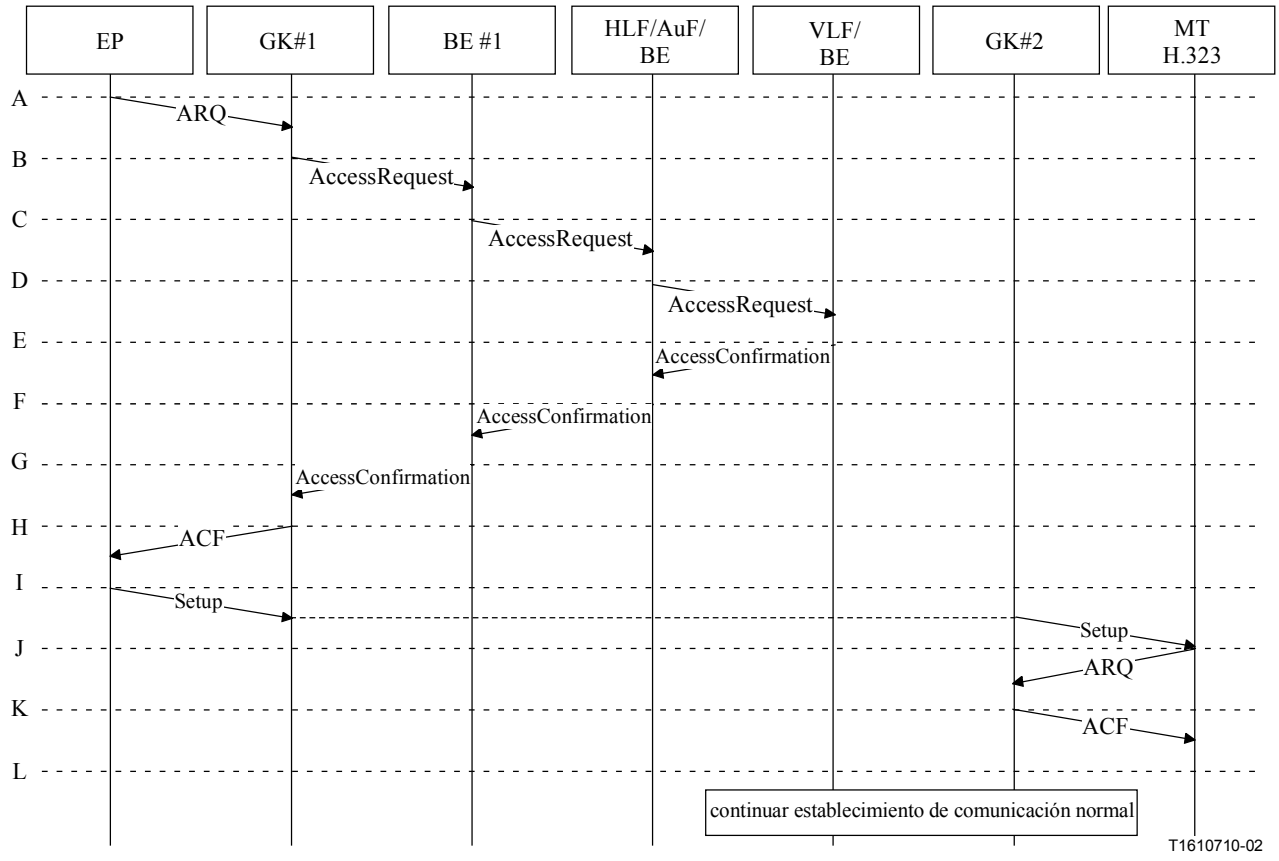


Figura 9/H.510 – Establecimiento de comunicación a un terminal móvil

La figura 9 representa el flujo de información en el caso de establecimiento exitoso de una comunicación a un terminal móvil H.323. A continuación se presenta una descripción más detallada del procedimiento:

A: El punto extremo llamante envía un mensaje ARQ a su controlador de acceso (GK#1). El campo *destinationInfo* contiene al menos una *aliasAddress* (identidad de usuario llamable) de un usuario móvil. El controlador de acceso GK#1 intenta resolver la dirección o direcciones de alias.

Si el usuario llamado está también registrado en GK#1 (es decir, caso de llamada intrazona), se omiten los pasos B-G, y el controlador de acceso retorna inmediatamente ACF (paso H).

B: Si el usuario llamado no está registrado en el mismo controlador de acceso, el controlador de acceso en el que el punto extremo llamante está registrado (GK#1) envía un mensaje **AccessRequest** al elemento de frontera (BE#1) con que está asociado (como otra posibilidad, GK#1 puede enviar un mensaje LRQ; esto no modifica esencialmente los procedimientos, salvo que el mensaje **AccessConfirmation** en el paso G se sustituye por LCF). El mensaje **AccessRequest** incluirá una o más identidades de usuario llamables del usuario llamado como *aliasAddresses* en el campo *destinationInfo*. Estas *aliasAddresses* se toman del mensaje ARQ recibido por el controlador de acceso del punto extremo llamante.

Los siguientes pasos C-F pueden omitirse si el usuario llamado está registrado actualmente en un controlador de acceso asociado con BE#1 (es decir, BE#1 es también la VLF/BE actual del usuario llamado).

C: El BE#1 deduce la HLF/BE del usuario llamado a partir de las *aliasAddress(es)* y reenvía el mensaje **AccessRequest** a la HLF/BE.

D: La HLF/BE conoce la VLF/BE que mantiene la información de ubicación relativa al usuario indicada por las identidades de usuario recibidas, y envía un mensaje **AccessRequest** a esta VLF/BE. El mensaje incluirá una o más identidades de usuario (primarias o llamables) elegidas por la HLF/BE como elementos *alias Address* en el campo *destinationInfo*.

Como otra posibilidad, la HLF/BE puede devolver un mensaje **AccessConfirmation** a BE#1, incluyendo una *template* (plantilla) que contiene una o más identidades de usuario adecuadas como dirección o direcciones de alias específicas y un campo *routeInfo* que indica *sendAccessRequest* en el *messageType* y la *transportAddress* de VLF/BE en el campo *contacts*. BE#1 puede entonces enviar otro mensaje **AccessRequest** a VLF/BE para obtener la ubicación del usuario llamado. El resultado de esta variante es el mismo (pero no se aplica el paso F).

E: La VLF/BE comprueba su información de ubicación relativa al usuario indicada por las identidades de usuario recibidas y devuelve un mensaje **AccessConfirmation** a la HLF/BE (o a BE#1 si se aplica el otro procedimiento posible del paso D). El mensaje incluirá una *template* que contiene una identidad de usuario adecuada como la *aliasAddress* específica y un campo *routeInfo* que indica *sendSetup* en el *messageType* y la *transportAddress* de señalización de llamada, bien del controlador de acceso en el que está registrado el usuario (GK#2), o bien del propio terminal móvil H.323, en el campo *contacts*. La elección de la identidad de usuario y de la dirección de transporte es un asunto de política local en el dominio visitado.

F: La HLF puede modificar el mensaje **AccessConfirmation** como sea necesario (por ejemplo puede añadir o sustituir identidades de usuario), y envía el mensaje a BE#1.

G: El BE#1 redirige el mensaje **AccessConfirmation**, posiblemente modificado, a GK#1.

H: GK#1 envía un mensaje ACF al punto extremo llamante, basándose en la información recibida en el mensaje **AccessConfirmation**. Este es el procedimiento H.323 normal.

I: La información recibida en el mensaje ACF determina los siguientes procedimientos de señalización de llamada según la Rec. UIT-T H.323: se envía un mensaje **Setup** utilizando, sea la señalización de llamada directa, sea la señalización encaminada por GK vía GK#1 y/o GK#2. Esto se indica por la línea discontinua que conecta las flechas "Setup" en cada lado.

J, K, L: El establecimiento de comunicación normal continúa de acuerdo con la Rec. UIT-T H.323.

Si BE#1 no está apto para deducir la dirección de la HLF a partir de las identidades de usuario llamables contenidas en el mensaje **AccessRequest** enviado por un GK (como en el anterior

paso B), o si la VLF/BE no tiene información de ubicación que corresponda a las identidades de usuario recibidas en el mensaje **AccessRequest** enviado por una HLF/BE (como en el anterior paso D), el BE#1 o la VLF/BE responderán con un mensaje **AccessRejection** con el campo *reason* fijado a *noMatch*. De manera similar, si la HLF/BE no tiene conocimiento del usuario indicado por el mensaje **AccessRequest** que recibió de un BE (como en el anterior paso C), responderá mediante un mensaje **AccessRejection** con el campo *reason* fijado a *noMatch*.

Al recibir el mensaje **AccessRejection** de la VLF/BE, la HLF/BE reenviará el mensaje **AccessRejection** a BE#1. Al recibir un mensaje **AccessRejection** de una HLF/BE, el BE reenviará el mensaje al GK que inició la **AccessRequest** (GK#1) y el GK enviará un mensaje ARJ al punto extremo llamante con el campo *reason* fijado a *calledPartyNotRegistered*.

La siguiente lista contiene un resumen del contenido de los mensaje que ofrecen interés para esta Recomendación (en el caso de mensajes o campos de mensajes no indicados aquí, el mensaje o campo de mensaje deberá utilizarse como se indica en las Recomendaciones UIT-T H.323, H.225.0 o H.501):

ARQ (lado llamante)

Campo	Descripción
destinationInfo	Una o más identidades de usuario llamables.

ARJ

Campo	Descripción
reason	
calledPartyNotRegistered	Si no se puede localizar al usuario llamado.

AccessRequest

Campo	Descripción
destinationInfo	
logicalAddresses	Para indagaciones por el GK al BE o por el BE a la HLF, una o más entidades de usuario llamables. Para indagaciones a la VLF/BE por la HLF/BE, facultativamente también la identidad de usuario primaria, del usuario.

AccessConfirmation

Campo	Descripción
templates	
pattern	
specific	Una o más identidades de usuario llamables y/o la identidad de usuario primaria, del usuario, según proceda.
routeInfo	
messageType	
sendSetup	Indica que el punto extremo/GK de origen puede enviar el mensaje Setup a la dirección especificada en la transportAddress en el campo contacts.
contacts	
transportAddress	Dirección TSAP de señalización de llamada del usuario llamado o de su GK.

AccessRejection

Campo	Descripción
reason	
noMatch	Si la entidad funcional que recibe el mensaje AccessRequest no tiene conocimiento del usuario indicado por las identidades de usuario en el mensaje AccessRequest ni tampoco sobre ninguna otra entidad funcional que pudiera resolver la ubicación del usuario.

7.5.3 Procedimientos de gestión de la movilidad en la fase de establecimiento de comunicación en el caso de llamadas salientes

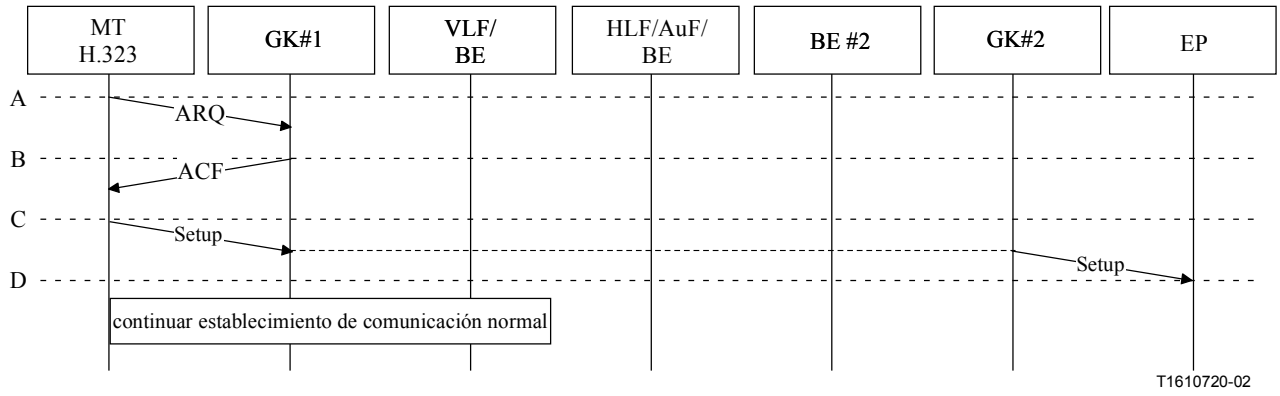


Figura 10/H.510 – Establecimiento de comunicación desde un terminal móvil

La figura 10 representa el flujo de información en el caso de establecimiento exitoso de una comunicación saliente cuando se introducen procedimientos de gestión de la movilidad. A continuación se presenta una descripción más detallada del procedimiento:

A: El terminal móvil H.323 llamante envía un mensaje ARQ a su controlador de acceso (GK#1) de acuerdo con los procedimientos H.323.

B: El controlador de acceso retorna un mensaje ACF con la ubicación del usuario llamado, según los procedimientos H.323 normales.

NOTA – Si el usuario llamado es asimismo un usuario móvil se utilizan también los procedimientos de 7.5.2.

C: La información recibida en el mensaje ACF determina los siguientes procedimientos de señalización de llamada según la Rec. UIT-T H.323: Se envía un mensaje Setup (establecimiento) utilizando señalización de llamada directa o señalización encaminada por GK vía GK#1 y/o GK#2. Esto se indica por la línea discontinua que conecta la flecha "Setup" en cada lado.

D: El establecimiento normal de la comunicación continúa de acuerdo con la Rec. UIT-T H.323.

7.5.4 Seguridad

Los aspectos de seguridad para H.510 se especifican en la Rec. UIT-T H.530. Estos procedimientos permiten a un dominio sirviente autenticar un usuario/terminal móvil cuando éste intenta localizar un controlador de acceso o registrarse. Como resultado del proceso de autenticación, el usuario/terminal visitante obtiene también autenticación del dominio sirviente. Cualquier otro procedimiento de seguridad se aplica localmente entre terminal móvil H.323 y controlador de acceso.

7.6 Traspaso

Si el terminal móvil se desplaza en el curso de una llamada, unos mecanismos en las capas de protocolo inferiores pueden proporcionar la necesaria funcionalidad de traspaso en una forma que sea transparente a H.323, es decir, de una manera que no implique un cambio del NPoA del terminal.

Los traspasos que implican el cambio del NPoA, es decir, que también necesitan la intervención de capas de protocolo H.323, quedan en estudio.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2002