(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 373 357**

(51) Int. CI.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08873006 .4**
(96) Fecha de presentación: **11.12.2008**
(97) Número de publicación de la solicitud: **2250786**
(97) Fecha de publicación de la solicitud: **17.11.2010**

(54) Título: **TÉCNICA PARA REALIZAR LA CONVERSIÓN DE SEÑALIZACIÓN ENTRE LOS DOMINIOS HTTP Y SIP.**

(30) Prioridad:
29.02.2008 US 32815 P

(45) Fecha de publicación de la mención BOPI:
02.02.2012

(45) Fecha de la publicación del folleto de la patente:
02.02.2012

(73) Titular/es:
Telefonaktiebolaget L M Ericsson (PUBL)
164 83 Stockholm, SE

(72) Inventor/es:
FIKOURAS, Ioannis;
FIKOURAS, Nikolaos, Albertos y
LEVENSHTEYN, Roman

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Técnica para realizar la conversión de señalización entre los dominios HTTP y SIP

Campo técnico

La presente invención se refiere de manera general a la conversión de señalización entre los dominios HTTP y SIP. En particular, la invención se dirige a una técnica de conversión que permite una comunicación de estado entre los dos dominios.

Antecedentes

En la actualidad, el Protocolo de Transporte de HiperTexto (HTTP) constituye el medio principal para la entrega de contenido en la Web a nivel Mundial (WWW). El HTTP es un protocolo de capa de aplicaciones sin estado, basado en texto que define un mecanismo de intercambio de mensajes basado en petición/respuesta entre un cliente HTTP y un servidor HTTP. En el modelo cliente-servidor HTTP, una petición HTTP se emite por un Cliente de Agente de Usuario HTTP, mientras que la respuesta HTTP a la petición llega desde un Servidor de Agente de Usuario HTTP.

La demanda creciente de servicios WWW personalizados ha llevado al desarrollo de sesiones de estado HTTP que comprenden dos o más (nominalmente independientes) parejas de mensajes de petición y respuesta HTTP. Actualmente, los planteamientos dominantes para la administración de sesión HTTP son las cookies, los parámetros en los Localizadores de Recursos Universales (URL) HTTP y los denominados URL gruesos.

En cuanto a las cookies, el memorando RFC2965 publicado por el Grupo de Trabajo de Ingeniería de Internet (IETF) y titulado “Mecanismo de Gestión de Estado HTTP” propone varias cabeceras HTTP capaces de transportar la información de estado entre los puntos finales de un intercambio de mensajes de petición-respuesta HTTP. Las cookies se definen como Pares de Valores de Atributos (AVP) de nombres y valores arbitrarios que se pueden acompañar por una gama de parámetros predefinidos como se describe en la RFC2965. En un mensaje de petición o respuesta HTTP único, se pueden incluir una o más cookies según se requiera.

Un ejemplo de una petición HTTP que contiene cookies es el siguiente:

```
GET URI HTTP/1.1

Cookie: dialog-id=ali2alice1;method=bye
```

Esta petición HTTP contiene dos cookies que identifican colectivamente el estado actual de una sesión. La primera cookie define el atributo ‘dialog-id’ como ‘ali2alice1’, mientras que la segunda cookie asigna al atributo ‘method’ el valor ‘bye’.

Otra posibilidad para conservar la información de estado HTTP son los parámetros HTTP y los componentes de consulta. Es bien conocido que los esquemas URL basan su sintaxis URL en un formato general de nueve partes (ver RFC2396):

```
<scheme>://<user>:<password>@<host>:<port>/<path>;<params>?<query>#<frag>
```

Usando este formato, es posible transportar la información de estado de sesión a aplicaciones de red remotas o bien como parámetros o bien como componentes de consulta. Los listados de código siguientes ilustran dos peticiones HTTP de un cliente HTTP para entregar la información de estado de sesión a un servidor HTTP.

Señalando la información de estado de sesión como parámetros HTTP:

```
GET path;dialog-id=ali2alice1;method=bye HTTP/1.1 host: URI
```

Señalando la información de estado como componentes de consulta HTTP:

```
GET path?dialog-id=ali2alice1&method=bye HTTP/1.1 host: URI
```

En ambos casos el servidor HTTP es informado de que los valores actuales para los atributos ‘dialog-id’ y ‘method’ son ‘ali2alice1’ y ‘bye’, respectivamente.

Los URL gruesos son versiones extendidas de los URL, añadidos sufijos con información usada para identificar el estado actual de una sesión HTTP. La siguiente petición HTTP ilustra cómo se puede incluir la información de estado en la indicación del trayecto en un URL:

```
GET path/dialog-id=ali2alice1/method=bye HTTP/1.1 host: URI
```

En el ejemplo anterior, el cliente HTTP emite una petición a un servidor HTTP que es consciente de que los últimos dos segmentos del trayecto corresponden a la información de estado de sesión. En este caso particular, el atributo ‘dialog-id’ es equivalente a ‘ali2alice1’ y el atributo ‘method’ es equivalente a ‘bye’.

Mientras que HTTP constituye el medio principal para la distribución de contenido en la WWW, el Protocolo de Inicio de Sesiones (SIP) es el protocolo de señalización principal en el plano de control del IMS (Subsistema Multimedia del Protocolo Internet) y otras redes de aprovisionamiento de servicios. SIP es un protocolo basado en texto usado para autorizar el acceso de usuario así como establecer, controlar y terminar las sesiones de medios entre las aplicaciones alojadas por los puntos finales habilitados SIP.

Similar a HTTP, SIP se basa en la transmisión de mensajes de petición y respuesta. Estos mensajes se intercambian entre los Agentes de Usuario instalados en los puntos finales SIP de comunicación. Un Agente de Usuario SIP puede actuar o bien como un Cliente de Agente de Usuario (cuando envía un mensaje de petición) o bien como un Servidor de Agente de Usuario (cuando responde al mensaje de petición con un mensaje de respuesta).

SIP define que solamente se puedan establecer una o más sesiones de medios entre dos puntos finales SIP dentro del contexto de un diálogo SIP. El diálogo es una relación conceptual entre los puntos finales SIP implicados que se mantiene por la Capa de Usuario de Transacción de las Capas de Protocolo SIP. En la práctica, un diálogo se manifiesta como una colección de información que refleja el estado actual del diálogo para cada punto final. Como se entiende aquí dentro, cada diálogo SIP comprende una o más transacciones SIP, y cada transacción SIP implica uno o más mensajes (típicamente un mensaje de petición y uno o más mensajes de respuesta). En este sentido, cada mensaje SIP se puede ver como parte de una transacción SIP.

Cada diálogo SIP se identifica por un identificador (el denominado ID de diálogo) que está formado por una serie de atributos negociados entre los puntos finales SIP durante el inicio de una sesión y que permanecen válidos durante el tiempo de vida del diálogo. Específicamente, el ID del diálogo de un diálogo entre un Cliente de Agente de Usuario y un Servidor de Agente de Usuario (los dos puntos finales de un diálogo SIP) se definen como:

> Dialog (-ID) – call-ID, local tag (To-header tag of dialog response), remote tag (From-header tag of dialog request)

El SIP y los Identificadores de Recursos Universales (URI) de SIP siguen las pautas fijadas por la RFC2396. La forma general de un URI SIP como se define en la RFC3261 tiene la siguiente sintaxis:

> sip:user:password@host:port;uri-parameters?headers

La estructura URI SIP permite la inclusión de varios parámetros y cabeceras dentro de su forma genérica.

Mientras que HTTP es el protocolo estándar para la entrega de contenido en la WWW, no existe actualmente solución documentada o implementada que permitiría al equipo de usuario habilitado con HTTP iniciar, conducir y terminar sesiones con un Agente de Usuario SIP.

La EP 1093281 describe métodos para la conversión del Lenguaje de Marcado de Hipertexto (HTML) – SIP. En un método para convertir HTML a SIP, un Agente de Usuario SIP recibe un mensaje HTML, analiza sintácticamente el mensaje HTML para la clase y contenido, y analiza la clase y contenido para crear una señal SIP a partir del mensaje HTML. La señal SIP se envía a un intermediario SIP. Igualmente, se describe un método de conversión de una señal SIP en un mensaje HTML. Un Agente de Usuario SIP recibe la señal SIP desde un intermediario SIP, analiza sintácticamente la señal SIP para el tipo de mensaje y extrae el contenido, la parte que llama, y la parte llamada. Usando la información extraída, el Agente de Usuario SIP genera un mensaje HTML y envía el mensaje HTML a la parte llamada.

Resumen

Por consiguiente, hay una necesidad para permitir una conversión de señalización eficiente entre los dominios HTTP y SIP que preserve el concepto de sesión.

De acuerdo con un primer aspecto, se proporciona un método de realizar la conversión de señalización entre una sesión de estado HTTP y un diálogo SIP, que comprende recibir desde una entidad habilitada con HTTP un primer mensaje de petición HTTP, el primer mensaje de petición HTTP que incluye la información de estado HTTP; crear un primer mensaje SIP en respuesta a la recepción del primer mensaje de petición HTTP, el primer mensaje SIP que pertenece a un diálogo SIP; enviar el primer mensaje SIP a una entidad habilitada con SIP; y establecer una asignación entre la información de estado HTTP y el diálogo SIP, como en la reivindicación 1.

La información de estado HTTP puede tener cualquier formato y contenido. En una implementación, la información de estado HTTP toma la forma de una cadena de caracteres alfanuméricos que es única al menos localmente (por ejemplo, entre los componentes de red que controlan la transferencia del mensaje descrita aquí dentro).

La asignación entre la información de estado HTTP y el diálogo SIP se puede realizar en una interfaz entre un dominio HTTP que comprende una o más entidades habilitadas HTTP y un dominio SIP que comprende una o más entidades habilitadas SIP. Específicamente, se puede usar la asignación para ligar la señalización relacionada con la sesión que se origina o termina en el dominio SIP con la señalización relacionada con la sesión que se origina o

termina en el dominio HTTP. Para este fin, la asignación se puede establecer, consultar y/o actualizar cada vez que un mensaje previsto para el dominio SIP llega desde el dominio HTTP, y viceversa. Como resultado, la asignación puede formar la base para que cualquier entidad habilitada con HTTP inicie, acepte, conduzca y termine una o más sesiones con una entidad habilitada con SIP (por ejemplo una entidad habilitada IMS tal como un abonado IMS o un servidor de aplicaciones IMS), y viceversa.

Las técnicas tratadas aquí dentro se pueden realizar en contexto con un diálogo SIP que ya se ha establecido (por ejemplo, para el cual uno o más mensajes ya se han intercambiado entre la entidad habilitada con HTTP y la entidad habilitada con SIP). Alternativamente, las técnicas también se pueden realizar en contexto con un diálogo SIP que está a punto de ser establecido (por ejemplo, para el cual solamente la entidad habilitada con HTTP y la entidad habilitada con SIP han transmitido hasta el momento un mensaje con el propósito de establecer un diálogo).

Como se estableció anteriormente, el primer mensaje SIP se crea en respuesta a la recepción del primer mensaje de petición HTTP. Además en respuesta a la recepción del primer mensaje de petición HTTP, un primer mensaje de respuesta HTTP se puede enviar a la entidad habilitada con HTTP. El primer mensaje de respuesta HTTP opcionalmente puede incluir o referenciar la información de estado HTTP a través del primer mensaje de petición HTTP.

El método además comprende los pasos de recibir un segundo mensaje SIP; determinar el diálogo SIP al cual pertenece el segundo mensaje SIP; determinar la información de estado HTTP asociada con el diálogo SIP; generar un segundo mensaje de petición HTTP que incluye o referencia la información de estado HTTP determinada de esta manera; y enviar el segundo mensaje de petición HTTP a la entidad habilitada con HTTP.

Adicionalmente, un segundo mensaje de respuesta HTTP en respuesta al segundo mensaje de petición HTTP se puede recibir desde la entidad habilitada con HTTP. El segundo mensaje de respuesta HTTP opcionalmente puede incluir o referenciar la información de estado HTTP.

En base a la información de estado HTTP, la pareja de primeros mensajes de petición y respuesta HTTP así como la pareja de segundos mensajes de petición y respuesta HTTP se pueden agrupar en una sesión de estado HTTP. En otras palabras, asociando la información de estado HTTP (o la información únicamente derivada de allí o que referencia a la misma) con dos o más parejas de mensajes de petición y respuesta HTTP, las parejas de mensajes se pueden clasificar como pertenecientes a una sesión específica que se extiende entre el dominio HTTP y el dominio SIP.

El primero o cualquier mensaje de petición HTTP posterior además puede incluir la información de dirección indicativa de un Agente de Usuario SIP de la entidad habilitada con SIP. La información de dirección incluida en el primer mensaje de petición HTTP se puede usar para dirigir el primer mensaje SIP al Agente de Usuario SIP. Para este fin, la información de dirección se puede escribir (por ejemplo, copiar) en el primer mensaje SIP.

El primero o cualquier mensaje de petición HTTP posterior además puede incluir la información de diálogo HTTP. La información de diálogo HTTP y la información de diálogo SIP pueden cada una identificar únicamente un diálogo específico relacionado con la sesión entre al menos una entidad habilitada con HTTP y al menos una entidad habilitada con SIP. En algunos casos, uno y el mismo identificador puede constituir simultáneamente la información de diálogo HTTP y la información de diálogo SIP, de manera que una asignación llegaría a estar obsoleta y un simple almacenamiento de este identificador sería suficiente. Junto con la información de diálogo HTTP y/o SIP, se puede almacenar la información acerca del estado actual del diálogo específico. Este planteamiento permite buscar el estado actual de cualquier diálogo en base a la información de diálogo HTTP y/o SIP. Tal búsqueda se puede realizar en contexto con la construcción de uno o más mensajes SIP para continuar, modificar o terminar el diálogo.

De acuerdo aún con una posibilidad adicional, el primero o cualquier mensaje de petición HTTP posterior puede incluir información de descripción de sesiones tal como la información de acuerdo con el estándar del Protocolo de Descripción de Sesiones (SDP). La información de descripción de sesiones se puede enviar, por ejemplo, en un contexto de ofrecimiento/contestación SDP. En el caso que el primer mensaje de petición HTTP incluya información de descripción de sesiones, esta información se puede reenviar a través del primer mensaje SIP a la entidad habilitada con SIP. En otras palabras, la información de descripción de sesiones recibida a través del primer mensaje de petición HTTP se puede incluir (por ejemplo, copiar) en el primer mensaje SIP.

Existen varias posibilidades para insertar la información de estado HTTP en al menos uno del primer mensaje de petición HTTP y el segundo mensaje de petición HTTP. De acuerdo con una primera variante, las cookies HTTP se usan para transportar la información de estado. De acuerdo con una segunda variante, se transmite la información de estado en forma de un URL grueso. Como una variante adicional, se puede mencionar la utilización de los parámetros y los componentes de consulta HTTP. Dos o más de estas variantes se pueden combinar según se necesite.

El primer mensaje de petición HTTP puede incluir una indicación de mensaje SIP que permite al destinatario del primer mensaje de petición HTTP identificar el tipo de mensaje SIP que va a ser creado. La indicación del mensaje SIP puede referirse directa o indirectamente a cualquier método SIP tal como INVITE, ACK, BYE, CANCEL, OPTIONS, REGISTER e INFO. De acuerdo con otra variante, la indicación del mensaje SIP puede referirse directa o

indirectamente a un código SIP tal como cualquiera de los siguientes (u otros) códigos de respuesta: 1xx Informational (por ejemplo, 100 Trying, 180 Ringing), 2xx Successful (por ejemplo, 200 OK, 202 Accepted), 3xx Re-Direction, 4xx Request Failure, 5xx Server Failure, y 6xx Global Failure. De acuerdo con una variante adicional, la indicación del mensaje SIP puede referirse directa o indirectamente a un código de estado HTTP que se puede traducir en un código SIP o método SIP correspondiente.

De acuerdo con un aspecto adicional, se proporciona un método de realización de la conversión de señalización entre un diálogo SIP y una sesión de estado HTTP, que comprende recibir desde una entidad habilitada con SIP un primer mensaje SIP, el primer mensaje SIP que pertenece a un diálogo SIP; establecer una asignación entre la información de estado HTTP y el diálogo SIP; crear un primer mensaje de petición HTTP indicativo de un contenido del primer mensaje SIP, el primer mensaje de petición HTTP que incluye la información de estado HTTP que se asigna en el diálogo SIP; y enviar el primer mensaje de petición HTTP a una entidad habilitada con HTTP, como en la reivindicación 8.

El método puede comprender además recibir un primer mensaje de respuesta HTTP en respuesta al primer mensaje de petición HTTP desde la entidad habilitada con HTTP. El primer mensaje de respuesta HTTP opcionalmente puede incluir o referenciar la información de estado HTTP recibida por la entidad habilitada con HTTP a través del primer mensaje de petición HTTP.

Aún además, el método puede comprender los pasos de recibir un segundo mensaje de petición HTTP que incluye la información de estado y, opcionalmente, que incluye una indicación de mensaje SIP indicativa de un segundo mensaje SIP que va a ser creado; determinar el diálogo SIP asignado en la información de estado HTTP; crear un segundo mensaje SIP en respuesta a la recepción de un segundo mensaje de petición HTTP en base al diálogo SIP determinado (y opcionalmente en base a la indicación del mensaje SIP si está disponible); y enviar el segundo mensaje SIP a la entidad habilitada con SIP. Además, un segundo mensaje de respuesta HTTP se puede devolver a la entidad habilitada con HTTP en respuesta al segundo mensaje de petición HTTP. El segundo mensaje de respuesta HTTP opcionalmente puede incluir o referenciar la información de estado HTTP.

En base a la información de estado HTTP, la pareja de primeros mensajes de petición y respuesta HTTP así como la pareja de segundos mensajes de petición y respuesta HTTP se pueden agrupar en la sesión de estado HTTP. En otras palabras, mientras que HTTP como tal es sin estado, la inclusión de la información de estado HTTP en al menos los mensajes de petición HTTP (y opcionalmente también en los mensajes de respuesta correspondientes) permite extender el paradigma de sesión de estado del dominio SIP en el dominio HTTP.

La información de estado HTTP se puede generar (por ejemplo, en respuesta a la recepción del primer mensaje SIP) por cualquiera de los componentes de red implicados en el intercambio del mensaje. Si, por ejemplo, la sesión se inicia desde el dominio HTTP (es decir, por una entidad habilitada con HTTP), la información de estado HTTP se puede generar por la entidad habilitada con HTTP y transmitir con el primer mensaje de petición HTTP. Si, por otra parte, la sesión se inicia desde el dominio SIP (es decir, por una entidad habilitada con SIP), la información de estado HTTP se puede generar por el componente de red que establece la asignación entre la información de estado HTTP y el diálogo SIP. Por supuesto, existen varias posibilidades adicionales de cómo y dónde se puede generar la información de estado HTTP.

La entidad habilitada con HTTP que participa en la transferencia del mensaje descrita aquí dentro puede tomar la forma de cualquier equipo de usuario, tal como un teléfono móvil, un asistente digital personal, un ordenador personal, un ordenador portátil, una tarjeta de red o datos etc. La entidad habilitada con SIP puede ser una entidad IMS tal como un servidor de aplicaciones IMS o un equipo de usuario habilitado IMS.

El diálogo SIP realizado entre la entidad habilitada con HTTP y la entidad habilitada con SIP se puede realizar en cualquier contexto de mensajería SIP. Los posibles contextos de mensajería SIP incluyen un contexto de registro de usuario, un contexto de inicio de sesión y un contexto de terminación de sesión.

De acuerdo con otro aspecto, se proporciona un producto de programa informático. El producto de programa informático comprende partes de código de programa para realizar uno o más de los pasos de uno o más de los métodos descritos aquí dentro cuando el producto de programa informático se ejecuta en uno o más dispositivos informáticos, como en la reivindicación 14. El producto de programa informático se puede almacenar en un medio de grabación legible por ordenador tal como una memoria permanente o re escribible, un CD-ROM, o un DVD. El producto de programa informático también se puede proporcionar por descarga a través de una o más redes informáticas tales como Internet, una red de telecomunicaciones celular o una Red de Área Local (LAN) inalámbrica o cableada.

De acuerdo aún con un aspecto adicional, se proporciona un aparato para realizar la conversión de señalización entre una sesión de estado HTTP y un diálogo SIP, como en la reivindicación 16. El aparato comprende un Agente de Usuario HTTP adaptado para recibir desde una entidad habilitada con HTTP un primer mensaje de petición HTTP, el primer mensaje de petición HTTP que incluye la información de estado HTTP; un Agente de Usuario SIP adaptado para enviar un primer mensaje SIP a una entidad habilitada con SIP en respuesta a la recepción del primer mensaje de petición HTTP, el primer mensaje de petición SIP que pertenece a un diálogo SIP; y una lógica de

asignación adaptada para establecer una asignación entre la información de estado HTTP y el diálogo SIP. El aparato se puede configurar para realizar cualquier de los aspectos del método tratados aquí dentro.

El Agente de Usuario SIP u otro componente del aparato se puede configurar también para crear el primer mensaje SIP. Además, el Agente de Usuario HTTP se puede adaptar para devolver un primer mensaje de respuesta HTTP a la entidad habilitada con HTTP.

Un aparato adicional para realizar la conversión de señalización entre un diálogo SIP y una sesión de estado HTTP comprende un Agente de Usuario SIP adaptado para recibir desde una entidad habilitada con SIP un primer mensaje SIP, el primer mensaje SIP que pertenece a un diálogo SIP; una lógica de asignación adaptada para establecer una asignación entre la información de estado HTTP y el diálogo SIP; y un Agente de Usuario HTTP adaptado para enviar un primer mensaje de petición HTTP indicativo de un contenido del primer mensaje SIP a una entidad habilitada con HTTP, el primer mensaje de petición HTTP que incluye o que referencia la información de estado HTTP asignada en el diálogo SIP, como en la reivindicación 18. El aparato se puede configurar para realizar cualquiera de los aspectos del método tratados aquí dentro.

El Agente de Usuario HTTP u otro componente del aparato se puede adaptar también para crear el primer mensaje de petición HTTP. El Agente de Usuario HTTP se puede adaptar además para recibir un primer mensaje de respuesta HTTP en respuesta al primer mensaje de petición HTTP desde la entidad habilitada con HTTP.

Cualquiera de los aparatos descritos aquí dentro se pueden configurar como un nodo de red intermedio que interconecta (o que puentea) un dominio HTTP por un lado y el dominio SIP por el otro. En una posible implementación, el aparato se configura como un intermediario Web.

Breve descripción de los dibujos

A continuación, la presente invención se describirá en más detalle con referencia a las realizaciones ejemplares ilustradas en los dibujos, en los cuales:

La Fig. 1 ilustra esquemáticamente una infraestructura de red que comprende una realización del nodo de red;

La Fig. 2 es un diagrama de bloques que ilustra los componentes internos de la realización del nodo de red;

La Fig. 3 es un diagrama de señalización esquemático que ilustra un mecanismo de señalización básico que implica la realización del nodo de red de la Fig. 2;

La Fig. 4 ilustra esquemáticamente la arquitectura de los componentes lógicos de un componente de Agente de Usuario HTTP de la realización del nodo de red ilustrado en la Fig. 2;

La Fig. 5 es un diagrama de señalización esquemático que ilustra la señalización de inicio de sesión;

La Fig. 6 ilustra una realización de una tabla de estado de diálogo según se mantiene por el nodo de red mostrado en la Fig. 4;

La Fig. 7 ilustra una realización de una tabla de resolución de diálogo;

La Fig. 8 ilustra una realización de una tabla de recuento de transacciones;

La Fig. 9 es un diagrama de señalización esquemático que ilustra en más detalle algunos aspectos de la señalización de inicio de sesión;

La Fig. 10 es un diagrama de señalización esquemático que ilustra genéricamente la señalización en contexto con la aceptación de una invitación de sesión;

La Fig. 11 es un diagrama de señalización esquemático adicional que ilustra en más detalle algunos aspectos de la aceptación de una invitación de sesión;

La Fig. 12 es un diagrama de señalización esquemático que ilustra una primera variante de la señalización de terminación de sesión;

La Fig. 13 es un diagrama de señalización esquemático que ilustra una segunda variante de la señalización de terminación de sesión;

La Fig. 14 es un diagrama de señalización esquemático que ilustra la señalización de registro de la Pasarela de Confianza;

La Fig. 15 ilustra una realización de una tabla de abonado;

La Fig. 16 ilustra una realización de una tabla de registro.

Descripción detallada

En la siguiente descripción, para propósitos de explicación y no de limitación, se establecen en adelante detalles específicos tales como las configuraciones de red específicas y los escenarios de señalización específicos para proporcionar una comprensión minuciosa de las técnicas reveladas aquí dentro. Será evidente para un experto en la técnica que las técnicas se pueden practicar en otras realizaciones sin salir de estos detalles específicos. Por ejemplo, los expertos apreciarán que las técnicas tratadas aquí dentro se pueden practicar en combinación con otras configuraciones de red y distintos pasos de señalización. Además, mientras que las realizaciones siguientes se describirán en primer lugar en relación con las entidades IMS habilitadas SIP, será fácilmente evidente que las técnicas descritas aquí dentro también se pueden practicar en contexto con las entidades habilitadas SIP que no son compatibles con el estándar IMS.

Aquellos expertos en la técnica apreciarán además que los métodos, pasos y funciones explicadas aquí dentro se pueden implementar usando circuitería de componentes físicos individual, usando componentes lógicos que funcionan en conjunto con un microprocesador programado u ordenador de propósito general, usando un Circuito Integrado de Aplicaciones Específicas (ASIC) y/o usando uno o más Procesadores de Señal Digitales (DSP). También se apreciará que, mientras que las siguientes realizaciones se describirán en primer lugar en forma de métodos y aparatos, las técnicas reveladas aquí dentro también se pueden integrar en un procesador informático y una memoria acoplada al procesador, en donde la memoria se codifica con uno o más programas que realizan los pasos tratados aquí dentro cuando se ejecutan por el procesador.

Se hace ahora referencia a la Fig. 1, la cual muestra una arquitectura de red ejemplar 100 en la cual se pueden implementar las diversas técnicas descritas aquí dentro. La arquitectura de red 100 comprende una red IMS 102, una red de Acceso HTTP a IMS (HIAnet) 104 y varios elementos de Equipo de Usuario habilitado con HTTP (HUE) 106. En el escenario ejemplar ilustrado en la Fig. 1, los HUE 106 se configuran como teléfonos móviles.

La HIAnet 104 proporciona un nodo de red central que aloja una denominada Función de Acceso HTTP a IMS (HIAF) 108. La HIAF 108 sirve a los diversos HUE 106 a través de los enlaces de red basados en HTTP y al mismo tiempo mantiene un enlace de red basado en SIP con la red IMS 102. La HIAF 108 de esta manera interactúa o interviene entre la pluralidad de los HUE 106 por una parte y la red IMS 102 por otra parte.

La red IMS 102 comprende una pluralidad de nodos de red distribuidos sobre un plano de aplicación, un plano de control y un plano de transporte. El plano de control incluye una pluralidad de servidores SIP e intermediarios SIP que se llaman colectivamente Funciones de Control de Sesión de Llamada (CSCF) y que se usan para procesar la señalización SIP. Una CSCF Intermediaria (P-CSCF) 110 es un intermediario SIP que constituye el primer punto de contacto para las entidades habilitadas IMS externas tales como teléfonos móviles. La P-CSCF 110 se asigna a una entidad habilitada IMS durante el registro y proporciona servicios de autentificación. Una CSCF de Servicio (S-CSCF) 112 es el nodo central del plano de control. Es un servidor SIP pero también realiza el control de sesión. Las tareas principales de la S-CSCF 112 incluyen el manejo de registros SIP y la selección de un Servidor de Aplicaciones (AS) 114 que va a proporcionar un servicio requerido. Una CSCF de Interrogación (I-CSCF) 116 es otra función SIP configurada para consultar a un Servidor Local de Abonado (HSS) 118 en respuesta a la recepción de una petición SIP, y para encaminar la petición SIP recibida a la S-CSCF asignada 112 en base a la información recuperada desde el HSS 118.

En la capa de aplicaciones, el uno o más AS 114 alojan y ejecutan los servicios, que incluyen servicios de voz, datos y multimedia. Los AS 114 interactúan con la S-CSCF 112 a través de la señalización SIP. El HSS 118 es un componente de la capa de aplicaciones adicional que mantiene la información relacionada con la suscripción (perfiles de usuario), y que participa en los procesos de autentificación y autorización. La Función de Recursos de Medios (MRF) 120 es un servidor de medios que proporciona las funciones relacionadas con los medios que incluyen la manipulación de los medios (por ejemplo, la mezcla de secuencias de voz).

Una Función de Controlador de Pasarela de Medios (MGCF) 122 es una pasarela de la Red Pública de Telefonía Conmutada (PSTN) a cargo de la conversión del protocolo de control de llamada entre SIP y el protocolo de la Parte de Usuario ISDN (ISUP). Una Pasarela de Medios (MGW) 124 es una pasarela PSTN adicional que se sitúa en la capa de transporte e interactúa con el plano de medios de la PSTN realizando la conversión de protocolos entre el Protocolo de Transporte en Tiempo Real (RTP) como se usa en la red IMS 102 y la Modulación de Código de Pulsos (PCM) como se usa en las PTSN de circuitos conmutados.

La red IMS 102 además comprende el equipo de usuario habilitado con SIP 110', 112', 116', 122', 124' que incluye los teléfonos móviles (como se ilustran esquemáticamente en la Fig. 1, por ejemplo en conexión con la S-CSCF 112). Básicamente, la configuración y operación de los componentes IMS individuales tratadas anteriormente es bien conocida por las personas expertas en la técnica, y por esta razón se omitirá aquí una discusión más detallada de las mismas a menos que sea necesario para comprender la comunicación entre la red IMS 102 y la HIAF 108 de la HIAnet 104.

Como se mencionó anteriormente, la HIAF 108 constituye el nodo de red central de la HIAnet 104. La HIAF 108 funciona como un intermediario Web e intercepta las peticiones HTTP generadas por los HUE 106. La dirección de

red de la HIAF 108 se puede preconfigurar estáticamente, o se puede descubrir dinámicamente como se describirá en más detalle más adelante.

La tarea básica de la HIAF 108 es permitir una interacción entre los HUE 106 por una parte y la red IMS 102 por otra. Esta interacción incluye el inicio, aceptación y terminación de las sesiones multimedia con las entidades IMS habilitadas SIP incluyendo los abonados IMS (es decir, el equipo de usuario habilitado IMS) y los AS de IMS 114. La HIAF 108 se configura para establecer, actualizar y terminar las asignaciones entre los diálogos SIP y la información de estado HTTP (es decir, las sesiones de estado HTTP). En base a estas asignaciones, la HIAF 108 realiza adicionalmente la conversión de señalización que permite a los HUE 106 iniciar las sesiones de medios hacia las entidades IMS, y ser el objetivo de las sesiones de medios iniciadas por las entidades IMS.

La Fig. 2 ilustra la configuración interna de la HIAF 108. La HIAF 108 aloja un Cliente de Agente de Usuario HTTP (HUAC) y Servidor (HUAS) en una función llamada colectivamente Agente de Usuario HTTP (HUA) 130. El HUAC emite las peticiones HTTP y recibe las respuestas HTTP, mientras que el HUAS recibe las peticiones HTTP y devuelve las respuestas HTTP. La HIAF 108 además comprende un Cliente de Agente de Usuario SIP y un Servidor de Agente de Usuario SIP alojado en una función llamada colectivamente Agente de Usuario SIP 132. El Cliente de Agente de Usuario SIP emite las peticiones SIP y recibe las respuestas SIP, y el Servidor de Agente de Usuario SIP recibe las peticiones SIP y devuelve las respuestas SIP.

El Agente de Usuario HTTP 130 constituye un punto final de la mensajería HTTP, mientras que el Agente de Usuario SIP 132 constituye un punto final para la mensajería SIP. Una función llamada Lógica de Asignación HTTP a SIP (HSML) 134 se acopla entre el Agente de Usuario HTTP 130 y el Agente de Usuario SIP 132. La HSML 134 está a cargo de establecer (por ejemplo, determinar, crear, actualizar o borrar) la información de estado para las sesiones HTTP y SIP y adicionalmente realiza la conversión de señalización entre ellas. Específicamente, en la HSML 134 cada mensaje SIP se puede asociar con y traducir en una pareja de mensaje petición-respuesta HTTP y viceversa. El patrón de señalización resultante se ilustra en la Fig. 3.

La Fig. 3 ilustra el intercambio de mensajes basado en HTTP entre un HUE 106 y la HIAF 108. También mostrados están los mensajes SIP asociados enviados por la HIAF 108 hacia la red IMS 102. De una manera similar que la HIAF 108, el HUE 106 comprende un HUAC 106A y un HUAS 106B. La HIAF 108 está limitada a un número de puertos del Protocolo de Control de Transmisión (TCP) predefinido conocido por todos los HUE 106.

Como es bien conocido, HTTP es un protocolo sin estado en el cual cada pareja de mensajes de petición y respuesta se abre una nueva conexión TCP (como se muestra en el lado izquierdo de la Fig. 3). En la presente realización, la información de estado HTTP se transporta con al menos un mensaje de cada pareja de mensaje de petición y respuesta. Identificando la información de estado HTTP similar o interrelacionada en mensajes que pertenecen a distintas parejas de mensajes de petición y respuesta HTTP (es decir, a distintas conexiones TCP), las parejas de mensajes de petición y respuesta individuales se pueden agrupar a una sesión HTTP de estado única.

La HIAF 108 establece adicionalmente (por ejemplo, genera y/o mantiene) una asignación entre un diálogo SIP (que implica un mensaje de petición SIP y un mensaje de respuesta SIP en el escenario ejemplar mostrado en el lado derecho de la Fig. 3) y la información de estado HTTP incluida en las dos parejas de mensajes de petición y respuesta HTTP de la Fig. 3. De esta manera, se realiza aproximadamente una asociación entre la sesión HTTP de estado y la sesión SIP a la que se refiere el diálogo SIP. Como resultado, y a pesar de la falta de estado inherente del HTTP, el HUE 106 puede iniciar las sesiones hacia las entidades IMS y también puede ser el objetivo de las sesiones iniciadas por las entidades IMS.

Los mensajes HTTP ilustrados en la Fig. 3 se procesan por el Agente de Usuario HTTP 130 de la HIAF 108 mostrada en la Fig. 2. La configuración interna de los componentes lógicos del Agente de Usuario HTTP 130 se ilustra esquemáticamente en la Fig. 4.

Como se muestra en la Fig. 4, el Agente de Usuario HTTP 130 comprende tres capas distintas, a saber una capa de conexión de transacciones 140, una capa de administración de transacciones 142 y una capa de administración de diálogos 144. Conceptualmente, el cliente independiente y los componentes de servidor 142A, 142B dentro del Agente de Usuario HTTP 130 comparten la misma capa de conexión de transacciones 140 pero son entidades separadas en la capa de administración de transacciones 142. La capa de administración de diálogos 144 se extiende sobre ambos componentes 142A, 142B de la capa de administración de transacciones 142.

La capa de conexión de transacciones 140 y la capa de administración de transacciones 142 se configuran para realizar las operaciones de procesamiento basadas en transacción. Una transacción típicamente comprende el intercambio de un mensaje de petición SIP único y uno o más mensajes de respuesta SIP relacionados como parte de un diálogo SIP. Cada diálogo SIP, a su vez, incluye una o más transacciones individuales (tales como las transacciones INVITE, las transacciones non-INVITE y las peticiones de ACK, que constituyen su propia transacción).

Como ya se mencionó, los mensajes de petición y respuesta SIP individuales se asignan en parejas de mensajes de petición y respuesta HTTP separados en base a la información de estado HTTP. Es el propósito de la capa de conexión de transacción 140 explotar la asignación en contexto con la utilización de la información de estado HTTP

incluida dentro de las parejas de petición y respuesta HTTP para hacer coincidir cada mensaje de petición HTTP (que contiene, por ejemplo, una petición de transacción SIP) con su mensaje de respuesta HTTP asociado. Además, la capa de conexión de transacción 140 maneja los tiempos de espera y las retransmisiones HTTP. Para este propósito, la capa de conexión de transacción 140 implementa una máquina de estado separada que depende del tipo de componente de administración de transacción requerido (cliente 142A o servidor 142B) y el tipo de transacción (por ejemplo, transacción INVITE o non-INVITE).

La capa de administración de transacción 142 se dispone por encima de la capa de conexión de transacción 140 y es responsable de crear (o iniciar) y cancelar las transacciones SIP que pertenecen a los diálogos SIP individuales. La capa de administración de diálogos 144 mantiene la información de estado para cada diálogo SIP establecido. Además, la capa de administración de diálogos 144 comprende la lógica de comunicación entre elementos que interviene entre los componentes del cliente y el servidor 142A, 142B de cada Agente de Usuario HTTP 130 y administra la pila completa de capas de componentes lógicos.

A continuación, la cooperación de las capas de componentes lógicos individuales 140, 142 y 144 ilustrada en la Fig. 4 se tratará ejemplarmente en contexto con el diagrama de señalización esquemático ilustrado en la Fig. 5. En el escenario de mensajería de la Fig. 5, el HUE 106 inicia una transacción INVITE. Para este fin, el HUAC 106 B del HUE 106 emite un primer mensaje de petición HTTP como se muestra en la Fig. 5 (paso 1 en la Fig. 4). El mensaje de petición HTTP contiene varios elementos de información que incluyen la información de estado HTTP, una indicación del mensaje SIP en forma de una petición (INVITE) de transacción y una información de descripción de sesión (en forma de un ofrecimiento SDP). La información de estado HTTP se transmite como una cookie en la cabecera del mensaje de petición HTTP. La indicación del mensaje SIP y la información de descripción de sesión compatible con SDP, por otra parte, se transportan en el cuerpo del mensaje de petición HTTP.

El Protocolo de Descripción de Sesiones, o SDP, se describe en la RFC2327 y define una sintaxis para describir las sesiones multimedia con la información requerida para participar en esa sesión. Las descripciones de sesión se pueden enviar usando protocolos de aplicaciones existentes arbitrarios para el transporte.

El modelo de ofrecimiento/contestación como se define en la RFC3264 permite a los puntos finales usar SDP para obtener una visión compartida de un sesión. Algunos parámetros de sesión se negocian (por ejemplo, los códec a usar), mientras que otros simplemente se comunican desde un punto final a otro (por ejemplo, las direcciones IP). De acuerdo con el modelo de ofrecimiento/contestación de SDP, un punto final de comunicación (el 'oferente') genera un mensaje SDP que constituye la oferta. La oferta necesita ser transportada al otro punto final (el 'que contesta'). El que contesta genera una contestación, que es un mensaje SDP que responde al ofrecimiento presentado por el oferente. La contestación tiene una secuencia de medios de coincidencia para cada secuencia en el ofrecimiento, que indica si la secuencia se acepta o no. El modelo de ofrecimiento/contestación SDP no define un medio de transporte específico para entregar los mensajes SDP entre los puntos finales.

La información de estado HTTP recibida con el primer mensaje de petición HTTP de la Fig. 5 se transporta desde el HUAC 106B a la HIAF 108 en la forma ejemplar de una cookie. Se apreciará que otros mecanismos para transferir la información de estado HTTP (tal como los URL gruesos o los parámetros URI) se podrían utilizar alternativamente o adicionalmente.

El mensaje de petición HTTP desde el HUAC 106B se recibe en la capa de conexión de transacción 140 del Agente de Usuario HTTP 130 de la HIAF 108. En la capa de conexión de transacción 140, se procesa el mensaje de petición HTTP, y un mensaje de respuesta HTTP en respuesta al mensaje de petición HTTP se devuelve al HUAC 106B como se muestra en la Fig. 5 (paso 2 en la Fig. 4). El mensaje de respuesta HTTP opcionalmente puede incluir la información de estado HTTP (por ejemplo, en forma de una cookie).

Entonces, la petición de transacción, el ofrecimiento SDP y la información de estado HTTP se pasan desde la capa de conexión de transacción 140 al componente de cliente 142A de la capa de administración de transacción 142. En respuesta a la recepción de estos elementos, el componente de cliente 142A crea un nuevo caso de transacción de cliente (paso 3 en la Fig. 4). Después de la creación del nuevo caso de transacción de cliente, se crea un nuevo caso de diálogo SIP en la capa de administración de diálogo 144 (paso 4 en la Fig. 4) y un mensaje de petición SIP (mensaje INVITE) que incluye el ofrecimiento SDP se envía a la red IMS (es decir, a la S-CSCF 112) como se muestra en la Fig. 5 para iniciar la sesión SIP requerida.

En respuesta a la recepción del mensaje de petición SIP (INVITE) que incluye el ofrecimiento SDP, la S-CSCF 112 devuelve un mensaje de respuesta SIP con el código de respuesta 183 y una consulta SDP como se muestra en la Fig. 5. Tras la recepción del mensaje de respuesta SDP, la lógica de comunicación entre elementos dentro de la capa de administración de diálogo 144 da instrucciones al componente de servidor 142B de la capa de administración de transacción 142 para crear un nuevo caso de transacción de servidor (paso 5 en la Fig. 4) y entregar la contestación SDP recibida desde la S-CSCF 112 junto con el código de respuesta a la capa de conexión de transacción 140.

La capa de conexión de transacción 140 construye un nuevo mensaje de petición HTTP que transporta el código de respuesta, la contestación SDP así como una cookie con la información de estado HTTP como se recibe desde el

HUE 106 con el primer mensaje de petición HTTP. El mensaje de petición HTTP recién creado entonces se envía en un siguiente paso al HUAS 106A del HUE 106 como se muestra en la Fig. 5 (paso 6 en la Fig. 4). En respuesta a la recepción del mensaje de petición HTTP, el HUAS 106A devuelve un mensaje de respuesta HTTP a la HIAF 108 como también se muestra en la Fig. 5.

Dado que la misma (o únicamente asociable) información de estado HTTP se incluye tanto en el primer mensaje de petición HTTP enviado desde el HUAC 106B a la HIAF 108 y el segundo mensaje de petición HTTP enviado desde la HIAF 108 al HUAS 106A, el HUE 106 y la HIAF 108 pueden agrupar las dos parejas de mensajes de petición y respuesta HTTP nominalmente independientes en una sesión HTTP correspondiente a un diálogo SIP en forma de una transacción INVITE. Además, este mecanismo de gestión de estado HTTP también se puede usar para asignar los mensajes de petición y respuesta HTTP en la señalización SIP de diálogo adicional tal como las peticiones y respuestas de registro.

En caso que el HUE determine en base a la contestación SDP que ciertos parámetros (por ejemplo, los parámetros relacionados con los medios o los parámetros relacionados con la capacidad del terminal) necesitan ser renegociados, el patrón de mensajería tratado anteriormente puede repetir en sí mismo cuando el HUAC 106B envíe un nuevo mensaje de petición HTTP a la HIAF 108 que ofrece renegociar (ver la Fig. 5). En respuesta a este nuevo mensaje de petición HTTP, la HIAF 108 construye un mensaje PRACK con una nueva oferta y envía este mensaje a la S-CSCF 112. La S-CSCF 112 contesta al mensaje PRACK con un mensaje 200 OK. Entonces, y aún con referencia a la Fig. 5, la S-CSCF 112 envía un mensaje 200 (INVITE) a través de la HIAF 108 al HUE 106 y recibe un mensaje de ACK como respuesta.

Durante los diversos diálogos realizados en contexto con la señalización ilustrada en la Fig. 5, la capa de administración de diálogo 144 del Agente de Usuario HTTP 130 ilustrada en la Fig. 4 hace el seguimiento de todos los diálogos activos. Para este fin, la capa de administración de diálogo 144 mantiene una tabla de estado de diálogo 600 como se ilustra en la Fig. 6. La tabla de estado de diálogo 600 comprende las siguientes columnas. En la primera columna, se almacena la dirección local en forma del URI de SIP local usado en el diálogo particular. La segunda columna identifica el objetivo remoto (es decir, la S-CSCF 112) por su URI de SIP. La tercera columna indica la secuencia local, que es el número de índice del último mensaje de petición SIP enviado para el diálogo específico. En la cuarta columna, la secuencia remota indica el número de índice del último mensaje de petición SIP recibido. La columna de contacto indica la dirección IP del punto final remoto (esta columna es importante solamente para la comunicación entre HIAnet sin la intervención de la HIAF 108). En la columna ID de diálogo, se da a cada diálogo SIP un identificador localmente único.

En el escenario ilustrado en las Fig. 4 y 5, se supone que la HIAF 108 es capaz de conducir el modelo ofrecimiento/contestación SDP con el punto final SIP remoto (a través de la S-CSCF 112). Alternativamente, el modelo ofrecimiento/contestación SDP también se podría conducir directamente entre el HUE 106 y el punto final SIP remoto. Para este fin, el mensaje SDP se puede incluir en el cuerpo del mensaje de los mensajes de petición y respuesta HTTP enviados y recibidos por el HUE 106.

Habiendo descrito el concepto de mensajería general entre el HUE 106 y la S-CSCF 112 bajo el control de la HIAF 108, el mecanismo de gestión de estado realizado por el HSML 134 de la HIAF 108 (ver la Fig. 2) se describirá ahora en más detalle para proporcionar una mejor comprensión de cómo se puede realizar la asignación de los diálogos SIP en las sesiones de estado HTTP (es decir, la información de estado HTTP). Como se explico anteriormente, esta asignación se explota para agrupar múltiples parejas de mensajes de petición y respuesta HTTP en sesiones de estado HTTP que corresponden con las transacciones SIP que pertenecen a los diálogos SIP.

Los siguientes ejemplos de asignación se basan ejemplarmente en el diagrama de señalización de inicio de sesión detallado de la Fig. 9. El diagrama de señalización detallado de la Fig. 9 básicamente corresponde a los primeros y los dos últimos intercambios de mensajes entre el HUE 106 y la S-CSCF 112 (a través de la HIAF 108) de la Fig. 5 (con la excepción de que no se transfiere ninguna contestación SDP a través del penúltimo intercambio de mensaje en la Fig. 5).

Con referencia ahora a la Fig. 9, la mensajería comienza de nuevo con el HUE 106 que envía un mensaje de petición HTTP a la HIAF 108. El mensaje de petición HTTP incluye varias cookies HTTP para transportar distintos elementos de información. Las cookies ‘dialog-id’ y ‘transaction’ constituyen (tanto individualmente como en su combinación) la información de estado HTTP. Dado que en el presente caso la mensajería se inicia por el HUE 106, la información de estado HTTP se genera igualmente por el HUE 106. La información de estado HTTP indica que el mensaje de petición HTTP está asociado con el diálogo ali2alice1 y es parte del número de transacción 000001. En la presente realización, las peticiones SIP y las respuestas SIP correspondientes están a cuestas en mensajes de petición y respuesta HTTP separados. Como puede haber más de una petición pendiente para el mismo diálogo SIP, el número de transacción se usa por el HUE 106 como la información de estado encajar las respuestas HTTP con sus peticiones, y viceversa.

El id de llamada es en el caso más simple el call-id de SIP. No obstante, el id de llamada también se puede asignar a otro identificador que ocurre que ser más conveniente que el dialog-id. El contador de transacción es un identificador que corresponde a las sesiones de medios que existen dentro del diálogo SIP. Un ejemplo sería

múltiples secuencias de vídeo dentro de un diálogo SIP. El contador de transacciones pudiera ser usado en tal caso para distinguir entre estas diferentes secuencias de vídeo.

El elemento de información “method” en el cuerpo del primer mensaje de petición HTTP de la Fig. 9 indica que el HUE 106 requiere el inicio de una transacción INVITE en relación con un Agente de Usuario SIP remoto. La dirección SIP de este Agente de Usuario se incluye en la primera línea del estado GET (sip:alice@baba). Como se muestra en la Fig. 9, el cuerpo del mensaje de petición HTTP incluye un elemento de información adicional que transporta la información de descripción de sesión en forma de un ofrecimiento SDP.

En base a la información recibida a través del mensaje de petición HTTP desde el HUE 106, la HIAF 108 es informada de que se requiere una transacción INVITE (method=invite) y que un procedimiento de ofrecimiento/contestación SDP tiene que ser realizado. Ya que la sesión resultante se extenderá entre el dominio HTTP del HUE 106 por una parte y el dominio SIP de la S-CSCF 112 por otra parte, la información de estado HTTP necesita ser almacenada por la HIAF 108 para permitir una comunicación de estado con el HUE 106 en el contexto de esta sesión.

Para almacenar la información de estado HTTP, la HIAF llena las tablas locales en base a la información de estado HTTP recibida a través del mensaje de petición HTTP desde el HUE 106 y el ID de diálogo SIP asociado generado por la capa de administración de diálogo 144 como se trató anteriormente en contexto con la Fig. 4. Para este fin, el HSML 134 de la HIAF 108 mantiene dos tablas de asignación separadas, a saber una Tabla de Resolución de Diálogo (DRT) 700, como se ilustra en la Fig. 7, por una parte y una Tabla de Recuento de Transacciones (TCT) 800, como se ilustra en la Fig. 8, por otra parte. Ambas tablas se mantienen y actualizan por el HSML 134 con el propósito de asignar las sesiones de estado HTTP a los diálogos SIP así como para monitorizar el progreso de las transacciones SIP y las sesiones HTTP.

Como se muestra en la Fig. 7, la DTR 700 asigna el ID de diálogo SIP como se asigna por la capa de administración de diálogo 144 a un ID diálogo HIAF (ali2alice1) como se recibe en el presente caso desde el HUE 106. Usando cualquier ID de diálogo contenido en la DRT 700, es posible para el HSML 134 determinar el estado actual del diálogo y construir cualquier mensaje SIP necesario para continuar, modificar o terminar el diálogo. El estado de diálogo para cada diálogo se mantiene por el Agente de Usuario SIP 132 para cada diálogo que implica a la HIAF 108.

La TCT 800 mostrada en la Fig. 8 se usa por el HSML 134 en conjunto con la DRT 700 de la Fig. 7 para producir los mensajes de petición y respuesta HTTP adecuados dirigidos al HUE 106. Una entrada en la TCT 800 indica que hay una transacción activa entre el HUE 106 y la HIAF 108 con un número de transacción dado. Los números de transacción se usarán en la señalización intercambiada entre el HUE y los puntos finales de la HIAF para completar las transacciones. Dos transacciones dentro del mismo diálogo SIP no deberían usar el mismo número de transacción, independientemente de si estas transacciones se emiten por el HUE 106 o la HIAF 108. Se debería señalar que además de la TCT 800 de la HIAF 108 mostrada en la Fig. 8, el HUE 106 mantendrá independientemente su propia tabla de recuento de transacciones de una manera similar a la TCT 800.

En base a la DRT 700 y la TCT 800, el ID de diálogo SIP se puede buscar de esta manera cuando se conoce el ID de diálogo de la HIAF y el número de transacción. Cada vez que la HIAF 108 determina que un nuevo diálogo está a punto de ser establecido, asigna un nuevo ID de diálogo de la HIAF y actualiza la DRT 700 (nuevo ID de diálogo SIP) y la TCT 800 (nuevo número de transacción) en consecuencia. Como se muestra en las Fig. 7 y 8, la DRT 700 y la TCT 800 se pueden usar para mantener otros datos de estado. Tales otros datos de estado pueden incluir los parámetros del ramal SIP.

Siempre que la HIAF 108 recibe un mensaje de petición HTTP desde el HUAC del HUE 106, realiza las siguientes tareas en relación con la DRT 700 y la TCT 800. En un primer paso, la HIAF 108 determina si el HUE 106 solicitante tiene un registro válido con un tiempo de vida pendiente. Para este fin, la HIAF 108 busca a través de su tabla de registro local (como se trata en más detalle más adelante) una entrada que contenga la dirección IP que ha obtenido el mensaje de petición HTTP entrante (es decir la dirección IP del HUE 106). En un siguiente paso, la HIAF 108 usa la información de la tabla de registro, la DRT 700 y el mensaje de petición HTTP para construir el mensaje de petición SIP requerido. En el mismo momento, la HIAF 108 actualiza su DRT 700.

En un paso adicional, la HIAF 108 utiliza la información adquirida a partir de la DRT 700 y la TCT 800 para construir un mensaje de respuesta HTTP para el HUE 106. Como se ilustra en la Fig. 9, el mensaje de respuesta HTTP transporta el código 200 OK. Se debería señalar que el código de estado contenido en el mensaje de respuesta HTTP se relaciona meramente con la capacidad de la HIAF 108 para ejecutar los contenidos de la petición HTTP, y no con el resultado de la ejecución. En otras palabras, en el caso ilustrado en la Fig. 9 el código de estado 200 OK incluido en el mensaje de respuesta HTTP solamente indica que es válido el mensaje de petición HTTP previo, pero no que el mensaje INVITE enviado por la HIAF 108 a la S-CSCF 112 fue exitoso. Si, por cualquier razón, una petición HTTP específica no se puede servir por la HIAF 108, entonces se devolverá un mensaje de respuesta HTTP con un código de estado non-200 (por ejemplo, un código 4xx de SIP) y una frase con la razón adecuada al HUE 106.

Siempre que la HIAF 108 recibe un mensaje SIP de la red IMS (es decir, desde la S-CSCF 112), se realizan las siguientes tareas (ver la Fig. 9). Primero, se actualiza la DRT 700 con respecto al tipo de mensaje SIP recibido y la información contenida en el mensaje SIP. La HIAF 108 entonces usa la información de la tabla de registro, la DRT 700 y la TCT 800 para producir una petición HTTP que se envía al HUAS del HUE 106 (ver la Fig. 9). En un siguiente paso, la HIAF 108 recibe un mensaje de respuesta HTTP desde el HUAS del HUE 106. Como llega a ser evidente a partir de la Fig. 9, la información de estado HTTP contenida en el mensaje de respuesta HTTP es la misma que la información de estado HTTP contenida en el mensaje de respuesta HTTP enviado inicialmente por el HUE 106 a la HIAF 108 en contexto con iniciar la transacción INVITE requerida.

En la realización de señalización tratada anteriormente en contexto con la Fig. 9, se supone que el establecimiento de sesión se desencadena desde el dominio HTTP por el HUE 106. De acuerdo con unas realizaciones de señalización alternativas que serán tratadas ahora con referencia a las Fig. 10 y 11, el establecimiento de sesión se desencadena por una entidad habilitada con SIP tal como el AS de SIP 114 ilustrado en la Fig. 1 o un equipo de usuario habilitado con SIP.

La Fig. 10 ilustra cómo se puede realizar un escenario de ofrecimiento/contestación SDP complejo usando la HIAF 108 asignando los mensajes de petición SIP en los mensajes petición/respuesta HTTP, y viceversa. La señalización entrante desde la entidad habilitada con SIP se pasa por la S-CSCF 112 a la HIAF 108 como se ilustra por el mensaje INVITE (que incluye un ofrecimiento SDP) en la Fig. 10. En respuesta a la recepción del mensaje INVITE, la HIAF 108 genera la información de estado HTTP adecuada y envía la misma junto con el ofrecimiento SDP en un mensaje de petición HTTP al HUAS 106A del HUE 106. El HUAS 106A responde con un mensaje de respuesta HTTP que incluye de nuevo la información de estado HTTP. La mensajería continúa con el HUAC 106B del HUE 106 enviando un mensaje de petición HTTP con la información de estado HTTP y una contestación SDP a la HIAF 108. La HIAF 108 asigna este mensaje de petición HTTP en una respuesta SIP (código de estado 183) que incluye la contestación SDP y en el mismo momento reconoce la recepción del mensaje de petición HTTP mediante un mensaje de respuesta HTTP al HUE 106.

Entonces, la HIAF 108 recibe un mensaje PRACK desde la S-CSCF 112 y asigna este mensaje a un nuevo mensaje de petición HTTP incluyendo de nuevo la información de estado HTTP generada previamente así como un nuevo ofrecimiento SDP (offer2) como se recibe a través del mensaje PRACK. El nuevo mensaje de petición HTTP enviado desde la HIAF 108 al HUAS 106A provoca un reconocimiento en forma de un mensaje de respuesta HTTP. El intercambio de mensajes adicional tiene similitudes con el intercambio de mensajes tratado anteriormente en contexto con la Fig. 5, pero en la dirección contraria. Similar a la situación ilustrada en la Fig. 5, se requiere la comunicación interna entre el HUAS 106A y el HUAC 106B del HUE 106 para facilite la reacción con los mensajes de petición HTTP enviados por el HUAC 106B después de la recepción de los mensajes de petición HTTP por el HUAS 106A.

El diagrama de señalización de la Fig. 11 ilustra en más detalle la señalización implicada con la recepción de un mensaje INVITE desde la S-CSCF 112 por la HIAF 108 para el escenario en que el HUE 106 es el destinatario de una petición de transacción. Los tres primeros mensajes de la Fig.11 corresponden a los tres primeros mensajes de la Fig. 10. El intercambio de mensajes adicional ilustrado en la Fig. 11 tiene similitudes con el intercambio de mensajes ilustrado en la Fig. 9, pero en la dirección contraria. Se cree que en base a las explicaciones dadas en contexto con la Fig. 9, el diagrama de señalización de la Fig. 11 es en gran medida auto explicativo. Por esta razón, se omite aquí una discusión más detallada del mismo. Se señala solamente que la información de contacto negociada durante el modelo de ofrecimiento/contestación SDP corresponde con las parejas dirección IP/puertos asignada por el HUE 106 y los puntos finales SIP a la sesión particular. Como tal, la sesión se conduce directamente entre el HUE 106 y los puntos finales SIP.

Los diagramas de señalización de las Fig. 12 y 13 ilustran la señalización de terminación de sesiones iniciada por el HUE 106 por una parte (Fig. 12) y a través de la S-CSCF 112 por otra parte (Fig. 13). La terminación de sesiones en cada caso implica la transmisión de un mensaje BYE o bien a la S-CSCF 112 o bien a través de la S-CSCF 112. El mensaje BYE se acompaña en cada caso por dos parejas de mensajes de petición y respuesta HTTP. Como llega a ser evidente a partir de las Fig. 12 y 13, la misma información de estado HTTP (dialog-id=alice2ali1; transaction=000008) se incluye en cada uno de estos cuatro mensajes HTTP. En base a la información de estado HTTP, las dos parejas de mensajes de petición y respuesta HTTP están limitadas de esta manera al diálogo SIP correspondiente como se ilustra en las tablas de las Fig. 7 y 8.

En las realizaciones siguientes, se explican algunos aspectos adicionales relacionados con la HIAF que se pueden implementar en combinación con las realizaciones anteriores o de una manera separada. Específicamente, se tratan los aspectos técnicos del descubrimiento de la HIAF, la transcodificación de medios HIAF, la autentificación HIAF y los mensajes de registro HIAF.

El descubrimiento HIAF implica la determinación de la dirección de la HIAF 108 en la HIAnet 104 (ver la Fig. 1). Cuando el HUE 106 despliega el Servicio General de Paquetes de Radio (GPRS) como el medio de acceso de red, la dirección de la HIAF 108 se puede determinar durante la activación del contexto del Protocolo de Datos por Paquetes (PDP) general o de señalización. Potencialmente, se puede necesitar que sea definido un nuevo Nombre de Punto de Acceso (APN) para la activación del contexto PDP de Acceso IMS de HTTP.

Alternativamente, el HUE 106 puede usar el Protocolo de Configuración Dinámica de Servidor (DHCP) para descubrir la HIAF 108. Si la dirección de la HIAF 108 se devuelve por el DHCP como un Nombre de Dominio Totalmente Cualificado (FQDN), entonces la dirección IP de la HIAF 108 se puede adquirir a través del Sistema de Nombres de Dominio (DNS) como es bien conocido en la técnica. Como una posibilidad adicional, la HIAF 108 se puede descubrir automáticamente con la ayuda de un Protocolo de Autoconfiguración Intermediario (PAD) tal como el estándar del Protocolo de Autodescubrimiento Intermediario Web (WPAD) o la Autoconfiguración Intermediaria (PAC).

La HIAF 108 también puede realizar las operaciones de transcodificación de medios. Durante la negociación de un formato de sesión de medios, la HIAF 108 puede declararse a sí misma como la destinataria de la sesión de medios. Como resultado, la sesión de medios se recibe por la HIAF 108, y la HIAF 108 realiza la transcodificación de medios en un formato de sesión que se ha negociado previamente entre (o preconfigurado en) la HIAF 108 y el HUE 106. Después de la operación de transcodificación, la nueva sesión de medios se entrega al HUE 106. Tal transcodificación de medios basada en la HIAF ayuda a reducir la carga de procesamiento y la complejidad en el lado del HUE 106.

Ahora, se tratarán en más detalle varios aspectos relacionados con la autentificación y el registro que preceden una sesión de medios real.

El HTTP ofrece una estructura de autentificación con soporte para un esquema básico (autentificación básica) y un esquema basado en las generaciones de claves criptográficas (autentificación de acceso de resumen) ambos que implementan un mecanismo de autentificación reto-respuesta. En autentificación básica, un Cliente de Agente de Usuario responderá a un reto del Servidor de Agente de Usuario emitiendo una cadena codificada base64 que contiene su nombre de usuario y contraseña. El hecho de que la autentificación básica dicte la transmisión de las credenciales de usuario casi en texto claro hace este esquema de autentificación inadecuado para ciertas aplicaciones. En autentificación de acceso de resumen, el cliente de Agente de Usuario es retado con un número aleatorio y se le pide que devuelva una cadena producida aplicando un algoritmo de resumen con un secreto compartido sobre el número aleatorio y un conjunto de datos.

Un HUE 106 que desea ser alcanzable en un URI de SIP o disfrutar de los servicios de valor añadido de IMS tiene que realizar inicialmente el registro IMS. Para este fin, la HIAF 108 puede, por ejemplo, proporcionar el modo de autentificación de la Pasarela de Confianza.

Generalmente, el registro HIAF implica un registro HTTP conducido entre el HUE 106 y la HIAF 108, y un registro SIP conducido entre la HIAF 108 y la red IMS 102. En el modo de autentificación de la Pasarela de Confianza, la HIAF 108 autentifica cada HUE 106 a través de la autentificación HTTP (por ejemplo, usando autentificación de acceso básica o de resumen) y confirma a la red IMS 102 la autenticidad del HUE 106. En este modo de funcionamiento, la HIAF 108 es autorizada a actuar a favor del HUE 106 y originar (o responder a) las peticiones y respuestas de registro SIP intercambiadas con la red IMS 102. Los registros HTTP y SIP en ambos lados de la HIAF 108 son independientes entre sí. Esto significa que un registro HTTP con éxito no significa necesariamente que el registro SIP sea igualmente un éxito.

A continuación, el contenido de los mensajes de registro HIAF así como los pasos básicos del método de autentificación de la Pasarela de Confianza se tratarán en más detalle. En este sentido se asumirá que el dominio SIP está considerando la HIAF 108 como de confianza. Consecuentemente, todas las peticiones de registro que vienen de la HIAF 108 se aceptarán automáticamente. No obstante, la HIAF 108 no confía en los HUE 106, los cuales en consecuencia tienen que ser autentificados.

Cada petición de registro HIAF desde un HUE 106 incluye un mensaje de petición HTTP que contiene información que indica que la sesión HTTP está introduciendo el estado de registro. Un posible mensaje de petición HTTP enviado desde el HUE 106 a la HIAF 108 se muestra en el diagrama de señalización esquemático de la Fig. 14 ilustrando el registro HIAF de la Pasarela de Confianza. Como llega a ser evidente a partir del primer mensaje de petición HTTP en este diagrama de señalización, el HUE 106 está usando la cookie “method=register” para notificar a la HIAF 108 que la sesión HTTP está introduciendo el estado de registro.

La respuesta de registro de la HIAF 108 es un mensaje de respuesta HTTP. Si el código de estado del mensaje de respuesta HTTP es 200 OK como se ilustra en la Fig. 14, entonces la petición de registro HIAF se ha procesado con éxito. En tal caso, el mensaje de respuesta HTTP correspondiente también contendrá información que indica el nuevo estado introducido por la sesión HTTP. En el ejemplo dado en la Fig. 14, la HIAF 108 está emitiendo un mensaje de petición HTTP que incluye la cookie “code=401”. Esta cookie indica al HUE 106 que tiene que autentificarse a sí mismo con la red IMS 102. El valor del código de 401 corresponde al código de estado del mensaje de respuesta SIP recibido por la HIAF 108.

Se debería señalar que el HUE 106 y la HIAF 108 no afrontan el problema de tener que determinar una coincidencia entre los mensajes de petición y respuesta de registro HIAF dado que estos mensajes se transportan sobre una y la misma conexión TCP. Por esta razón, no necesita ser iniciada la sesión HTTP de estado.

A continuación, se describirá en más detalle un ejemplo de un proceso de autentificación de la Pasarela de

Confianza con referencia al diagrama de señalización de la Fig. 14 y las tablas de las Fig. 15 y 16. En una realización presente el registro HIAF con la autorización de la Pasarela de Confianza se basa en las siguientes suposiciones:

1. La información de la autorización se ha establecido a priori entre el HUE 106 y la HIAF 108. Es decir, el HUE 106 está en una posición de autentificarse a sí mismo con la HIAF 108 usando o bien la autentificación básica o bien la de resumen.

2. La HIAF 108 mantiene una tabla de abonados 1500 como se muestra en la Fig. 15 que asigna los nombres de usuario de autentificación del HUE a los abonados IMS. La tabla de abonados 1500 contiene todos los campos necesarios con los que se puede autentificar el HUE 106. La columna de esquema de autentificación de la tabla 1500 indica el método específico por el cual el usuario debería ser autentificado. Las restantes columnas se usan para construir la cabecera de autentificación (con la cual se desafía al usuario) y para verificar la validez de la respuesta del usuario.

La autentificación de la Pasarela de Confianza básicamente comprende dos partes. Durante la primera parte, el HUE 106 es autentificado con la HIAF 108. El método de autentificación HTTP específico usado a este respecto depende del perfil del abonado según se define en la tabla de abonados 1500. Por ejemplo, un abonado con la entrada de la tabla “de resumen” en la columna del esquema de autentificación será autentificado usando autentificación de resumen.

Con referencia ahora al diagrama de señalización de la Fig. 14, tras la recepción del mensaje de petición HTTP inicial, el HSML 134 de la HIAF 108 (ver la Fig. 2) realiza los siguientes pasos. En un primer paso, el HSML 134 evalúa la cookie en el mensaje de petición HTTP y determina el propósito del mensaje de petición HTTP que ha sido recibido. La cookie “method=register” indica que este mensaje es una petición de registro HIAF. En un siguiente paso, y usando el contenido de la petición URI en la línea de petición de la petición de registro HIAF, el HSML 134 realiza una búsqueda en la tabla de abonado 1500 para adquirir el perfil de abonado. En un siguiente paso, el HSML 134 realiza la autentificación de acceso con respecto al método de autentificación definido para el abonado en la tabla de abonado 1500.

Una vez que la autentificación se ha realizado con éxito y antes de la transmisión del mensaje de respuesta HTTP (200 OK) al HUE 106, la HIAF 108 crea una entrada para el usuario en una tabla de registro HIAF 1600 como se ilustra en la Fig. 16.

La tabla de registro 1600 tiene varias columnas. La columna de Nombre de Usuario de Autentificación indica el Nombre de Usuario de Autentificación usado por el HUE 106 durante el registro HIAF. La columna de ID de Usuario Público indica el ID correspondiente del abonado y se puede reservar para uso futuro. La columna de Dominio Local del HUE 106 está rellenada con el contenido correspondiente de la cabecera de autentificación en el mensaje de petición de registro HIAF. La columna de Dirección IP está rellenada con la Dirección IP del HUE 106. Esta dirección se deriva generalmente de la Dirección IP fuente de los mensajes de petición de registro HIAF entrantes. La columna de Estado indica el Estado de los registros HIAF y la columna de Tiempo de Vida indica el Tiempo de Vida de los registros HIAF.

Después de cada autentificación con éxito, se crea y se rellena una nueva entrada en la tabla de registro HIAF 1600 como sigue. Los campos de Nombre de Usuario de Autentificación y Dominio Local se rellenan con los valores usados por el abonado durante la autentificación. La lista de ID de Usuario Público se mantiene vacía y se reserva para uso futuro. El campo de dirección IP se fija a la dirección usada por el HUE 106 durante el registro HIAF. El campo de Estado se fija a REGISTRADO y el tiempo de vida se deja vacío.

La HIAF 108 entonces construye un mensaje REGISTER de SIP (ver la Fig. 14) rellenando el campo individual de mensaje como sigue. Los campos De y A se rellenan con el valor dado por la Petición URI en la petición de registro HIAF. Se crea un nuevo ID de Llamada que puede contener en su fondo la dirección IP del HUE 106. Este ID de Llamada tiene que ser grabado en las entradas respectivas de la tabla de registro 1600. El campo de Contacto se rellena con el propio URI de SIP de la HIAF 108. Este es básicamente la dirección donde la HIAF 108 desea recibir las invitaciones de sesión futuras para este abonado. En un paso adicional, se añade una cabecera Path indicando su propio URI de SIP que conduce a la red IMS 102 a creer que la HIAF 108 está actuando como la P-CSCF 110 para un abonado IMS (ver la Fig. 1).

Para cada mensaje de respuesta de registro SIP recibido desde la red IMS 102, el HSML 134 de la HIAF 108 realiza las siguientes acciones. En un primer paso, el HSML 134 actualiza el valor del tiempo de vida de la entrada respectiva en la tabla de registro 1600 con el valor correspondiente en el mensaje de respuesta de registro SIP. Entonces construye un mensaje de respuesta HTTP con una línea de estado 200 OK que contiene la cookie “lifetime=xxxx” en su cuerpo de mensaje. Esta cookie indica al HUE 106 el tiempo de vida del registro HIAF.

Como ha llegado a ser evidente a partir de las realizaciones anteriores, las técnicas presentadas aquí dentro permiten al equipo de usuario habilitado con HTTP iniciar, conducir y terminar sesiones con un Agente de Usuario SIP en base a las asignaciones que se establecen entre los diálogos SIP y las sesiones de estado HTTP. El paradigma de sesión se puede extender de esta manera en el dominio HTTP, lo cual aumenta la interoperabilidad

general de las redes que confían en distintos protocolos de la capa de aplicaciones. La conversión de señalización se puede realizar de manera eficiente en una interfaz entre los dominios HTTP y SIP.

En lo anteriormente mencionado, se han descrito los principios, las realizaciones preferentes y varios modos de implementar las técnicas reveladas aquí dentro. No obstante, la presente invención no debería ser construida como que está limitada a los principios, realizaciones y modos particulares tratados anteriormente. De esta manera se apreciará que se pueden hacer variaciones y modificaciones por una persona experta en la técnica sin salir del alcance de la presente invención como se define por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método para realizar la conversión de señalización entre una sesión de estado del Protocolo de Transferencia Hipertexto, o HTTP, y un diálogo del Protocolo de Inicio de Sesiones, o SIP, **caracterizado por:**

- recibir desde una entidad habilitada con HTTP un primer mensaje de petición HTTP, el primer mensaje de petición HTTP que incluye la información de estado HTTP;

- crear un primer mensaje SIP en respuesta a la recepción del primer mensaje de petición HTTP, el primer mensaje SIP que pertenece a un diálogo SIP;

- enviar el primer mensaje SIP a una entidad habilitada con SIP; y

- establecer una asignación entre la información de estado HTTP y el diálogo SIP.

2. El método de la reivindicación 1, que además comprende devolver un primer mensaje de respuesta HTTP a la entidad habilitada con HTTP.

3. El método de la reivindicación 1 o 2, que además comprende:

- recibir un segundo mensaje SIP;

- determinar el diálogo SIP al cual pertenece el segundo mensaje SIP;

- determinar la información de estado HTTP asociada con el diálogo SIP;

- generar un segundo mensaje de petición HTTP que incluye o que referencia la información de estado HTTP determinada de esta manera; y

- enviar el segundo mensaje de petición HTTP a la entidad habilitada con HTTP.

4. El método de la reivindicación 3, que además comprende recibir un segundo mensaje de respuesta HTTP en respuesta al segundo mensaje de respuesta HTTP desde la entidad habilitada con HTTP.

5. El método de cualquiera de las reivindicaciones precedentes, en el que basado en la información de estado HTTP la pareja de primeros mensajes de petición y respuesta HTTP así como la pareja de segundos mensajes de petición y respuesta HTTP se agrupan en la sesión de estado HTTP y/o en el que el primer mensaje de petición HTTP además incluye información de dirección indicativa de un Agente de Usuario SIP de la entidad habilitada con SIP, y en el que la información de la dirección se usa para dirigir el primer mensaje SIP al Agente de Usuario SIP y/o en el que el primer mensaje de petición HTTP además incluye información de diálogo HTTP, y en el que la información de diálogo HTTP se asigna a la información de diálogo SIP y/o en el que el primer mensaje de petición HTTP además incluye información de descripción de sesión, y que además comprende insertar la información de descripción de sesión incluida en el primer mensaje de petición HTTP en el primer mensaje SIP.

6. El método de la reivindicación 5, en el que la información de descripción de sesión se envía en un contexto de ofrecimiento/contestación del Protocolo de Descripción de Sesiones, o SDP.

7. El método de cualquiera de las reivindicaciones precedentes, en el que la información de estado se incluye en al menos uno del primer mensaje de petición HTTP y el segundo mensaje de petición HTTP en forma de al menos uno de una cookie HTTP, un Localizador de Recursos Universal grueso, o URL grueso, un parámetro HTTP y una componente de consulta y/o en el que el primer mensaje de petición HTTP incluye una indicación de mensaje SIP indicativa de al menos uno de un método SIP, un código SIP y un código de estado HTTP.

8. Un método para realizar la conversión de señalización entre un diálogo de Protocolo de Inicio de Sesiones, o SIP, y una sesión de estado del Protocolo de Transferencia de Hipertexto, o HTTP, **caracterizado por:**

- recibir desde una entidad habilitada con SIP un primer mensaje SIP, el primer mensaje SIP que pertenece a un diálogo SIP;

- establecer una asignación entre la información de estado HTTP y el diálogo SIP;

- crear un primer mensaje de petición HTTP indicativo de un contenido del primer mensaje SIP, el primer mensaje de petición HTTP que incluye la información de estado HTTP asignada en el diálogo SIP; y

- enviar el primer mensaje de petición HTTP a una entidad habilitada con HTTP.

9. El método de la reivindicación 8, que además comprende recibir un primer mensaje de respuesta HTTP en respuesta al primer mensaje de respuesta HTTP desde la entidad habilitada con HTTP.

10. El método de la reivindicación 8 o 9, que además comprende

- recibir un segundo mensaje de petición HTTP, el segundo mensaje de petición HTTP que incluye la información de estado HTTP y una indicación opcional de un segundo mensaje SIP que va a ser creado;

- determinar el diálogo SIP asignado en la información de estado HTTP;

- crear un segundo mensaje SIP en respuesta a la recepción del segundo mensaje de petición HTTP en base a la indicación opcional en el segundo mensaje de petición HTTP y el diálogo SIP determinado; y

- enviar el segundo mensaje SIP a la entidad habilitada con SIP.

11. El método de la reivindicación 10, que además comprende devolver un segundo mensaje de respuesta HTTP a la entidad habilitada con HTTP.

12. El método de las reivindicaciones 8 a 11, en el que en base a la información de estado HTTP la pareja de primeros mensajes de petición y respuesta HTTP así como la pareja de segundos mensajes de petición y respuesta HTTP se agrupan en la sesión de estado HTTP y/o el método que además comprende generar la información de estado HTTP en respuesta a la recepción del primer mensaje SIP.

13. El método de cualquiera de las reivindicaciones precedentes, en el que la entidad habilitada con HTTP es un equipo de usuario y/o en el que la entidad habilitada con SIP es una entidad del Subsistema Multimedia de Protocolo de Internet (IMS) y/o en el que el diálogo SIP se realiza en uno de un contexto de registro de usuario, un contexto de inicio de sesión y un contexto de terminación de sesión.

14. Un producto de programa informático que comprende partes de código de programa para realizar los paso de cualquiera de las reivindicaciones precedentes cuando el producto de programa informático se ejecuta en un dispositivo informático.

15. El producto de programa informático de la reivindicación 14, almacenado en un medio de grabación legible por ordenador.

16. Un aparato (108) para realizar la conversión de señalización entre una sesión de estado del Protocolo de Transferencia Hipertexto, o HTTP, y un diálogo del Protocolo de Inicio de Sesiones, o SIP, **caracterizado por:**

- un Agente de Usuario HTTP (130) adaptado para recibir desde una entidad habilitada con HTTP un primer mensaje de petición HTTP, el primer mensaje de petición HTTP que incluye la información de estado HTTP;

- un Agente de Usuario SIP (132) adaptado para crear y enviar un primer mensaje SIP a una entidad habilitada con SIP en respuesta a la recepción del primer mensaje de petición HTTP, el primer mensaje SIP que pertenece a un diálogo SIP; y

- una lógica de asignación (134) adaptada para establecer una asignación entre la información de estado HTTP y el diálogo SIP.

17. El aparato de la reivindicación 16, en el que el aparato se adapta para realizar los pasos de cualquiera de las reivindicaciones 2 a 7.

18. Un aparato (130) para realizar la conversión de señalización entre un diálogo del Protocolo de Inicio de Sesiones, o SIP, y una sesión de estado del Protocolo de Transferencia Hipertexto, o HTTP, **caracterizado por:**

- un Agente de Usuario SIP (132) adaptado para recibir desde una entidad habilitada con SIP un primer mensaje SIP, el primer mensaje SIP que pertenece a un diálogo SIP;

- una lógica de asignación (134) adaptada para establecer una asignación entre la información de estado HTTP y el diálogo SIP;

- un Agente de Usuario HTTP (130) adaptado para crear y enviar un primer mensaje de petición HTTP indicativo de un contenido del primer mensaje SIP a una entidad habilitada con HTTP, el primer mensaje de petición HTTP que incluye la información de estado HTTP asignado en el diálogo SIP.

19. El aparato de la reivindicación 18, en el que el aparato se adapta para realizar los pasos de cualquiera de las reivindicaciones 9 a 13.

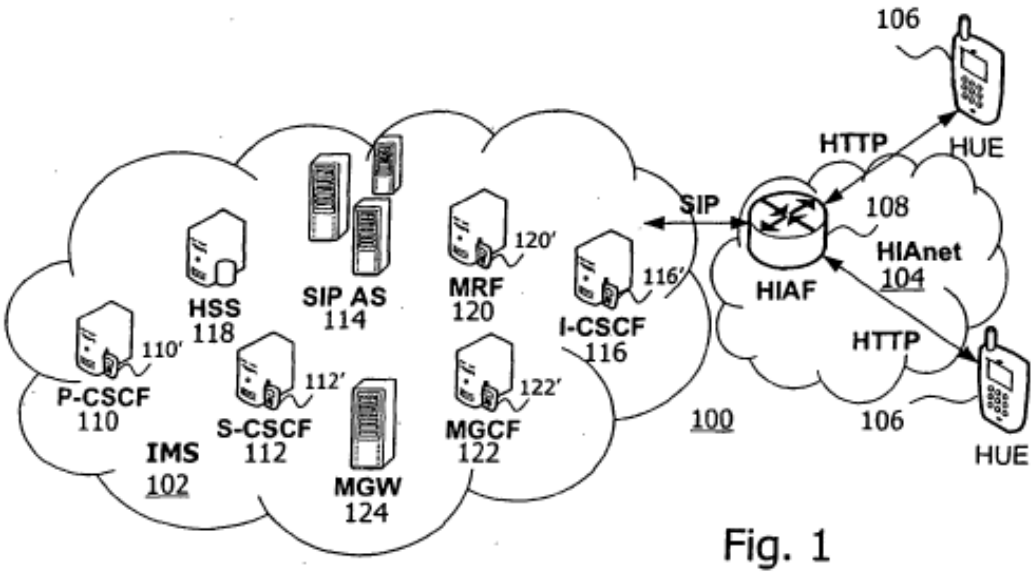
106
HTTP
HUE
SIP
108
HIAnet
104
HIAF
HTTP
106
HUE
100
HSS
118
SIP AS
114
MRF
120
120'
I-CSCF
116
116'
110'
P-CSCF
110
112'
S-CSCF
112
IMS
102
MGW
124
MGCF
122
122'

Fig. 1

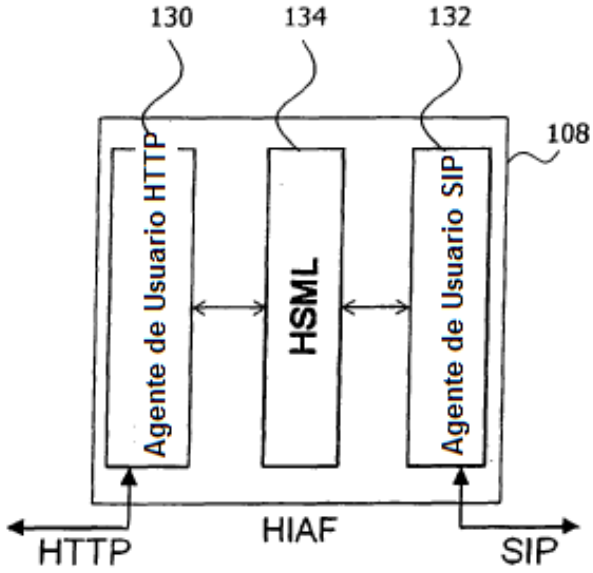
130
134
132
108
Agente de Usuario HTTP
HSML
Agente de Usuario SIP
HTTP
HIAF
SIP

Fig. 2

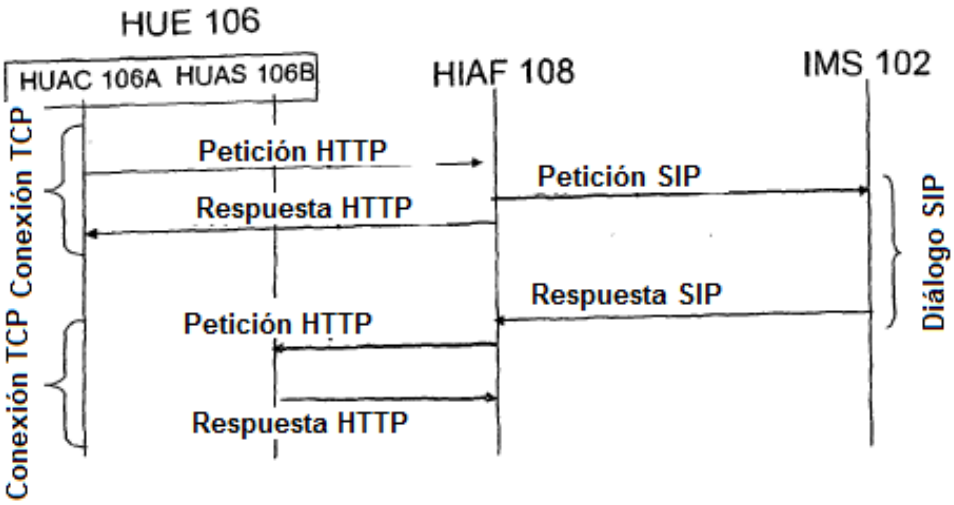
HUE 106
HUAC 106A HUAS 106B
HIAF 108
IMS 102
Conexión TCP Conexión TCP
Petición HTTP
Respuesta HTTP
Petición SIP
Respuesta SIP
Diálogo SIP
Petición HTTP
Respuesta HTTP

Fig. 3

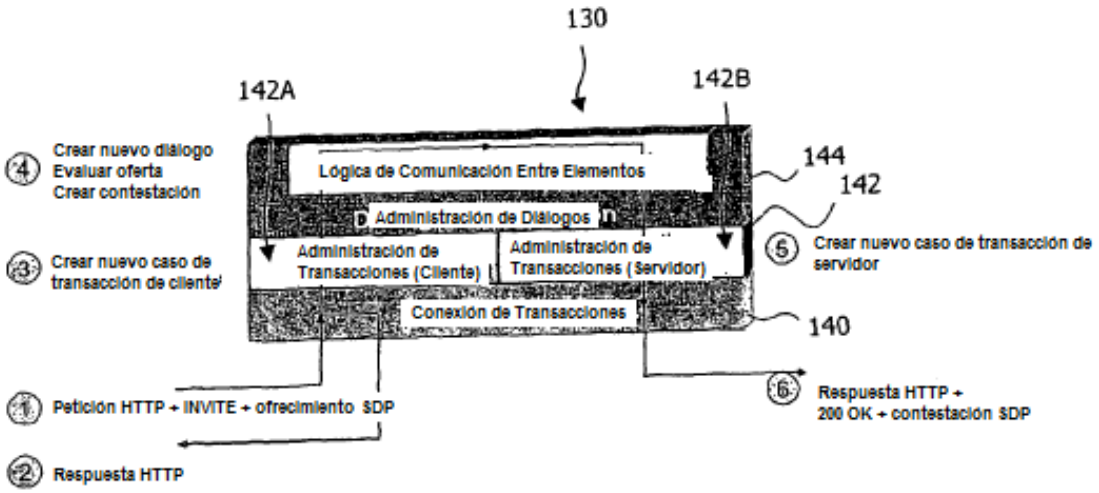
130
142A
142B
144
142
140
Lógica de Comunicación Entre Elementos
Administración de Diálogos
Administración de Transacciones (Cliente)
Administración de Transacciones (Servidor)
Conexión de Transacciones
4 Crear nuevo diálogo Evaluar oferta Crear contestación
3 Crear nuevo caso de transacción de cliente
5 Crear nuevo caso de transacción de servidor
1 Petición HTTP + INVITE + ofrecimiento SDP
2 Respuesta HTTP
6 Respuesta HTTP + 200 OK + contestación SDP

Fig. 4

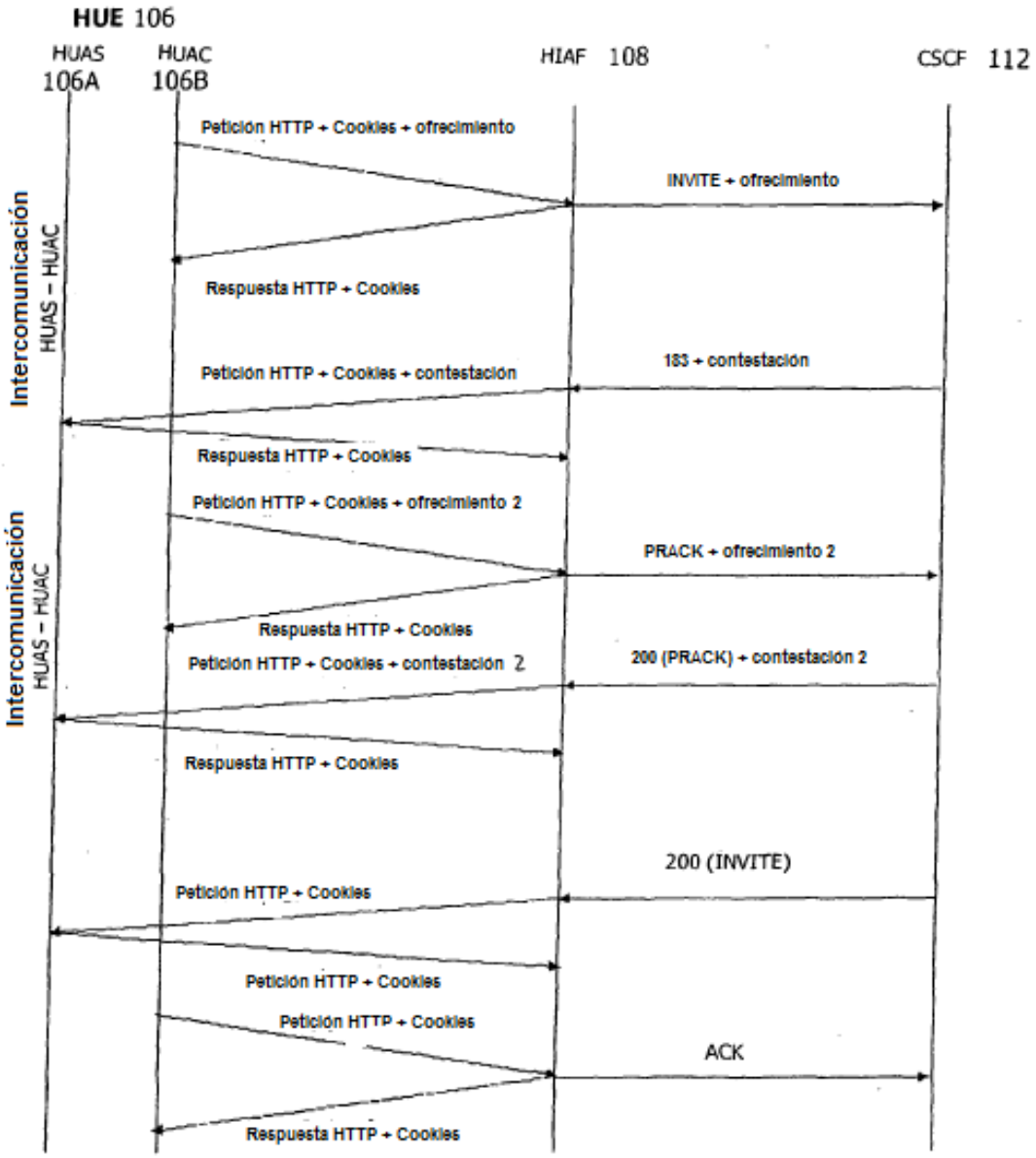
HUE 106
HUAS 106A
HUAC 106B
HIAF 108
CSCF 112
Intercomunicación HUAS – HUAC
Intercomunicación HUAS – HUAC
Petición HTTP + Cookies + ofrecimiento
INVITE + ofrecimiento
Respuesta HTTP + Cookies
183 + contestación
Petición HTTP + Cookies + contestación
Respuesta HTTP + Cookies
Petición HTTP + Cookies + ofrecimiento 2
PRACK + ofrecimiento 2
Respuesta HTTP + Cookies
200 (PRACK) + contestación 2
Petición HTTP + Cookies + contestación 2
Respuesta HTTP + Cookies
200 (INVITE)
Petición HTTP + Cookies
Petición HTTP + Cookies
Petición HTTP + Cookies
ACK
Respuesta HTTP + Cookies

Fig. 5

Dirección Local	Objetivo Remoto	Secuencia Local	Secuencia Remota	Contacto	ID de Diálogo
(URI de SIP Local)	(URI de SIP Remoto)	Índice de última petición emitida	Índice de última petición recibida	Dirección IP Remota	ID de Diálogo de diálogo activo
ali@test	alice@home	1	-	10.8.10.10	XXXXXXXX

600

Fig. 6

ID de Diálogo HIAF	ID de Diálogo SIP	Otros datos de estado
ali2alice1	XXXXXXXX	
rita2janni1	YYYYYYYY	

700

Fig. 7

ID de Diálogo HIAF	Transacción	Otros datos de estado
ali2alice1	00000001	
rita2janni1	00000002	

800

Fig. 8

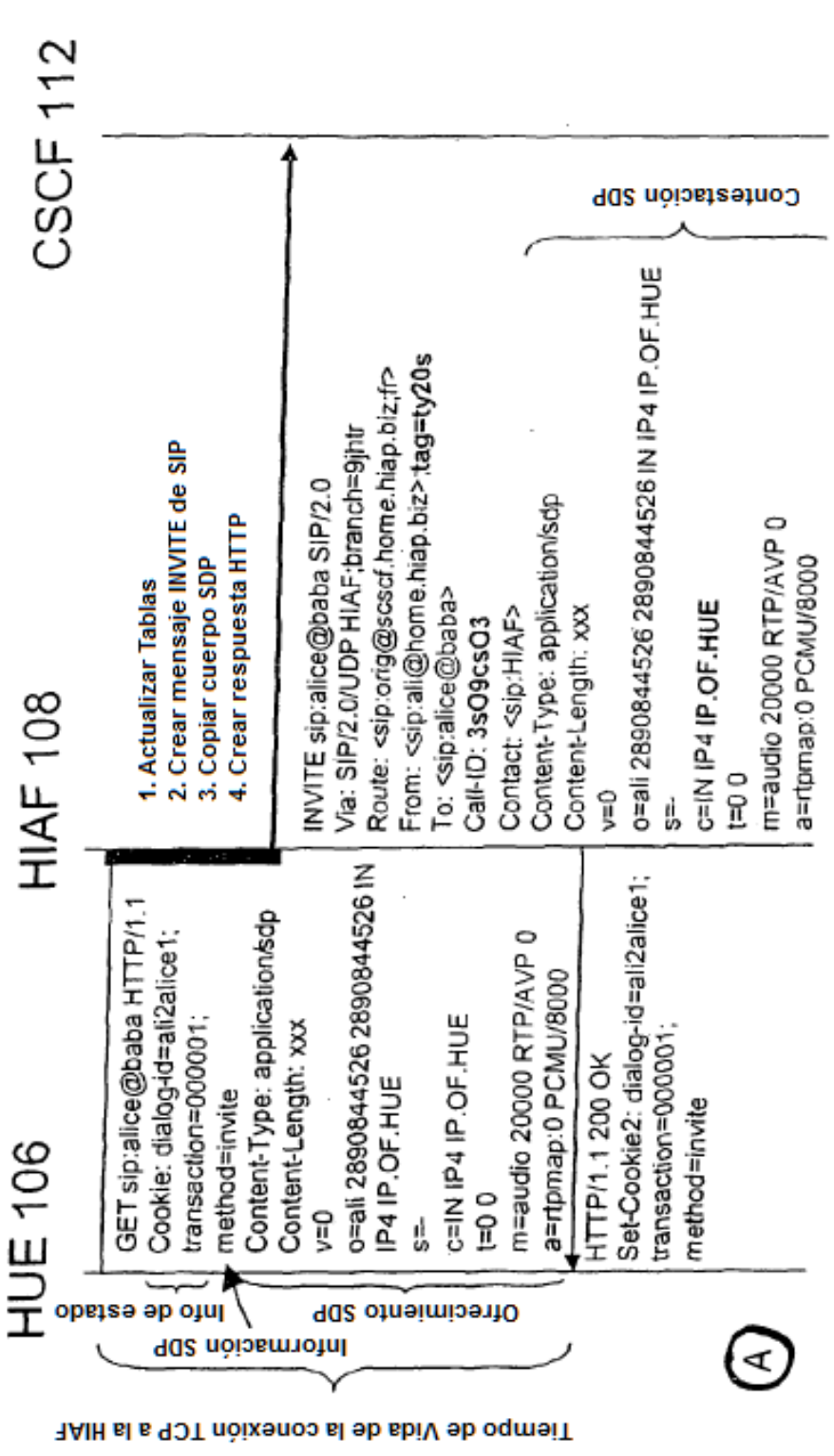
HUE 106
HIAF 108
CSCF 112
1. Actualizar Tablas
2. Crear mensaje INVITE de SIP
3. Copiar cuerpo SDP
4. Crear respuesta HTTP
GET sip:alice@baba HTTP/1.1
Cookie: dialog-id=ali2alice1;
transaction=000001;
method=invite
Content-Type: application/sdp
Content-Length: xxx
v=0
o=ali 2890844526 2890844526 IN
IP4 IP.OF.HUE
s=-
c=IN IP4 IP.OF.HUE
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
INVITE sip:alice@baba SIP/2.0
Via: SIP/2.0/UDP HIAF;branch=9jhtr
Route: <sip:orig@scscf.home.hiap.biz;fr>
From: <sip:ali@home.hiap.biz>;tag=ty20s
To: <sip:alice@baba>
Call-ID: 3sO9csO3
Contact: <sip:HIAF>
Content-Type: application/sdp
Content-Length: xxx
v=0
o=ali 2890844526 2890844526 IN IP4 IP.OF.HUE
s=-
c=IN IP4 IP.OF.HUE
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
HTTP/1.1 200 OK
Set-Cookie2: dialog-id=ali2alice1;
transaction=000001;
method=invite
Contestación SDP
Información SDP
Info de estado
Ofrecimiento SDP
Tiempo de Vida de la conexión TCP a la HIAF
A

Fig. 9A

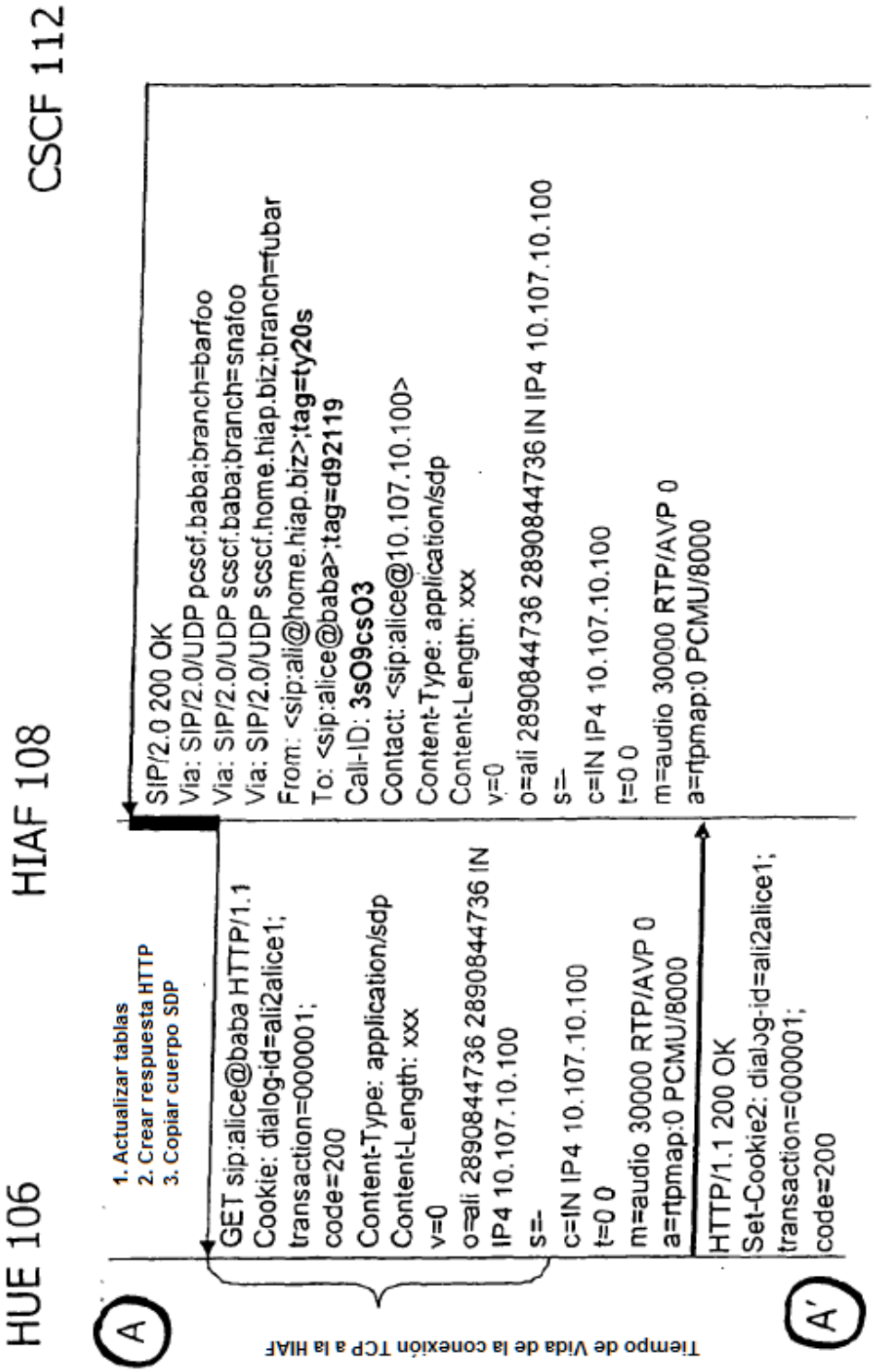
HUE 106
HIAF 108
CSCF 112
A
A'
1. Actualizar tablas
2. Crear respuesta HTTP
3. Copiar cuerpo SDP
GET sip:alice@baba HTTP/1.1
Cookie: dialog-id=ali2alice1;
transaction=000001;
code=200
Content-Type: application/sdp
Content-Length: xxx
v=0
o=ali 2890844736 2890844736 IN
IP4 10.107.10.100
s=-
c=IN IP4 10.107.10.100
t=0 0
m=audio 30000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf.baba;branch=barfoo
Via: SIP/2.0/UDP scscf.baba;branch=snafoo
Via: SIP/2.0/UDP scscf.home.hiap.biz;branch=fubar
From: <sip:ali@home.hiap.biz>;tag=ty20s
To: <sip:alice@baba>;tag=d92119
Call-ID: 3sO9csO3
Contact: <sip:alice@10.107.10.100>
Content-Type: application/sdp
Content-Length: xxx
v=0
o=ali 2890844736 2890844736 IN IP4 10.107.10.100
s=-
c=IN IP4 10.107.10.100
t=0 0
m=audio 30000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
HTTP/1.1 200 OK
Set-Cookie2: dialog-id=ali2alice1;
transaction=000001;
code=200
Tiempo de Vida de la conexión TCP a la HIAF

Fig. 9B

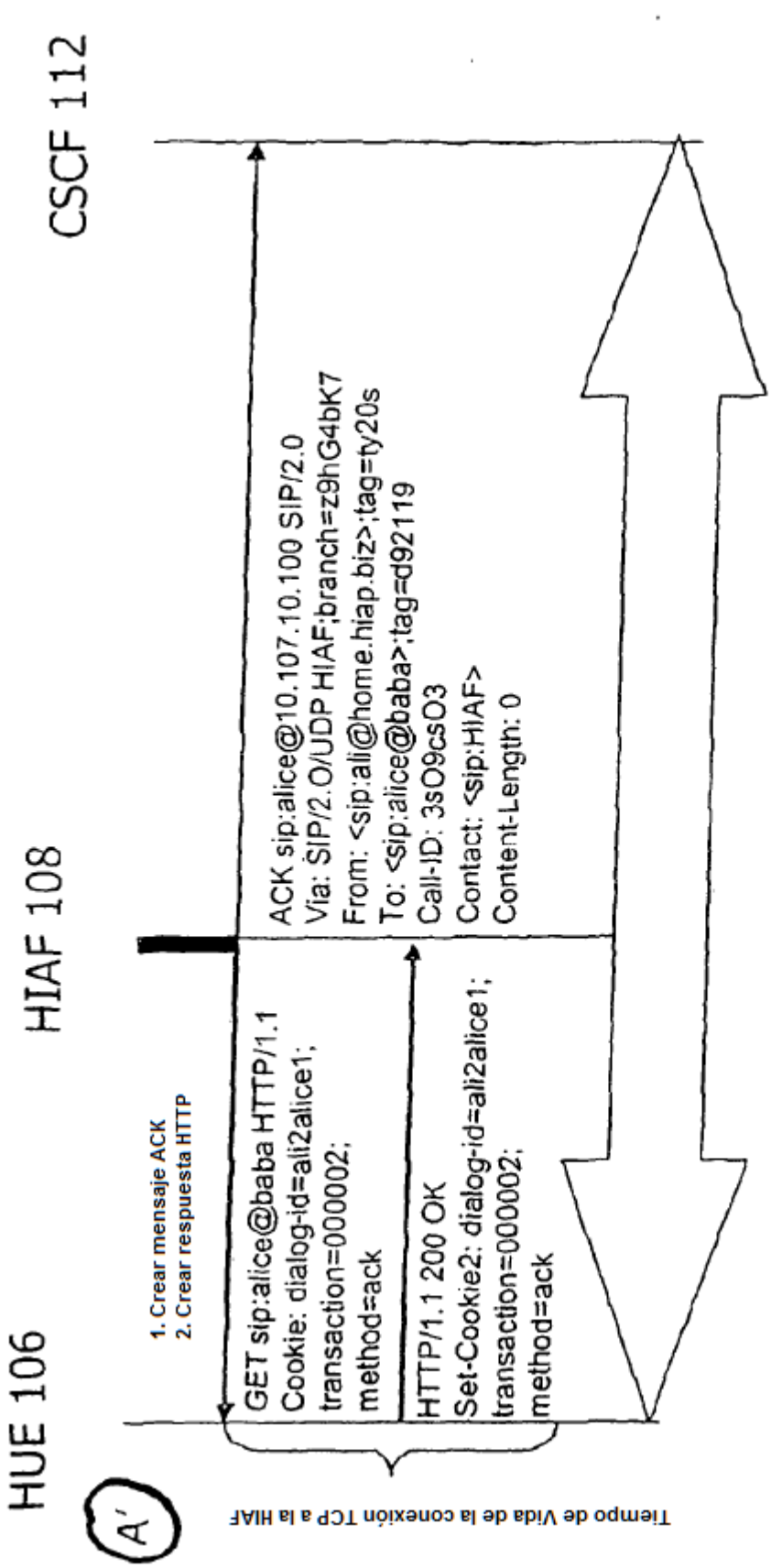
HUE 106
HIAF 108
CSCF 112
A'
1. Crear mensaje ACK
2. Crear respuesta HTTP
GET sip:alice@baba HTTP/1.1
Cookie: dialog-id=ali2alice1;
transaction=000002;
method=ack
HTTP/1.1 200 OK
Set-Cookie2: dialog-id=ali2alice1;
transaction=000002;
method=ack
ACK sip:alice@10.107.10.100 SIP/2.0
Via: SIP/2.O/UDP HIAF;branch=z9hG4bK7
From: <sip:ali@home.hiap.biz>;tag=ty20s
To: <sip:alice@baba>;tag=d92119
Call-ID: 3sO9csO3
Contact: <sip:HIAF>
Content-Length: 0
Tiempo de Vida de la conexión TCP a la HIAF

Fig. 9C

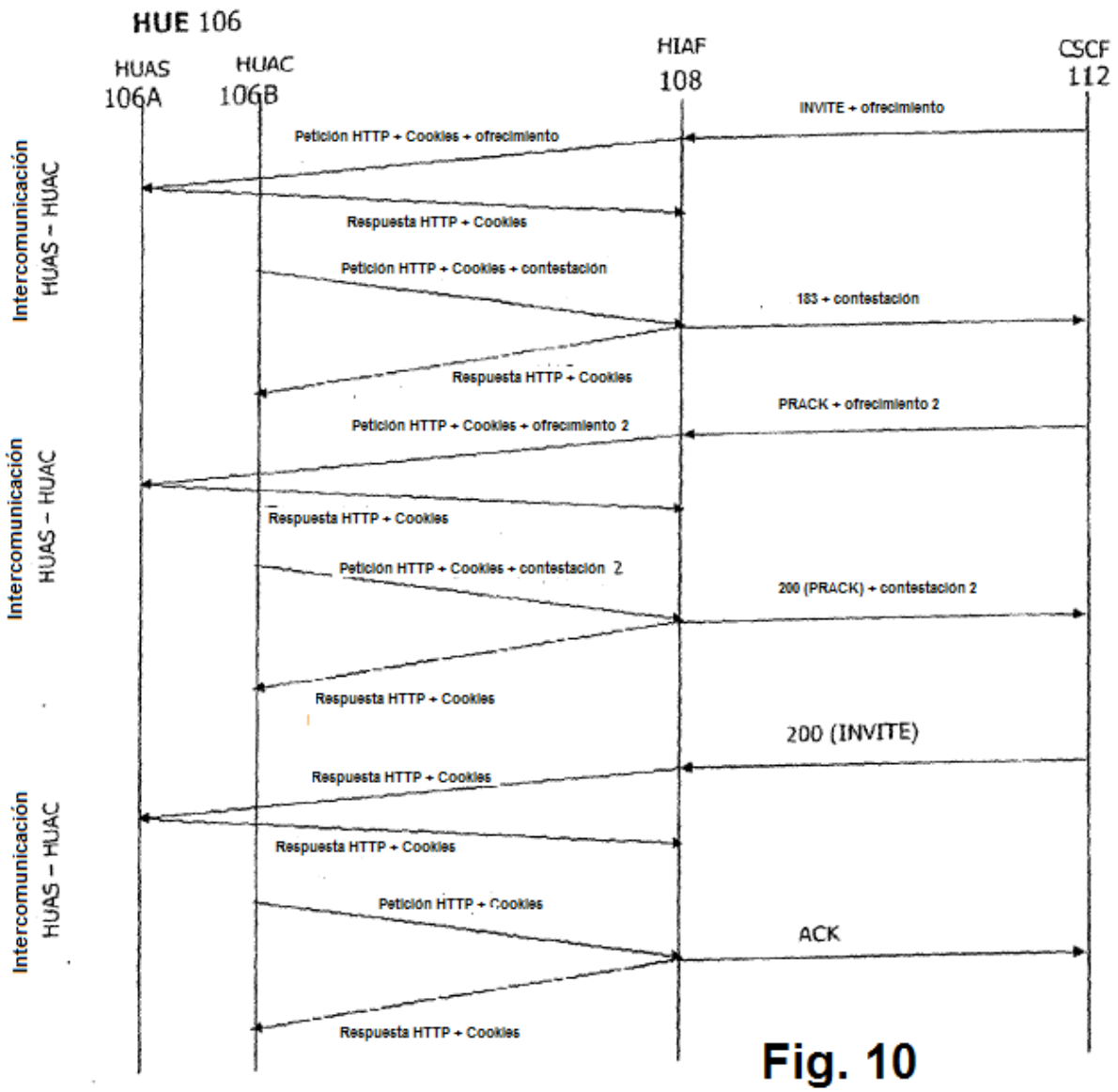
HUE 106
HUAS 106A
HUAC 106B
HIAF 108
CSCF 112
INVITE + ofrecimiento
Petición HTTP + Cookies + ofrecimiento
Respuesta HTTP + Cookies
Petición HTTP + Cookies + contestación
183 + contestación
Respuesta HTTP + Cookies
PRACK + ofrecimiento 2
Petición HTTP + Cookies + ofrecimiento 2
Respuesta HTTP + Cookies
Petición HTTP + Cookies + contestación 2
200 (PRACK) + contestación 2
Respuesta HTTP + Cookies
200 (INVITE)
Respuesta HTTP + Cookies
Respuesta HTTP + Cookies
Petición HTTP + Cookies
ACK
Respuesta HTTP + Cookies
Intercomunicación HUAS – HUAC
Intercomunicación HUAS – HUAC
Intercomunicación HUAS – HUAC

Fig. 10

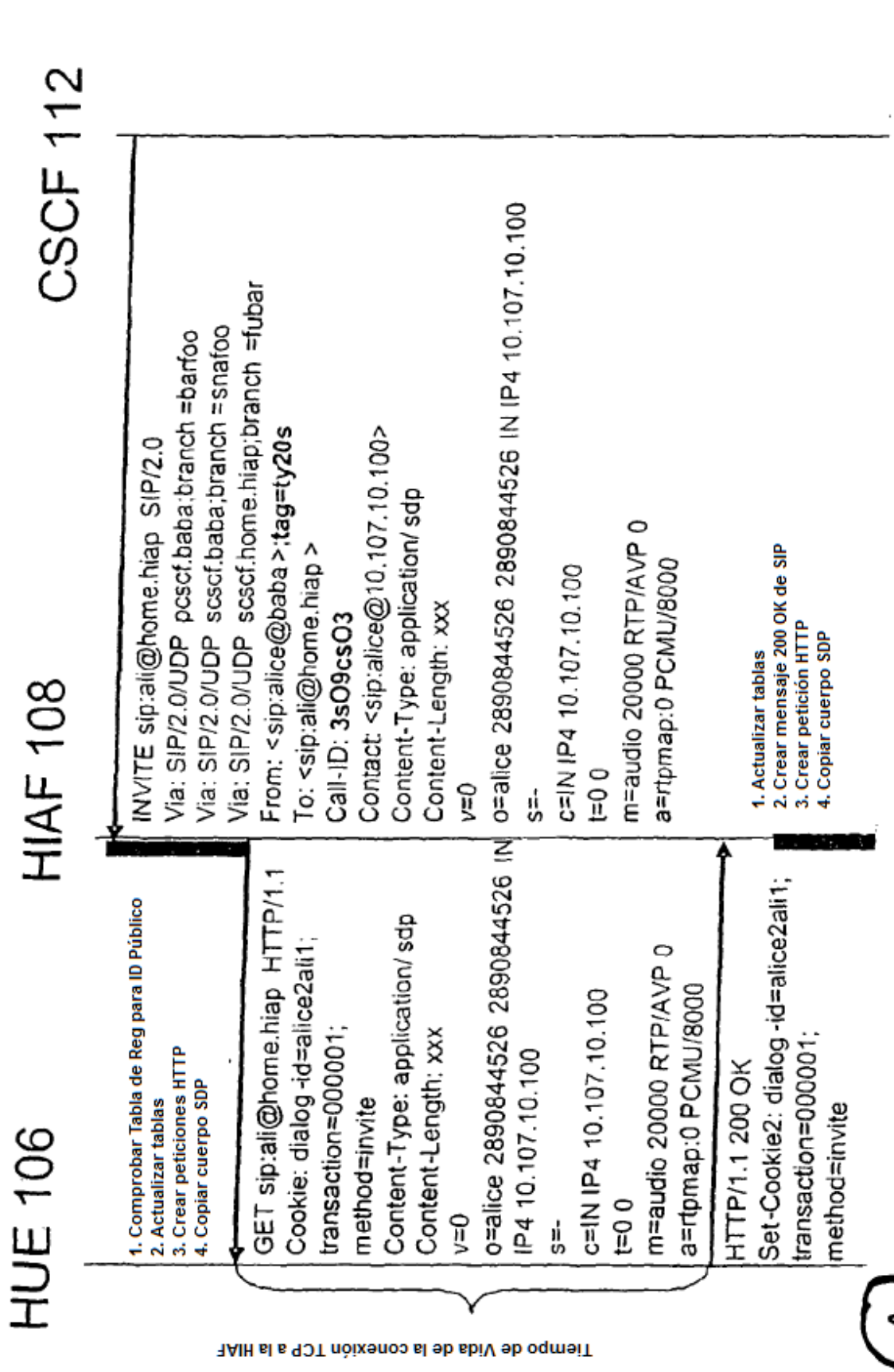
HUE 106
HIAF 108
CSCF 112
1. Comprobar Tabla de Reg para ID Público
2. Actualizar tablas
3. Crear peticiones HTTP
4. Copiar cuerpo SDP
GET sip:ali@home.hiap HTTP/1.1
Cookie: dialog -id=alice2ali1;
transaction=000001;
method=invite
Content-Type: application/ sdp
Content-Length: xxx
v=0
o=alice 2890844526 2890844526 IN
IP4 10.107.10.100
s=-
c=IN IP4 10.107.10.100
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
INVITE sip:ali@home.hiap SIP/2.0
Via: SIP/2.0/UDP pcscf.baba;branch =barfoo
Via: SIP/2.0/UDP scscf.baba;branch =snafoo
Via: SIP/2.0/UDP scscf.home.hiap;branch =fubar
From: <sip:alice@baba >;tag=ty20s
To: <sip:ali@home.hiap >
Call-ID: 3sO9csO3
Contact: <sip:alice@10.107.10.100>
Content-Type: application/ sdp
Content-Length: xxx
v=0
o=alice 2890844526 2890844526 IN IP4 10.107.10.100
s=-
c=IN IP4 10.107.10.100
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
1. Actualizar tablas
2. Crear mensaje 200 OK de SIP
3. Crear petición HTTP
4. Copiar cuerpo SDP
HTTP/1.1 200 OK
Set-Cookie2: dialog -id=alice2ali1;
transaction=000001;
method=invite
Tiempo de Vida de la conexión TCP a la HIAF
A

Fig. 11A

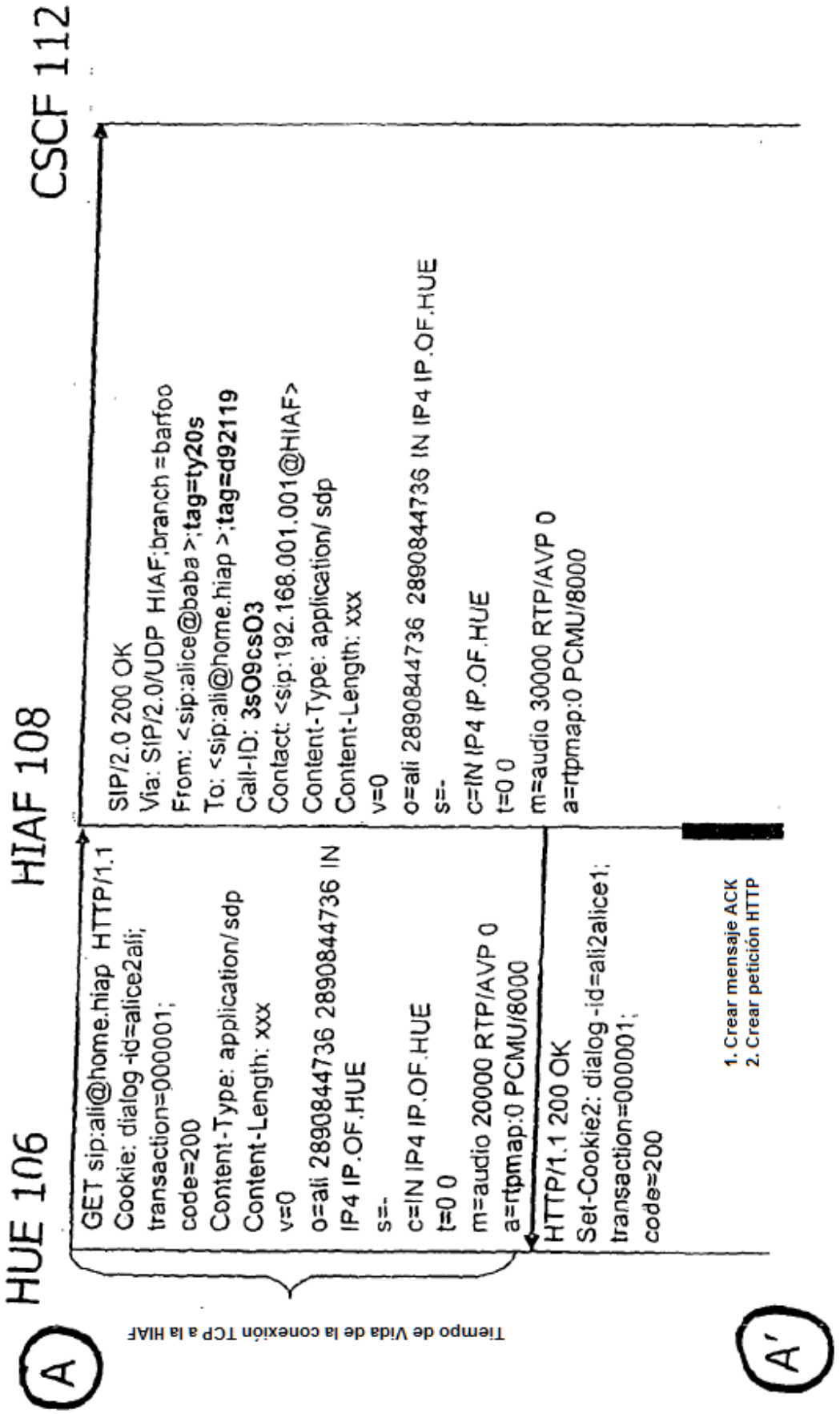
HUE 106
HIAF 108
CSCF 112
A
A'
GET sip:ali@home.hiap HTTP/1.1
Cookie: dialog -id=alice2ali;
transaction=000001;
code=200
Content-Type: application/ sdp
Content-Length: xxx
v=0
o=ali 2890844736 2890844736 IN
IP4 IP.OF.HUE
s=-
c=IN IP4 IP.OF.HUE
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
SIP/2.0 200 OK
Via: SIP/2.0/UDP HIAF;branch=barfoo
From: <sip:alice@baba >;tag=ty20s
To: <sip:ali@home.hiap >;tag=d92119
Call-ID: 3sO9csO3
Contact: <sip:192.168.001.001@HIAF>
Content-Type: application/ sdp
Content-Length: xxx
v=0
o=ali 2890844736 2890844736 IN IP4 IP.OF.HUE
s=-
c=IN IP4 IP.OF.HUE
t=0 0
m=audio 30000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
HTTP/1.1 200 OK
Set-Cookie2: dialog -id=ali2alice1;
transaction=000001;
code=200
1. Crear mensaje ACK
2. Crear petición HTTP
Tiempo de Vida de la conexión TCP a la HIAF

Fig. 11B

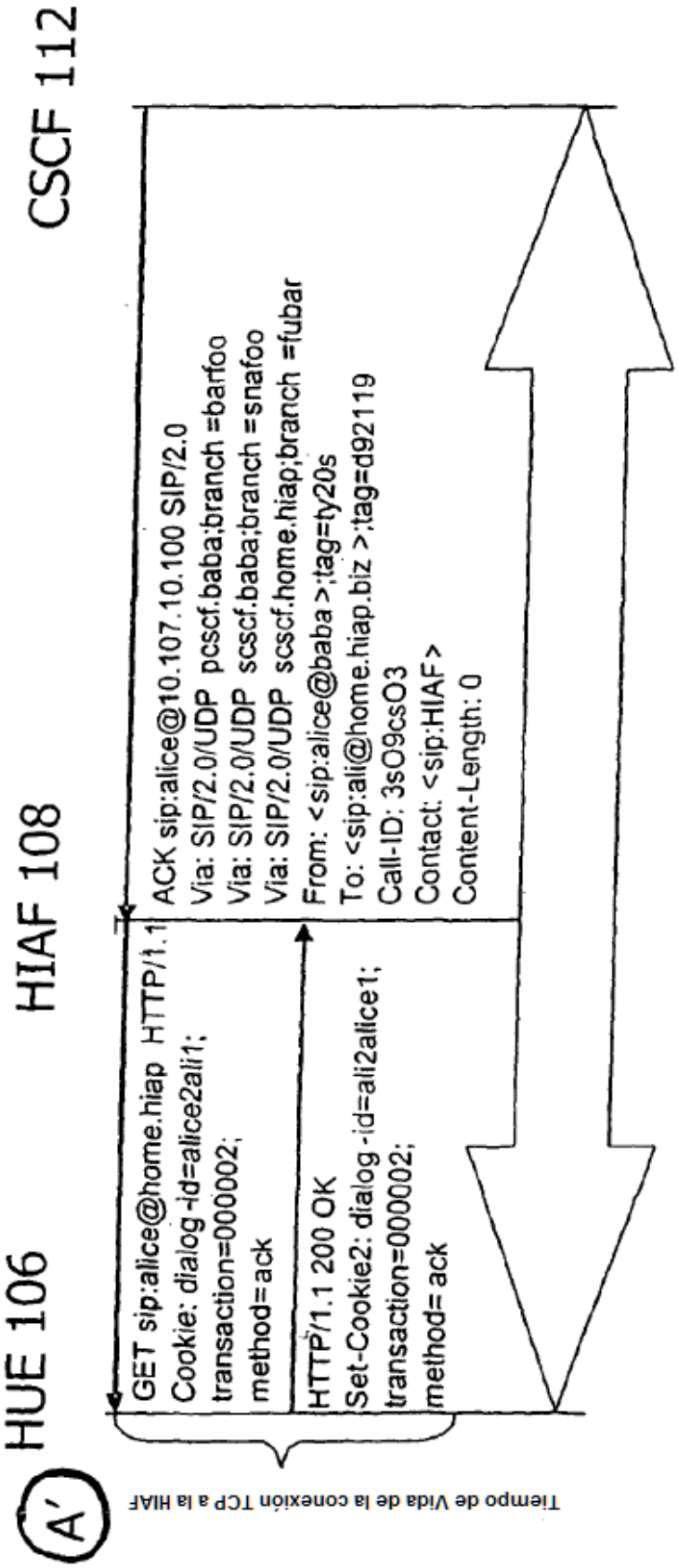
A'
HUE 106
HIAF 108
CSCF 112
GET sip:alice@home.hiap HTTP/1.1
Cookie: dialog -id=alice2ali1;
transaction=000002;
method= ack
HTTP/1.1 200 OK
Set-Cookie2: dialog -id=ali2alice1;
transaction=000002;
method= ack
ACK sip:alice@10.107.10.100 SIP/2.0
Via: SIP/2.0/UDP pcscf.baba;branch =barfoo
Via: SIP/2.0/UDP scscf.baba;branch =snafoo
Via: SIP/2.0/UDP scscf.home.hiap;branch =fubar
From: <sip:alice@baba >;tag=ty20s
To: <sip:ali@home.hiap.biz >;tag=d92119
Call-ID: 3sO9csO3
Contact: <sip:HIAF >
Content-Length: 0
Tiempo de Vida de la conexión TCP a la HIAF

Fig. 11C

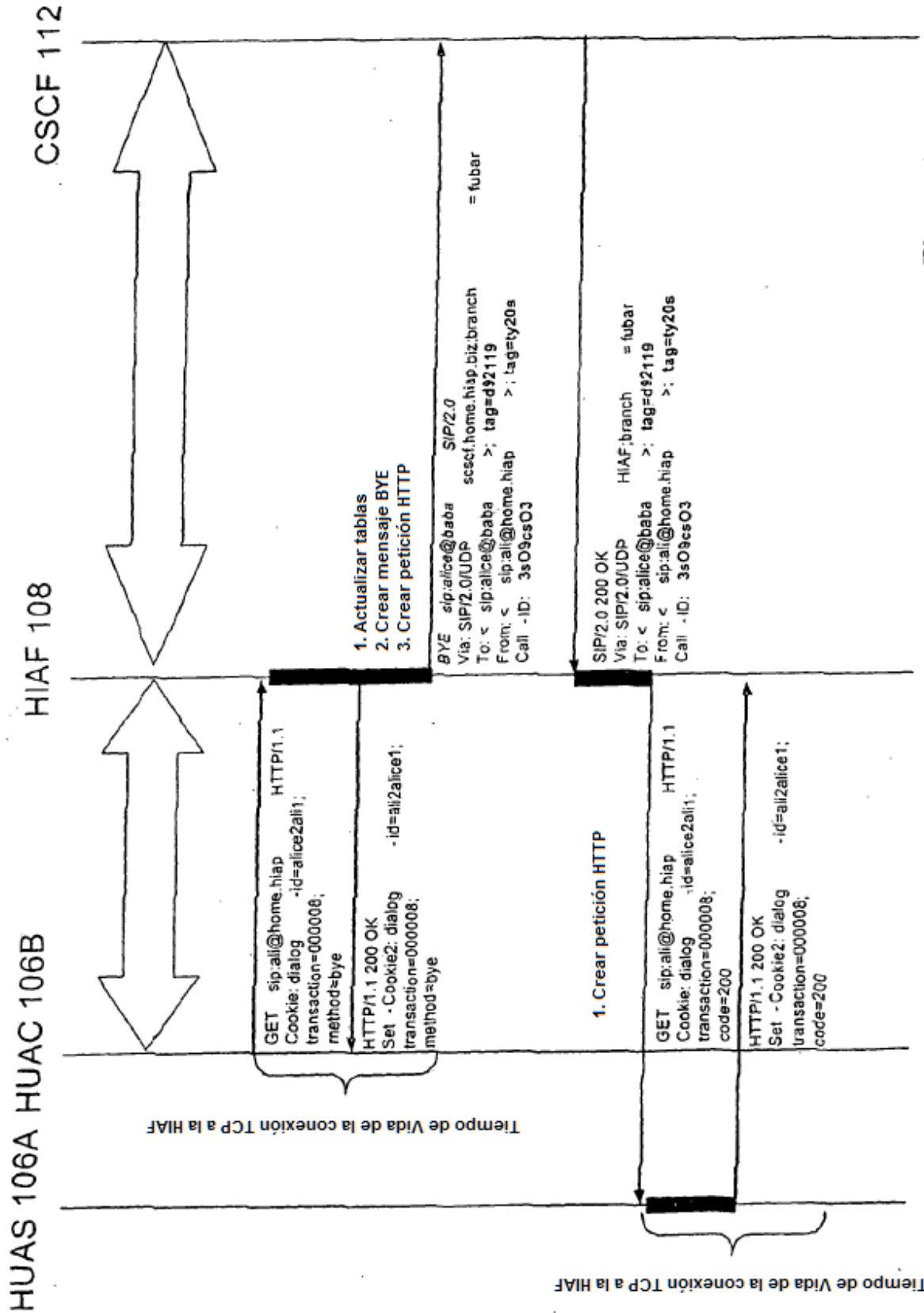
HUAS 106A HUAC 106B
HIAF 108
CSCF 112
GET sip:ali@home.hiap HTTP/1.1
Cookie: dialog -id=alice2ali1;
transaction=000008;
method=bye
HTTP/1.1 200 OK
Set - Cookie2: dialog -id=ali2alice1;
transaction=000008;
method=bye
Tiempo de Vida de la conexión TCP a la HIAF
1. Actualizar tablas
2. Crear mensaje BYE
3. Crear petición HTTP
BYE sip:alice@baba SIP/2.0
Via: SIP/2.0/UDP scscf.home.hiap;biz;branch = fubar
To: < sip:alice@baba >; tag=d92119
From: < sip:ali@home.hiap >; tag=ty20s
Call - ID: 3sO9csO3
SIP/2.0 200 OK
Via: SIP/2.0/UDP HIAF;branch = fubar
To: < sip:alice@baba >; tag=d92119
From: < sip:ali@home.hiap >; tag=ty20s
Call - ID: 3sO9csO3
1. Crear petición HTTP
GET sip:ali@home.hiap HTTP/1.1
Cookie: dialog ;id=alice2ali1;
transaction=000008;
code=200
HTTP/1.1 200 OK
Set - Cookie2: dialog -id=ali2alice1;
transaction=000008;
code=200
Tiempo de Vida de la conexión TCP a la HIAF

Fig. 12

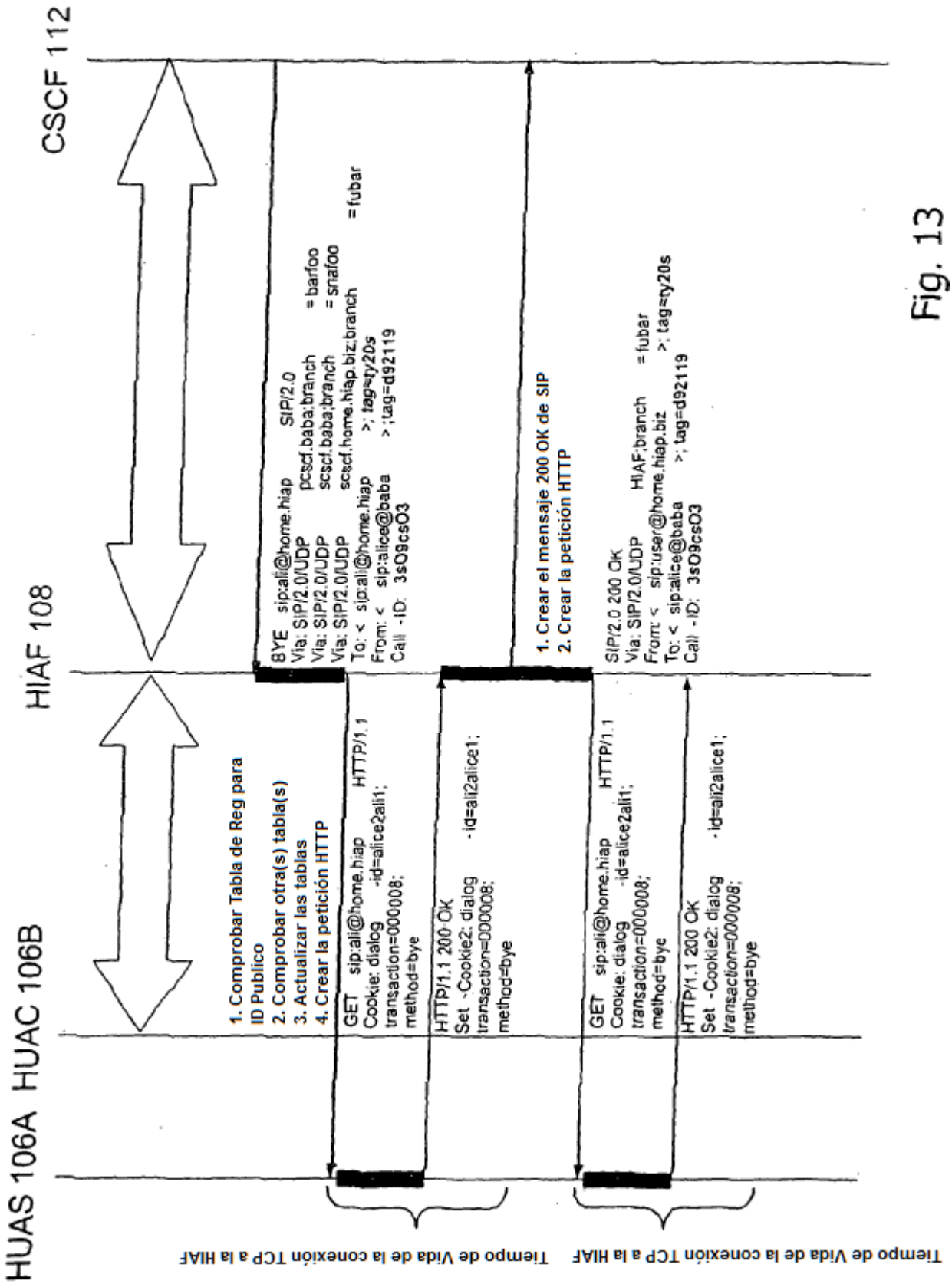
HUAS 106A
HUAC 106B
HIAF 108
CSCF 112
1. Comprobar Tabla de Reg para ID Publico
2. Comprobar otra(s) tabla(s)
3. Actualizar las tablas
4. Crear la petición HTTP
BYE sip:ali@home.hiap SIP/2.0
Via: SIP/2.0/UDP pcscf.baba;branch = barfoo
Via: SIP/2.0/UDP scscf.baba;branch = snafoo
Via: SIP/2.0/UDP scscf.home.hiap.biz;branch = fubar
To: < sip:ali@home.hiap >; tag=ty20s
From: < sip:alice@baba >;tag=d92119
Call -ID: 3sO9csO3
GET sip:ali@home.hiap HTTP/1.1
Cookie: dialog -id=alice2ali1;
transaction=000008;
method=bye
HTTP/1.1 200 OK
Set -Cookie2: dialog -id=ali2alice1;
transaction=000008;
method=bye
1. Crear el mensaje 200 OK de SIP
2. Crear la petición HTTP
SIP/2.0 200 OK
Via: SIP/2.0/UDP HIAF;branch = fubar
From: < sip:user@home.hiap.biz >; tag=ty20s
To: < sip:alice@baba >; tag=d92119
Call -ID: 3sO9csO3
GET sip:ali@home.hiap HTTP/1.1
Cookie: dialog -id=alice2ali1;
transaction=000008;
method=bye
HTTP/1.1 200 OK
Set -Cookie2: dialog -id=ali2alice1;
transaction=000008;
method=bye
Tiempo de Vida de la conexión TCP a la HIAF
Tiempo de Vida de la conexión TCP a la HIAF

Fig. 13

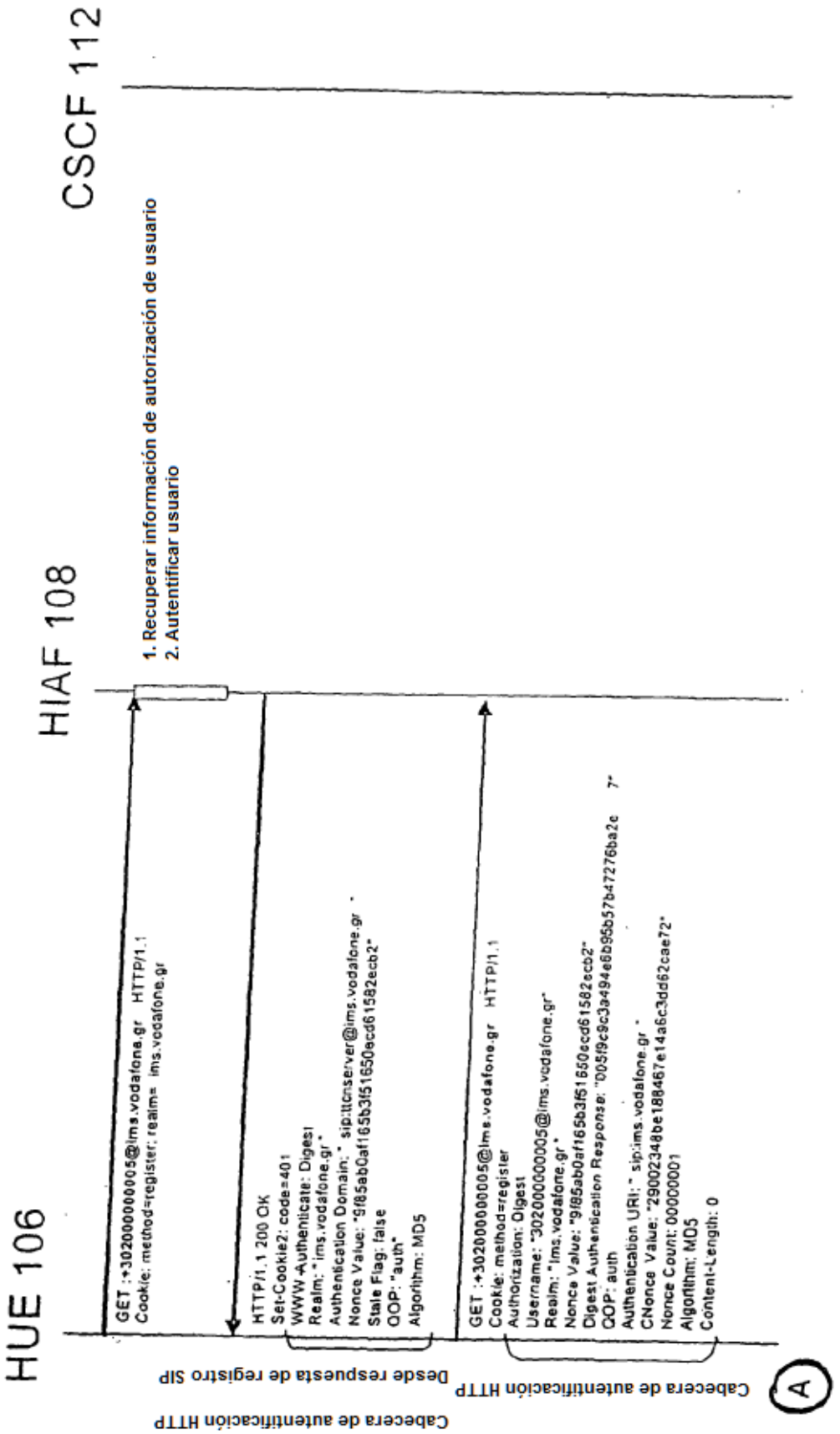
HUE 106
HIAF 108
CSCF 112
1. Recuperar información de autorización de usuario
2. Autentificar usuario
GET :+302000000005@ims.vodafone.gr HTTP/1.1
Cookie: method=register; realm= ims.vodafone.gr
HTTP/1.1 200 OK
Set-Cookie2: code=401
WWW-Authenticate: Digest
Realm: " ims.vodafone.gr "
Authentication Domain: " sip:ttcnserver@ims.vodafone.gr "
Nonce Value: "9f85ab0af165b3f51650ecd61582ecb2"
Stale Flag: false
QOP: "auth"
Algorithm: MD5
GET :+302000000005@ims.vodafone.gr HTTP/1.1
Cookie: method=register
Authorization: Digest
Username: "302000000005@ims.vodafone.gr"
Realm: "ims.vodafone.gr"
Nonce Value: "9f85ab0af165b3f51650ecd61582ecb2"
Digest Authentication Response: "005f9c9c3a494e6b95b57b47276ba2e 7"
QOP: auth
Authentication URI: " sip:ims.vodafone.gr "
CNonce Value: "290023488e188467e14a6c3dd62cae72"
Nonce Count: 00000001
Algorithm: MD5
Content-Length: 0
Cabecera de autentificación HTTP
Desde respuesta de registro SIP
Cabecera de autentificación HTTP
A

Fig. 14A

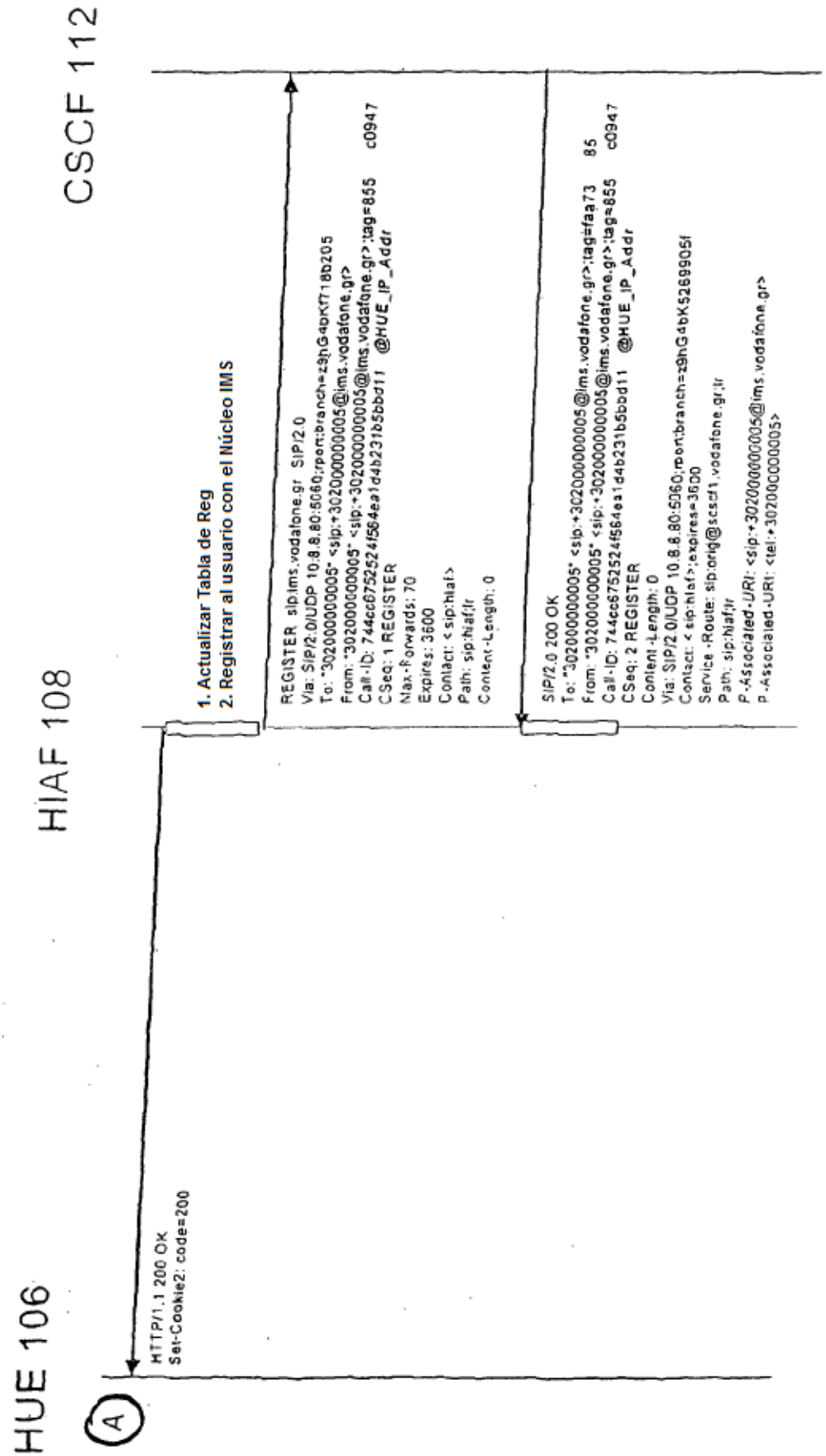
HUE 106
HIAF 108
CSCF 112
A
HTTP/1.1 200 OK
Set-Cookie2: code=200
1. Actualizar Tabla de Reg
2. Registrar al usuario con el Núcleo IMS
REGISTER sip:ims.vodafone.gr SIP/2.0
Via: SIP/2.0/UDP 10.8.8.80:5060;rport;branch=z9hG4bKff18b205
To: "302000000005" <sip:+302000000005@ims.vodafone.gr>
From: "302000000005" <sip:+302000000005@ims.vodafone.gr>;tag=855 c0947
Call-ID: 744cc67525245f564ea1d4b231b5bbd11 @HUE_IP_Addr
CSeq: 1 REGISTER
Max-Forwards: 70
Expires: 3600
Contact: <sip:hiaf>
Path: sip:hiaf;lr
Content-Length: 0
SIP/2.0 200 OK
To: "302000000005" <sip:+302000000005@ims.vodafone.gr>;tag=faa73 85
From: "302000000005" <sip:+302000000005@ims.vodafone.gr>;tag=855 c0947
Call-ID: 744cc67525245f564ea1d4b231b5bbd11 @HUE_IP_Addr
CSeq: 2 REGISTER
Content-Length: 0
Via: SIP/2.0/UDP 10.8.8.80:5060;rport;branch=z9hG4bK5269905f
Contact: <sip:hiaf>;expires=3600
Service-Route: sip:orig@scscf1.vodafone.gr;lr
Path: sip:hiaf;lr
P-Associated-URI: <sip:+302000000005@ims.vodafone.gr>
P-Associated-URI: <tel:+302000000005>

Fig. 14B

Nombre de Usuario de Autentificación	Dominio Local URI	Contraseña	Esquema de Autentificación
Niko@home1.de	home1.de	XXX	Básico
Jfikouras@home1.de	home1.de	YYY	De Resumen

1500

Fig. 15

Nombre de Usuario de Autentificación	Lista de ID de Usuario Público	Dominio Local (Realm)	Dirección IP	Estado	Tiempo de Vida
niko_pri@home1.de		home1.de	192.168.1.1	REGISTERED	1000
janni_priv@home1.de		home1.de	192.168.1.2	REGISTERED	60000

1600

Fig. 16