(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 374 341**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08851466 .6**
(96) Fecha de presentación: **17.11.2008**
(97) Número de publicación de la solicitud: **2204962**
(97) Fecha de publicación de la solicitud: **07.07.2010**

(54) Título: **MÉTODO, SISTEMA Y DISPOSITIVO PARA PROCESAR INFORMACIÓN DE SOLICITUDES DE ACCESO.**

(30) Prioridad:
16.11.2007 CN 200710188318

(45) Fecha de publicación de la mención BOPI:
15.02.2012

(45) Fecha de la publicación del folleto de la patente:
15.02.2012

(73) Titular/es:
Huawei Technologies Co., Ltd.
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:
YANG, Zhenting

(74) Agente: **Lehmann Novo, Isabel**

DESCRIPCIÓN

Método, sistema y dispositivo para procesar información de solicitudes de acceso.

Campo de la invención

La presente invención está relacionada con el campo de las sesiones del Protocolo de Internet (IP), y en particular, con un método, un sistema y un dispositivo para procesar la información de las solicitudes de acceso en una sesión IP.

Antecedentes de la invención

Debido al éxito de las redes de banda ancha, la gestión y el control sobre los accesos de banda ancha constituyen una parte importante de la gestión y el control de las redes de banda ancha. Una forma extendida de gestionar y controlar los accesos de banda ancha consiste en establecer una sesión para controlar y gestionar un Equipo de Usuario (UE) que solicita acceder, incluidas la autenticación, autorización y contabilización para el UE. En el momento actual, la forma más extendida de gestionar y controlar los accesos de banda ancha consiste en establecer una sesión del protocolo Punto a Punto (PPP) para controlar y gestionar el acceso, proporcionando de esta forma al UE un modo de acceso de banda ancha, y posibilitando el control, la gestión y la contabilización apropiados del acceso. Sin embargo, el modo de acceso basado en las sesiones PPP tiene limitaciones, por ejemplo la falta de un soporte flexible.

La tendencia actual consiste en utilizar el modo de acceso basado en sesiones IP en lugar del modo de acceso basado en sesiones PPP para controlar y gestionar los accesos de banda ancha.

La sesión IP representa una sesión de acceso de la red de banda ancha asociada a una dirección IP. La sesión IP es equivalente a la sesión PPP. La sesión IP se termina generalmente en un dispositivo IP perimetral. En otras palabras, la sesión IP es el establecimiento de la conexión para una sesión entre el UE y el dispositivo IP perimetral. La dirección IP de la sesión IP está diseñada para identificar la parte esencial de los parámetros de la sesión IP. En general, la dirección IP de la sesión IP se asigna dinámicamente mediante un servidor a través del Protocolo de Configuración Dinámica de Host (Equipo) (DHCP). La sesión IP está diseñada para identificar la parte esencial de los parámetros de la sesión IP. En general, la dirección IP de la sesión IP se asigna dinámicamente mediante un servidor a través del Protocolo de Configuración Dinámica de Host (DHCP). La sesión IP está diseñada para gestionar y controlar el acceso del UE en una red de banda ancha, por ejemplo la autenticación, autorización y contabilización. Una sesión IP incluye estos procesos: configuración y establecimiento de la sesión IP, mantenimiento o detección del estado de la sesión IP, y terminación de la sesión IP.

En la actualidad se ofrecen algunas soluciones técnicas para el establecimiento, detección, mantenimiento y terminación de una sesión IP. Como consecuencia de que la sesión IP está diseñada para controlar y gestionar accesos de banda ancha, a lo largo del proceso de control y gestión de cada acceso de banda ancha se genera una gran cantidad de información de solicitudes de acceso, como, por ejemplo, la causa de la desconexión de una sesión IP y la causa de un fallo en el establecimiento de una sesión IP. Esta información de las solicitudes de acceso resulta de gran importancia para diagnosticar la sesión IP, reclamar la atención del UE en la sesión IP, o hacer copias de seguridad de los log (registros) de otros servidores de la red.

El documento D1 (US 6 782 004 B1) describe un sistema de comunicación que utiliza un protocolo de red de sistemas abiertos como, por ejemplo, TCP/IP, para transportar mensajes de señalización de Redes Inteligentes desde una red SS7 a un proveedor de servicios que no se encuentra directamente conectado a la red SS7. El límite de crédito del usuario no está relacionado con la terminación de una sesión IP, de modo que la consulta TCAP (Parte de Aplicación de Capacidades de Transacción) recibida por el SCP (Punto de Control del Servicio) no incluye el límite de crédito del usuario. Es más, en el documento D1 no se mencionan el mensaje BFD (Detección de Reenvío Bidireccional), el campo de Opción ni el campo de Diagnóstico.

El documento D2 (CN 1901459A) describe un método de control del estado on-line (en línea) y un sistema. Después de que el sistema de cargo empiece a contabilizar, un dispositivo de acceso mantiene la conexión con los terminales de usuario, el sistema de cargo envía al dispositivo de acceso un primer mensaje que incluye el volumen de servicio utilizable, y éste actualiza el atributo de la sesión local de acuerdo con dicho primer mensaje para controlar la conexión con el terminal de usuario. En el documento D2 no se mencionan la causa de terminación de la sesión IP, el mensaje BFD, el campo de Opción ni el campo de Diagnóstico.

Por otro lado, el inventor de la presente invención ha descubierto que la técnica anterior no proporciona ningún método para procesar la información de las solicitudes de acceso en una sesión IP, lo que dificulta la operación, la administración y el mantenimiento de los accesos de banda ancha e impide que el UE de la sesión IP u otros servidores de la red reciban a tiempo la información de las solicitudes o puedan tomar las medidas necesarias para gestionar la sesión IP, afectando de este modo negativamente a la percepción del usuario que utiliza el UE e incrementando el coste del mantenimiento de la sesión IP para el operador.

Resumen de la invención

Los modos de realización de la presente invención proporcionan un método para procesar la información de las solicitudes de acceso, y este método permite procesar la información de las solicitudes de acceso en una sesión IP.

Los modos de realización de la presente invención proporcionan un sistema para procesar la información de las solicitudes de acceso, y este sistema permite procesar la información de las solicitudes de acceso en una sesión IP.

La solución técnica amparada por la presente invención se realiza de la siguiente forma:

Un método para procesar la información de las solicitudes de acceso de acuerdo con la reivindicación 1.

El envío a un receptor del mensaje BFD que incluye la información de la solicitud de acceso, de forma que el receptor pueda ejecutar las operaciones correspondientes de acuerdo con la información de las solicitudes de acceso.

Un sistema de comunicación de acuerdo con la reivindicación 3.

En la solución técnica amparada por la presente invención, la información de las solicitudes de acceso recibida se incluye en un mensaje de señalización de control de la sesión IP que se envía al receptor. De esta forma, el receptor puede ejecutar las operaciones correspondientes de acuerdo con la información de las solicitudes de acceso. En consecuencia, el método, el sistema y el dispositivo proporcionados en la presente solicitud permiten el proceso de la información de las solicitudes de acceso en una sesión IP, lo que facilita la operación, la administración y el mantenimiento de los accesos de banda ancha mediante accesos basados en una sesión IP, y permite al UE de la sesión IP o al servidor de políticas de la red recibir a tiempo la información de las solicitudes.

Breve descripción de los dibujos

La FIG. 1 muestra una arquitectura de un sistema para el proceso de la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención;

La FIG. 2 es un diagrama de flujo de un método para procesar la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención;

La FIG. 3 es un diagrama de flujo del proceso de la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención;

La FIG. 4 muestra un formato de un mensaje del protocolo de Detección de Reenvío Bidireccional (BFD) para el proceso de la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención;

La FIG. 5 muestra un formato de un mensaje DHCP para el proceso de la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención;

La FIG. 6 muestra cómo notifica un dispositivo IP perimetral a un UE la causa de fallo en la identificación inicial (login) del usuario o la causa de fallo en el establecimiento de una sesión IP en un modo de realización de la presente invención;

La FIG. 7 muestra cómo notifica un dispositivo IP perimetral a un UE la información de identificación satisfactoria del usuario o de establecimiento satisfactorio de la sesión IP en un modo de realización de la presente invención;

La FIG. 8 muestra cómo notifica un dispositivo IP perimetral a un UE, o a un servidor de políticas durante el proceso de una sesión IP, la causa de terminación de una sesión IP en un modo de realización de la presente invención;

La FIG. 9 muestra cómo notifica un dispositivo IP perimetral a un UE la información de las solicitudes de acceso en un proceso de mantenimiento de una sesión IP en un modo de realización de la presente invención;

La FIG. 10 muestra cómo notifica un dispositivo IP perimetral a un UE y a un servidor de políticas la causa de terminación de una sesión IP, o la causa de desconexión (logout) de un usuario en un modo de realización de la presente invención;

La FIG. 11 muestra un sistema para el proceso de la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención;

La FIG. 12 muestra un dispositivo para el proceso de la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención; y

La FIG. 13 muestra otro dispositivo para el proceso de la información de las solicitudes de acceso en un modo de realización de la presente invención.

Descripción detallada de los modos de realización

Con objeto de clarificar la solución técnica, los objetivos y los méritos de la presente invención, se describen a continuación de forma detallada los modos de realización de la presente invención, mediante referencia a los dibujos que la acompañan.

Una sesión IP es independiente de las tecnologías de líneas de acceso, y se establece entre un dispositivo IP perimetral y un UE. La sesión IP se caracteriza por una gestión y un control del acceso orientados al usuario. En el proceso de negociación para el establecimiento, mantenimiento y terminación de una sesión IP, el dispositivo IP perimetral y el servidor de políticas generan información de solicitudes de acceso para facilitar su gestión, control y utilización. En los modos de realización de la presente invención, para procesar la información de las solicitudes de acceso en una sesión IP, el dispositivo IP perimetral controla el estado de la sesión IP durante el proceso de la misma, obtiene la información de las solicitudes de acceso a partir de un directorio creado localmente o desde otro servidor de la red de banda ancha, incluye la información de las solicitudes de acceso en un mensaje de señalización de control de la sesión IP, y envía el mensaje de señalización de control de la sesión IP al receptor, como, por ejemplo, un UE y/o un servidor de políticas de la red. El receptor lleva a cabo la gestión correspondiente de acuerdo con la información de las solicitudes de acceso incluida en el mensaje de señalización de control de la sesión IP.

En los modos de realización de la presente invención, la información de las solicitudes de acceso incluye, pero no se limita a: información de la solicitud acerca del éxito en el establecimiento de la sesión IP, la causa de fallo en el establecimiento de una sesión IP, la causa de terminación de una sesión IP o información de carácter comercial o de contabilización del usuario. La información de las solicitudes acerca del éxito en el establecimiento de la sesión IP puede ser información acerca del éxito de la identificación inicial del usuario. La causa de fallo en el establecimiento de una sesión IP puede ser una causa de fallo en la identificación inicial del usuario. La causa de terminación de una sesión IP puede ser una causa de desconexión del usuario. La información de carácter comercial puede ser una dirección IP de un portal publicitario en una red de banda ancha, o información de carácter comercial consistente en gráficos y texto. La información contable del usuario puede ser la duración restante o el importe restante disponibles en la cuenta de suscripción del usuario.

La FIG. 1 muestra una arquitectura de un sistema para el proceso de la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención. El sistema incluye un UE 100A y un dispositivo IP perimetral 100B, y puede incluir, además, un servidor 100C de políticas.

El UE 100A y el dispositivo IP perimetral 100B son las dos extremos de la sesión IP. Es decir, el UE 100A es la parte cliente de una sesión IP y el dispositivo IP perimetral 100B es la parte de red de una sesión IP. El UE 100A está conectado a través de la red de acceso al dispositivo IP perimetral 100B, y el dispositivo IP perimetral 100B puede estar conectado, a su vez, a un servidor 100C de políticas.

El UE 100A incluye: una Unidad 101A de Solicitud de Información del Cliente (CIPU), una Unidad 102A de Proceso de Señalización de la Sesión del Cliente (CSSPU), y una Unidad 103A de Adopción de Información del Cliente (CIAU). En los modos de realización de la presente invención, los UE incluyen: un Ordenador Personal (PC), una Pasarela Residencial (RG), y un terminal portátil inalámbrico, como, por ejemplo, un teléfono móvil o un Asistente Personal Digital (PDA). La CSSPU 102A está configurada para recibir un mensaje de señalización de control de la sesión IP que incluye información de la solicitud de acceso y para enviar el mensaje de señalización de control de la sesión IP a la CIAU 103A, donde el mensaje de señalización de control de la sesión IP puede ser un mensaje de un protocolo, como por ejemplo un mensaje DHCP, o un mensaje del protocolo de Detección de Reenvío Bidireccional (BFD). La CIAU 103A está configurada para: analizar el mensaje de señalización de control de la sesión IP recibido de la CSSPU 102A, obtener de él la información de la solicitud de acceso y, a continuación, ejecutar las operaciones necesarias de acuerdo con la información de la solicitud de acceso, por ejemplo, reiniciar la sesión IP de acuerdo con la información de la solicitud, tal como, una causa de la desconexión de la sesión, o enviar a la CIPU 101A la información de la solicitud como, por ejemplo, una causa de desconexión de la sesión, o guardar una copia de la información de la solicitud como, por ejemplo, una causa de desconexión de la sesión. La CIPU 101A está configurada para ejecutar las operaciones necesarias de acuerdo con la información de las solicitudes de acceso recibida de la CIAU, por ejemplo, mostrar al usuario la causa de la desconexión de la sesión o la información de carácter comercial a través de la interfaz hombre-máquina (o pantalla).

El dispositivo IP perimetral 100B incluye: una AICU 101B, una GSSPU 102B, una GSSMU 103B y una IMU 104B. En los modos de realización de la presente invención, algunos ejemplos de dispositivos IP perimetrales son: Servidores de Acceso a la Red (NAS) tales como un Servidor de Acceso Remoto de Banda Ancha (BRAS) o una Pasarela de Red de Banda Ancha (BNG), un router (enrutador) de servicios, y una pasarela de acceso. La GSSMU 103B está configurada para gestionar el estado de la sesión IP y obtener la información de las solicitudes de acceso en función

de la gestión del estado de la sesión IP. La gestión del estado de la sesión IP incluye: la gestión del establecimiento de la sesión IP, la gestión del mantenimiento de la sesión IP y la gestión de la terminación de la sesión IP. Por ejemplo, la GSSMU 103B envía a la AICU 101B la causa de terminación de la sesión IP, o la GSSMU 103B envía a la AICU 101B información del fallo en el establecimiento de la sesión IP. La AICU 101B está configurada para obtener la información de las solicitudes de acceso, incluyendo: la obtención de la información de las solicitudes de acceso a través de la GSSMU 103B o a través de la interfaz de control para la gestión de red. Tras haber obtenido la información de las solicitudes de acceso, la AICU 101B le indica a la IMU 104B que determine la asociación de la información de las solicitudes de acceso. La IMU 104B está configurada para: llevar a cabo la asociación de la información de las solicitudes de acceso y enviar a la GSSPU 102B la información de las solicitudes de acceso asociada. Por ejemplo, la IMU 104B convierte la causa de terminación de la sesión IP en un código de causa de terminación y, a continuación, le indica a la GSSPU 102B que incluya el código de causa de terminación en el mensaje de señalización de control de la sesión IP especificado. La GSSPU 102B está configurada para: incluir la información de la solicitud de acceso en el mensaje de señalización de control de la sesión IP y, a continuación, enviar el mensaje de señalización de control de la sesión IP que incluye la información de la solicitud de acceso al UE y/o al servidor de políticas.

El servidor 100C de políticas incluye: una Unidad 101C de Solicitud de Información del Servidor (SIPU), una Unidad 102C de Proceso de Señalización de la Sesión del Servidor (SSSPU), y una Unidad 103C de Adopción de Información del Servidor (SIAU). En los modos de realización de la presente invención, un servidor de políticas puede ser un servidor de Autenticación, Autorización y Contabilización (AAA) o un servidor DHCP. La SSSPU 102C está configurada para recibir el mensaje de señalización de control de la sesión IP que incluye la información de las solicitudes de acceso, y enviar el mensaje de señalización de control de la sesión IP a la SIAU 103C, donde el mensaje de señalización de control de la sesión IP puede ser un mensaje del protocolo de Servicios de Autenticación Remota de Conexiones de Usuarios (RADIUS). La SIAU 103C está configurada para: analizar el mensaje de señalización de control de la sesión IP recibido a partir de la SSSPU 102C, obtener de él la información de la solicitud de acceso y, a continuación, ejecutar las operaciones necesarias de acuerdo con la información de la solicitud de acceso, por ejemplo, detener la contabilización de la sesión IP de acuerdo con la información de la solicitud, como, por ejemplo, la causa de desconexión de una sesión, o enviar a la SIPU la información de la solicitud, como, por ejemplo, la causa de desconexión de una sesión, o guardar una copia de la información de la solicitud, como, por ejemplo, la causa de desconexión de una sesión; y solucionar los problemas de la sesión en función de la información de la solicitud, como, por ejemplo, la causa de desconexión de una sesión. La SIPU 101C está configurada para ejecutar las operaciones necesarias de acuerdo con la información de la solicitud de acceso recibida de la SIAU, por ejemplo, mostrar al administrador de la red la causa de la desconexión de la sesión a través de una interfaz hombre-máquina (o pantalla).

El método objeto de la presente invención se describe en detalle más abajo en relación con las unidades de los dispositivos que se ilustran en la FIG. 1.

La FIG. 2 es un diagrama de flujo de un método para procesar la información de las solicitudes de acceso de una sesión IP en un modo de realización de la presente invención. Las entidades de red involucradas incluyen: un UE 100A, un dispositivo IP perimetral 100B y/o un servidor 100C de políticas. Los pasos son los siguientes:

Paso 201: El dispositivo IP perimetral 100B obtiene la información de las solicitudes de acceso de la sesión IP.

En este paso, durante el proceso de la sesión IP la AICU 101B del dispositivo IP perimetral obtiene del GSSMU 103B la información de las solicitudes de acceso de la sesión IP especificada y le indica a la IMU 104B que lleve a cabo la asociación de la información de acceso. La información de las solicitudes de acceso procede de un directorio local o de otro servidor de políticas de la red, como, por ejemplo, un servidor DHCP o un servidor AAA. La AICU 101B puede hacerle la petición a la IMU 104B mediante el envío a la IMU 104B de una orden de operación. La orden de operación incluye el identificador de la sesión IP, junto con la información de las solicitudes de acceso. El identificador de la sesión IP incluye, al menos, uno de los siguientes elementos: la dirección IP, la dirección MAC del UE y el ID del UE.

Paso 202: El dispositivo IP perimetral 100B incluye la información de las solicitudes de acceso en el mensaje de señalización de control de la sesión IP, y envía el mensaje al UE de la sesión IP y/o al servidor de políticas que presta servicio a la sesión IP.

Más concretamente, la IMU 104B del dispositivo IP perimetral 100B asocia la información de las solicitudes de acceso al mensaje de señalización de control de la sesión IP y, a continuación, le indica a la GSSPU 102B que procese la información. Por ejemplo, la GSSPU 102B incluye la información de acceso en el mensaje de señalización de control de la sesión IP y, a continuación, reenvía el mensaje de señalización de control de la sesión IP que incluye la información de las solicitudes de acceso al UE 100A y/o al servidor 100C de políticas.

En este paso, la IMU 104B le indica a la GSSPU 102B que inserte o incluya la información de las solicitudes de acceso, o los códigos correspondientes a la información de las solicitudes de acceso, en el mensaje de señalización

de control especificado por la sesión IP. La IMU 104B asocia o convierte la información de las solicitudes de acceso en los códigos de información de las solicitudes. La GSSPU 102B inserta la información de las solicitudes de acceso, determina el destino del mensaje de señalización de control de la sesión IP (es decir, el cliente IP al que va destinado el mensaje de señalización de control de la sesión IP), y envía el mensaje de señalización de control de la sesión IP. El paso de determinación del destino del mensaje de señalización de control de la sesión IP incluye: buscar el destino del mensaje de señalización de control de la sesión IP en función del identificador de la sesión IP.

Paso 203: El UE 100A de la sesión IP y/o el controlador 100C de políticas que presta servicio a la sesión IP, realiza la gestión correspondiente de acuerdo con la información de las solicitudes de acceso incluidas en la información de control de la sesión IP recibida.

Más concretamente, la CIAU 103A del UE 100A obtiene de la CSSPU 102A la información de las solicitudes de acceso incluida en el mensaje de señalización de control de la sesión IP, y/o la SIAU 103C del controlador 100C de políticas obtiene de la SSSPU 102C la información de las solicitudes de acceso incluida en el mensaje de señalización de control de la sesión IP, y lleva a cabo la gestión correspondiente. En este paso, la gestión de la información de la solicitud de acceso realizada por el UE 100 puede incluir: que la CIAU 103A muestre al usuario la información de la solicitud de acceso a través de la interfaz de la CIPU 101A, o lo que es lo mismo, le pide al usuario que tome las medidas correspondientes; o que la CIAU 103A registre o almacene la información de la solicitud de acceso recibida. La información de la solicitud de acceso realizada por el controlador 100C de políticas incluye: la obtención por parte de la SIAU 103C de una copia de seguridad de la información de la solicitud de acceso recibida para su posterior mantenimiento, diagnóstico, rastreo y estadísticas.

El proceso de la información de las solicitudes de acceso en las sesiones IP en la presente invención incluye cuatro partes, que se detallan más abajo mediante referencia a la FIG. 3.

El proceso de establecimiento de la sesión IP tiene dos resultados posibles: éxito en el establecimiento, y fallo en el establecimiento. Como se muestra en la FIG. 3, la alternativa relacionada con el fallo en el establecimiento incluye los siguientes pasos:

Paso 301: El UE 100A intenta acceder a la red, es decir, establecer una sesión IP.

Más concretamente, la CSSPU 102A del UE 100A envía un mensaje de detección de establecimiento de sesión al dispositivo IP perimetral 100B.

En este paso, el UE es un cliente de la sesión IP; el mensaje de detección de establecimiento de la sesión es un mensaje de señalización de control de la sesión IP, por ejemplo, un mensaje DHCP de descubrimiento, un mensaje DHCP de solicitud y un mensaje DHCP AUTH (Autenticación).

Paso 302: Después de recibir el mensaje de detección de establecimiento de la sesión, la GSSPU 102B del dispositivo IP perimetral 100B le indica a la GSSMU 103B que ejecute el proceso de establecimiento de la sesión IP, como, por ejemplo, la autenticación y autorización. Si el intento de establecer la sesión IP falla, la GSSMU 103B le indica o notifica a la AICU 101B la causa de fallo en el establecimiento de la sesión IP.

Paso 303: La AICU 101B del dispositivo IP perimetral 100B le notifica a la IMU 104B la información de la solicitud de la sesión (causa de fallo en el establecimiento de la sesión IP). La IMU 104B convierte la causa de fallo en el establecimiento de la sesión IP en un código de error y, a continuación, le indica a la GSSPU 102B que inserte o incluya la causa de fallo en el establecimiento de la sesión IP o el código de error en la notificación de la causa de fallo en el establecimiento de la sesión IP. Posteriormente, la GSSPU 102B envía al UE la notificación de la causa de fallo en el establecimiento de la sesión IP.

La notificación de la causa de fallo en el establecimiento de la sesión IP es un mensaje de señalización de control de la sesión IP, que puede ser un mensaje DHCP o un mensaje del Protocolo de Autenticación Extensible (EAP). La causa de fallo en el establecimiento de la sesión IP se puede incluir en un campo existente o en un campo de ampliación de un mensaje DHCP o de un mensaje EAP.

La alternativa relacionada con el éxito en el establecimiento incluye los siguientes pasos:

Paso 304: El UE 100A intenta acceder a la red, es decir, establecer una sesión IP.

Por ejemplo, el UE 100A envía un mensaje al dispositivo IP perimetral 100B.

Paso 305: Después de recibir el mensaje de detección de establecimiento de la sesión, el dispositivo IP perimetral 100B establece una sesión IP. Si el intento de establecer la sesión IP tiene éxito, el dispositivo IP perimetral 100B obtiene la información de la solicitud que indica el éxito en el establecimiento de la sesión IP, y utiliza esta información como información de la solicitud de acceso.

Paso 306: El dispositivo IP perimetral 100B le notifica al UE 100A la información de la solicitud que indica el éxito en el establecimiento de la sesión IP, por ejemplo, envía una notificación de éxito en el establecimiento de la sesión que incluye la información de la solicitud que indica el éxito en el establecimiento de la sesión IP.

La notificación de éxito en el establecimiento de la sesión es un mensaje de señalización de control de la sesión IP, que puede ser un mensaje DHCP o un mensaje EAP. La información de la solicitud que indica el éxito en el establecimiento de la sesión IP se puede incluir en un campo existente o en un campo de ampliación de un mensaje DHCP o de un mensaje EAP. La información de la solicitud que indica el éxito en el establecimiento de la sesión IP incluye información de carácter comercial e información contable del usuario.

Como se muestra en la FIG. 3, durante el proceso de mantenimiento de la sesión IP, la interacción entre el UE 100A y el dispositivo IP perimetral 100B incluye los siguientes pasos.

Paso 307: El dispositivo IP perimetral 100B obtiene la información de la solicitud de acceso y envía al UE 100A de la sesión IP una notificación de información de la solicitud de acceso para el mantenimiento de la sesión, donde la notificación incluye la información de la solicitud de acceso. Más concretamente, la AICU 101B obtiene la información de la solicitud de acceso y le notifica a la IMU 104B la información de la solicitud de la sesión (información de carácter comercial e información contable). La IMU 104B asocia la información de la solicitud de la sesión al mensaje de señalización de control de la sesión IP especificado (mensaje de mantenimiento) y, a continuación, le indica a la GSSPU 102B que inserte o incluya la información de la solicitud al mensaje de mantenimiento de la sesión IP. La GSSPU 102B envía al UE 100A el mensaje de mantenimiento.

La notificación de la información de la solicitud de acceso para el mantenimiento de la sesión es un mensaje de señalización de control de la sesión IP. La información de la solicitud de acceso incluye información de carácter comercial e información contable del usuario. La notificación de la información de la solicitud de acceso para el mantenimiento de la sesión puede ser un mensaje del protocolo BFD o un mensaje DHCP. Más concretamente, se puede añadir un campo de Opción al mensaje BFD de control, al mensaje BFD de eco, al mensaje DHCP de eco o al mensaje DHCP de dirección IP temporal (lease) activa, y entonces la información de la solicitud de acceso se incluye en el campo de Opción.

Como se muestra en la FIG. 3, en el proceso de terminación de la sesión IP, la interacción entre el UE 100A y el dispositivo IP perimetral 100B incluye los siguientes pasos.

Paso 308: El dispositivo IP perimetral 100B detecta la terminación de la sesión IP. Al detectar la terminación de la sesión IP, la GSSMU 103B ejecuta el proceso de terminación para la sesión IP y, a continuación, le indica o notifica a la AICU 101B la causa de terminación de la sesión IP (o, lo que es lo mismo, el dispositivo IP perimetral 100B obtiene la causa de terminación). La causa de terminación de la sesión IP es uno de los tipos de información de las solicitudes de acceso.

Paso 309: El dispositivo IP perimetral 100B envía al UE 100A una notificación de la causa de terminación de la sesión. La notificación incluye la causa de terminación de la sesión IP. Más concretamente, la AICU 101B del dispositivo IP perimetral notifica a la IMU 104B la causa de terminación de la sesión IP. La IMU 104B convierte la causa de terminación de la sesión IP en un código de causa de terminación, y le indica a la GSSPU 102B que inserte o incluya la causa o el código de terminación de la sesión IP en la notificación de la causa de terminación de la sesión IP. Posteriormente, la GSSPU 102B envía al UE 100A la notificación de la causa de terminación de la sesión IP.

En este paso, la notificación de la causa de terminación de la sesión IP es un mensaje de señalización de control de la sesión IP, y puede ser un mensaje DHCP o un mensaje del protocolo BFD.

Paso 310: El dispositivo IP perimetral 100B envía al servidor 100C de políticas un mensaje de indicación de terminación de la sesión. El mensaje de indicación de terminación de la sesión incluye el código de la causa de terminación de la sesión IP.

En este paso, el mensaje de indicación de terminación de la sesión es un mensaje de señalización de control de la sesión IP, por ejemplo un mensaje RADIUS de contabilización o un mensaje del protocolo de autenticación, autorización y contabilización de abonado (protocolo Diameter). El paso 309 puede ocurrir antes, simultáneamente o después del paso 310.

En el proceso de terminación de la sesión IP de la FIG. 3, el mensaje de indicación de terminación de la sesión enviado por el dispositivo IP perimetral 100B incluye el código de la causa de terminación de la sesión IP. Más concretamente, el código se puede incluir en un campo de parámetros en un mensaje RADIUS o en un mensaje Diameter, y el campo de parámetros puede ser Field (Campo), Attribute (Atributo) o un par Attribute-Value (AVP). Después de recibir el mensaje de indicación de terminación de la sesión, el servidor 100C de políticas lleva a cabo la gestión correspondiente de acuerdo con la causa de terminación de la sesión IP incluida en el mensaje de indicación de terminación de la sesión. El proceso detallado se ilustra mediante un ejemplo más abajo:

El dispositivo IP perimetral 100B incluye la causa de terminación de la sesión IP en un campo Acct-Terminate-Cause (Causa de Terminación de la Contabilización) de un mensaje Accounting-Request (Solicitud de Contabilización) en un mensaje del protocolo RADIUS o en un mensaje del protocolo Diameter, donde el campo es "Field" o "Attribute" o AVP; a continuación, envía el mensaje Accounting-Request al servidor 100C de políticas. En este caso, el servidor 100C de políticas puede ser un servidor AAA.

Alternativamente, el dispositivo IP perimetral 100B incluye la causa de terminación de la sesión IP en un campo Disconnect-Cause (Causa de Desconexión) (este campo es un AVP) de un mensaje Disconnect-Peer-Request (Solicitud de Desconexión de un Igual) en un mensaje del protocolo Diameter, o a un campo Termination-Cause (Causa de Terminación) de un mensaje Session-Termination-Request (Solicitud de Terminación de Sesión) o de un mensaje Accounting-Request (Solicitud de Contabilización); a continuación, envía al servidor 100C de políticas el mensaje del protocolo Diameter. En este caso, el servidor 100C de políticas puede ser un servidor AAA.

En el proceso que se muestra en la FIG. 3, el dispositivo IP perimetral 100B incluye la información de las solicitudes de acceso en un mensaje del protocolo BFD, en un mensaje DHCP o en un mensaje EAP, y envía el mensaje al UE 100A.

El proceso detallado incluye los siguientes pasos:

El dispositivo IP perimetral 100B envía al UE 100A un mensaje del protocolo BFD que incluye la información de la solicitud de acceso. Como se muestra en la FIG. 4, el mensaje del protocolo BFD incluye un bloque de encabezamiento (header) del mensaje BFD y un cuerpo del mensaje BFD. El bloque de encabezamiento del mensaje BFD incluye un bloque de encabezamiento IP y un bloque de encabezamiento UDP. El mensaje BFD incluye un campo de Diagnóstico o un campo de Opción de Información. En el modo de realización que se ilustra en la FIG. 3, la GSSPU 102B del dispositivo IP perimetral 100B incluye la información de la solicitud en el campo de Diagnóstico o en el campo de Opción de Información y, a continuación, envía el mensaje al UE 100A. Por ejemplo, el IMU 104B del dispositivo IP perimetral 100B convierte la causa de terminación de la sesión IP en un código de causa de terminación y, a continuación, le indica al GSSPU 102B que incluya el código en el campo 402A de Diagnóstico del mensaje del protocolo BFD. Posteriormente, el dispositivo IP perimetral 100B envía el mensaje de control BFD al UE 100A. El UE 100A obtiene la causa de terminación de la sesión IP a partir del mensaje de control BFD enviado por el dispositivo IP perimetral 100B y, a continuación, lleva a cabo la gestión correspondiente, por ejemplo, muestra en la interfaz la causa de terminación de la sesión IP. En otro ejemplo, en el mensaje de control BFD se incluye un campo de Opción de Información a través de un campo de Opción existente o de un campo de Opción de ampliación del mensaje del protocolo BFD. El campo de Opción de Información incluye el Tipo de Información, la Longitud de la Información y los Datos de la Información. En el campo de Opción de Información del mensaje del protocolo BFD se incluyen la información de tipo publicitario, la información de tipo contable de usuario o el tipo de causa de terminación de la sesión IP. La IMU 104B del dispositivo IP perimetral 100B realiza la asociación del código de tipo, y la GSSPU 102B del dispositivo IP perimetral 100B lleva a cabo la inserción de la información de la solicitud de acceso, la asociación de la sesión IP al mensaje de señalización y el envío del mensaje. La asociación de la sesión IP con el mensaje de señalización puede consistir en la asociación con la sesión IP a través de la dirección IP de destino o del bloque de encabezamiento IP.

Alternativamente, el dispositivo IP perimetral 100B envía al UE 100A un mensaje DHCP que incluye la información de la solicitud de acceso. Como se muestra en la FIG. 5, el mensaje DHCP incluye un bloque de encabezamiento del mensaje DHCP y un cuerpo del mensaje DHCP. El bloque de encabezamiento del mensaje DHCP incluye un bloque de encabezamiento IP y un bloque de encabezamiento UDP. El mensaje DHCP incluye un Identificador de Transacción (XID), un tipo de mensaje DHCP y una Opción DHCP. La GSSPU 102B del dispositivo IP perimetral 100B incluye en el mensaje DHCP la información de la solicitud como un campo de Opción DHCP. La Tabla 1 describe la información de la solicitud de acceso permitida por el mensaje DHCP:

Tabla 1

Mensaje DHCP	Opción de Información de Solicitud Permitida
DHCP de descubrimiento (Discover/SOLICIT)	El mensaje enviado por el UE al IP perimetral no puede incluir una opción de solicitud de acceso.
DHCP de ofrecimiento Offer/ADVERTISE	El mensaje puede incluir una opción de información de solicitud de acceso, como las de carácter comercial.
Mensaje DHCP de confirmación de aceptación (Ack/REPLY)	El mensaje puede incluir una opción de información de solicitud de acceso, como las de carácter comercial y de contabilización.
Mensaje DHCP de reconfiguración (Renew/Reconfigure)	El mensaje puede incluir una opción de información de solicitud de acceso, como las de carácter comercial y de causa de terminación de la sesión.
Mensaje DHCP de denegación (NAK)	El mensaje puede incluir una opción de información de solicitud de acceso, como las de carácter comercial, de causa de terminación de la sesión y de fallo en el establecimiento de la sesión.
Mensaje DHCP de eco o Mensaje DHCP de dirección IP temporal	El mensaje puede incluir una opción de información de solicitud de acceso, como las de carácter comercial, de causa de terminación de la sesión y de contabilización.

Por ejemplo, el DHCP transporta la información de esta forma: La AICU 101B del dispositivo IP perimetral 100B obtiene la información de la solicitud y le indica a la IMU 104B que lleve a cabo la asociación de la información (asociar la información de la solicitud de acceso con un código de información de la solicitud de acceso, o asociar la información de la solicitud de acceso con el mensaje de señalización de control de la sesión IP del tipo especificado). La IMU 104B le indica a la GSSPU 102B que incluya en el mensaje DHCP la información de la solicitud como un campo de Opción DHCP. La GSSPU 102B permite utilizar el relay (repetidor) o el proxy (dispositivo de filtro/barrera) DHCP para procesar el mensaje DHCP, y la GSSPU 102B también permite que el mensaje DHCP sea procesado en el modo servidor DHCP.

Alternativamente, el dispositivo IP perimetral 100B permite que la información de las solicitudes de acceso se incluya en un campo existente o en un campo de ampliación del mensaje EAP. Este campo transporta la información de las solicitudes de acceso, e incluye la causa de fallo en la identificación inicial del usuario o la información de éxito en el establecimiento de la sesión IP. En este modo de realización, el EAP actúa como mecanismo de autenticación general y se puede incluir en un mensaje DHCP o en un mensaje del Protocolo de Paquetes de Datos de Usuario (UDP).

A continuación se proponen más modos de realización para ampliar el método objeto de la presente invención.

La FIG. 6 muestra cómo notifica un dispositivo IP perimetral a un UE la causa de fallo en una identificación inicial (login) de un usuario o la causa de fallo en el establecimiento de una sesión IP en un modo de realización de la presente invención. A continuación se describen detalladamente los pasos:

Paso 601: El UE envía un mensaje de control de acceso para establecer una sesión IP. El mensaje de control de acceso incluye la información de la sesión de acceso.

En este modo de realización, el mensaje de control de acceso puede ser, pero no está limitado a: un mensaje de descubrimiento DHCP, o un mensaje de solicitud DHCP o un mensaje DHCP AUTH.

Paso 602: Después de recibir el mensaje de control de acceso enviado por el UE, el dispositivo IP perimetral analiza el mensaje de control de acceso y obtiene la información de la sesión de acceso y, a continuación, lleva a cabo el proceso de acceso, autenticación y autorización.

En este paso, la información de la sesión de acceso incluye, pero no está limitada a: el nombre del usuario y la dirección del UE. El proceso de acceso, autenticación y autorización puede consistir en: enviar al servidor de políticas un mensaje RADIUS Access-Request para ejecutar la autenticación y la autorización.

Paso 603: Después de recibir el mensaje de acceso, autenticación y autorización enviado por el dispositivo IP perimetral, el servidor de políticas ejecuta el proceso de autorización: si la autenticación y la autorización fallan, el servidor de políticas devuelve un mensaje de denegación de acceso al dispositivo IP perimetral. El mensaje de denegación de acceso incluye información de la denegación de la solicitud de acceso.

En este paso, el mensaje de denegación de acceso puede ser un mensaje RADIUS Access-Reject (Denegación de Acceso), y la información de la denegación de la solicitud de acceso puede incluir "error de contraseña" o un código de causa (0x301). Por ejemplo, El Mensaje de Respuesta del mensaje RADIUS Access-Reject sirve como información de solicitud de acceso.

Paso 604: El dispositivo IP perimetral recibe el mensaje de denegación de acceso devuelto por el servidor de políticas, obtiene la información de la solicitud de acceso incluida en el mensaje de denegación de acceso, construye un mensaje de señalización de control de la sesión IP que incluye la información de la solicitud de acceso y se lo envía al UE.

En este modo de realización, existen diferentes causas para el fallo en el establecimiento de la sesión IP. La causa se puede asociar a un código de causa, como se muestra en la Tabla 2. La Tabla 2 proporciona las relaciones de asociación entre las causas comunes de fallo en el establecimiento de la sesión IP y los códigos de causa.

Tabla 2

Causa del fallo en el establecimiento de la sesión IP	Código de Causa
El nombre de usuario o la contraseña son incorrectos.	0x301 (0x representa un valor hexadecimal)
El saldo de la cuenta de suscripción del usuario no es suficiente.	0x302
Los recursos del sistema son insuficientes.	0x303
Fallo en la configuración de la sesión basada en el Protocolo de Control de Nodo de Acceso (ANCP) o el Mecanismo de Control de la Capa 2 (L2CM).	0x304
La dirección o identificación del terminal no es válida.	0x305

En este paso, el mensaje de señalización de control de la sesión IP puede incluir, además, la información de la sesión de acceso.

En este paso, el mensaje de señalización de control de la sesión IP que incluye la información de la solicitud de acceso puede ser un mensaje DHCP Offer, un mensaje DHCP Advertise, un mensaje DHCP NAK o un mensaje DHCP AUTH. El mensaje de señalización de control de la sesión IP puede incluir un campo de Opción. Este campo contiene información de la denegación de la solicitud de acceso o el código de la causa. Si el mensaje de señalización de control de la sesión IP es un mensaje EAP+DHCP AUTH (el EAP es transportado por el mensaje DHCP para la autenticación, y "EAP+DHCP" se puede considerar como una combinación de EAP y DHCP), la información de la denegación de la solicitud de acceso puede estar incluida en el mensaje EAP.

En este paso, el dispositivo IP perimetral es responsable de la correlación y asociación entre el mensaje de denegación de acceso enviado por el servidor de políticas y el mensaje de señalización de control de la sesión IP enviado por el UE. La correlación se refiere a la correspondencia entre el mensaje de denegación de acceso y el mensaje de señalización de control de la sesión IP. Por ejemplo, cuando el mensaje de denegación de acceso recibido es un mensaje DHCP de descubrimiento, al UE se le devuelve como respuesta un mensaje DHCP Offer; si el mensaje de denegación de acceso recibido es un mensaje DHCP de solicitud, al UE se le devuelve como respuesta un mensaje DHCP de denegación. La asociación se refiere a la asociación de la información acerca de la sesión de acceso.

Paso 605: Después de recibir el mensaje de señalización de control de la sesión IP que incluye la información de la sesión de acceso, el UE realiza la gestión correspondiente.

En este paso, el proceso de dicha gestión es: El UE obtiene la información de la solicitud de acceso a partir del mensaje DHCP Offer, el mensaje DHCP de denegación o el mensaje DHCP AUTH que incluye la información de la solicitud de acceso, por ejemplo, obtiene la información sobre la denegación de la solicitud de acceso o el código de la causa y, a continuación, convierte la información de la solicitud de acceso en un texto y lo muestra en la interfaz, o registra la información de la solicitud de acceso.

La FIG. 7 muestra cómo notifica un dispositivo IP perimetral a un UE la información de identificación satisfactoria del usuario o de establecimiento satisfactorio de la sesión IP en un modo de realización de la presente invención. A continuación se describen detalladamente los pasos:

Paso 701: El UE envía un mensaje de control de acceso para establecer una sesión IP. El mensaje de control de acceso contiene la información de la sesión de acceso.

Paso 702: Después de recibir el mensaje de control de acceso enviado por el UE, el dispositivo IP perimetral analiza el mensaje de control de acceso y obtiene la información de la sesión de acceso, y, a continuación, lleva a cabo el proceso de acceso, autenticación y autorización.

Paso 703: Después de recibir el mensaje de acceso, autenticación y autorización enviado por el dispositivo IP perimetral, el servidor de políticas lleva a cabo el proceso de autorización: si la autenticación y autorización son satisfactorias, el servidor de políticas devuelve al dispositivo IP perimetral un mensaje de aceptación de acceso. El mensaje de aceptación de acceso incluye la información de la solicitud de acceso.

En este paso, el mensaje de aceptación de acceso puede ser un mensaje RADIUS Access-Accept (Aceptación de Acceso), y la información de la solicitud de acceso se puede incluir en un Reply-Message (Mensaje de Respuesta) de un mensaje RADIUS Access-Accept. La información de la solicitud de acceso puede incluir información contable del usuario, por ejemplo, la duración restante para el usuario, o la cantidad disponible en la cuenta, y también puede incluir información de carácter comercial, como la dirección IP del portal en una red de banda ancha.

Paso 704: El dispositivo IP perimetral recibe el mensaje de aceptación de acceso devuelto por el servidor de políticas, obtiene la información de la solicitud de acceso incluida en el mensaje de aceptación de acceso, construye un mensaje de señalización de control de la sesión IP que incluye la información de la solicitud de acceso y se lo envía al UE.

En este paso, el mensaje de señalización de control de la sesión IP que transporta la información de la solicitud de acceso es un mensaje DHCP Offer, un mensaje DHCP Advertise, un mensaje DHCP de confirmación (ACK o Reply) o un mensaje DHCP AUTH. El mensaje de señalización de control de la sesión IP incluye un campo Opción diseñado para incorporar la información de la solicitud de acceso obtenida por el dispositivo IP perimetral a partir del mensaje de aceptación de acceso y otra información de la solicitud de acceso obtenida por el dispositivo IP perimetral.

En este paso, la información de la solicitud de acceso obtenida por el dispositivo IP perimetral puede comprender información contable e información de carácter comercial. La información de la solicitud de acceso incluye la información de la solicitud de acceso obtenida por el dispositivo IP perimetral procedente de un directorio local o de otros servidores de la red. Por ejemplo, el dispositivo IP perimetral obtiene la información de la solicitud de acceso de otros servidores a través de la interfaz con dichos servidores.

Paso 705: Después de recibir el mensaje de señalización de control de la sesión IP que incluye la información de la solicitud de acceso, el UE lleva a cabo la gestión correspondiente.

En este paso, el proceso detallado de dicha gestión es: la CIAU del UE obtiene la información de la solicitud de acceso a partir del mensaje DHCP Offer, del mensaje DHCP de confirmación o del mensaje DHCP AUTH recibido de la CSSPU, por ejemplo, obtiene información contable del usuario o información de carácter comercial, y, a continuación, muestra la información de la solicitud de acceso.

En este paso, la CIAU activa un navegador web de acuerdo con la información de carácter comercial (por ejemplo, una dirección de un portal) incluida en la información de la solicitud de acceso (el navegador en este caso es una CIPU) y se muestra la información de carácter comercial, tal como una página web.

La FIG. 8 muestra el primer método utilizado por un dispositivo IP perimetral para notificar a un UE, o a un servidor de políticas durante el proceso de una sesión IP, la causa de terminación de una sesión IP en un modo de realización de la presente invención. A continuación se describen detalladamente los pasos:

Paso 801: Ya se ha establecido una sesión IP entre el UE y el dispositivo IP perimetral.

Paso 802: El dispositivo IP perimetral obtiene una indicación o evento para actualizar la sesión IP, le envía al UE un mensaje DHCP Reconfigure, donde el mensaje DHCP Reconfigure se construye localmente o se recibe desde el servidor DHCP e incluye información de la solicitud de acceso.

En este paso, la actualización IP de la información de la sesión IP puede consistir en modificar la configuración de la dirección de la sesión IP.

El mensaje DHCP Reconfigure puede ser un mensaje DHCP Forcenew (Forzar Nueva Dirección). El mensaje DHCP de actualización incluye información de la solicitud de acceso. La información de la solicitud de acceso puede ser una causa de terminación de la sesión IP con la finalidad de modificar la configuración de la sesión IP, y la información de la solicitud de acceso se puede incluir en un campo de Opción DHCP.

Paso 803: Después de recibir el mensaje DHCP Reconfigure, el UE analiza el mensaje DHCP Reconfigure para obtener la información de la solicitud de acceso e identificar la causa de terminación de la sesión IP, y, a continuación, envía un mensaje de solicitud de configuración al dispositivo IP perimetral.

En este paso, el mensaje de solicitud de configuración puede ser un mensaje DHCP Request.

Paso 804: El dispositivo IP perimetral reenvía al servidor DHCP el mensaje de solicitud de configuración recibido del UE.

Paso 805: Después de recibir el mensaje de solicitud de configuración, el servidor DHCP actualiza la información de la sesión IP, por ejemplo, modifica la dirección IP de la sesión IP establecida, y envía un mensaje DHCP NAK (Confirmación Negativa de Aceptación) al dispositivo IP perimetral.

Paso 806: El dispositivo IP perimetral recibe el mensaje DHCP NAK del servidor DHCP, realiza el proceso de terminación de la sesión IP y, a continuación, reenvía al UE el mensaje DHCP NAK. El dispositivo IP perimetral puede incluir información de la solicitud de acceso en el mensaje DHCP NAK antes de reenviarlo, como por ejemplo una causa de terminación de la sesión IP.

Paso 807: El dispositivo IP perimetral envía al servidor AAA un mensaje de detención de la contabilización o un mensaje de terminación de la sesión. El mensaje incluye la causa de terminación de la sesión IP, y le indica al servidor AAA que almacene la causa de terminación de la sesión IP. Si el servidor AAA y el dispositivo IP perimetral se encuentran en la misma entidad física, el servidor AAA puede interactuar con el dispositivo IP perimetral mediante una Interfaz de Programación de Aplicación (API). Este paso es opcional, en función de la implementación que se haga.

En este paso, el mensaje de detención de la contabilización o el mensaje de terminación de la sesión incluye: el mensaje Accounting-Request (Solicitud de Contabilización) del protocolo RADIUS o del protocolo Diameter, o el mensaje Session-Termination-Request (Solicitud de Terminación de Sesión) del protocolo Diameter.

Más concretamente, el dispositivo IP perimetral incluye la causa de terminación de la sesión IP en el campo Termination-Cause (Causa de Terminación) del mensaje Session-Termination-Request del protocolo Diameter o en el campo Acct-Terminate-Cause (Causa de Terminación de la Contabilización) del mensaje Accounting-Request del protocolo RADIUS o Diameter.

Paso 808: Después de recibir el mensaje DHCP NAK, el UE obtiene la información de la solicitud de acceso y modifica la configuración, por ejemplo, registra o muestra la información de la solicitud de acceso, o establece de nuevo una sesión IP en función de la información de la solicitud de acceso.

En la FIG. 8, el paso 806 puede ocurrir antes, simultáneamente o después del paso 807.

La FIG. 9 muestra cómo envía un dispositivo IP perimetral la información de las solicitudes de acceso a un UE durante un proceso de mantenimiento de una sesión IP en un modo de realización de la presente invención. A continuación se describen detalladamente los pasos:

Paso 901: El dispositivo IP perimetral obtiene la información de la solicitud de acceso, que incluye información de carácter comercial e información contable del usuario.

En este paso, el dispositivo IP perimetral puede obtener la información de la solicitud de acceso localmente, u obtener la información de la solicitud de acceso de otro servidor de la red. Por ejemplo, el dispositivo IP perimetral obtiene la información de la solicitud de acceso a partir del servidor de políticas a través de un mensaje RADIUS, y obtiene la información de la solicitud de acceso a medida que ésta se genera periódicamente o se genera mediante una aplicación externa tal como una orden de gestión de red.

Paso 902: El dispositivo IP perimetral envía al UE la información de la solicitud de acceso obtenida.

En este paso, la información de la solicitud de acceso puede estar incluida en un mensaje del protocolo BFD. Más concretamente, se puede añadir un campo Opción al mensaje BFD de control o al mensaje BFD de eco y, a continuación, se incluye la información de la solicitud de acceso en el campo Opción del mensaje BFD de control o del mensaje BFD de eco.

Paso 903: El UE ejecuta el proceso correspondiente. Más concretamente, el UE obtiene la información de la solicitud de acceso a partir del mensaje del protocolo BFD recibido, por ejemplo, obtiene la información contable del usuario o la información de carácter comercial. El UE muestra en la interfaz la información contable del usuario como notificación para el usuario. El UE muestra la información de carácter comercial en función de la propia información de carácter comercial, como, por ejemplo, la dirección IP de un portal.

La FIG. 10 muestra el segundo método utilizado por un dispositivo IP perimetral para notificar a un UE y a un servidor de políticas la causa de terminación de una sesión IP o la causa de desconexión de un usuario en un modo de realización de la presente invención. A continuación se describen detalladamente los pasos:

Paso 1001: El dispositivo IP perimetral detecta la orden de terminación de la sesión IP y envía al UE un mensaje de terminación de la sesión IP mediante un protocolo Keep-alive (mantenimiento) de la sesión. El mensaje de terminación de la sesión IP incluye una causa de terminación de la sesión IP.

En este modo de realización, existen diferentes causas de terminación de la sesión. Cada causa tiene asociado un código de causa, como se muestra en la Tabla 3. La Tabla 3 muestra las causas comunes de terminación de la sesión IP.

Tabla 3

Causa de Terminación de la Sesión IP	Código de Causa
El saldo de la cuenta de suscripción del usuario es insuficiente	0x401
Se ha agotado el tiempo máximo permitido de la sesión.	0x402
Los recursos del sistema son insuficientes (por ejemplo, el ancho de banda es insuficiente, o los recursos del dispositivo IP perimetral son insuficientes).	0x403
Se ha denegado el acceso al usuario (por ejemplo, el usuario accede a un sitio web no permitido o ataca la red de forma maliciosa).	0x404
La sesión se ha desconectado por razones de mantenimiento o de gestión (por ejemplo, el administrador desconecta la sesión de forma activa).	0x405
Falla la reautorización (por ejemplo, falla la política de reconfiguración de la sesión, o falla la reautenticación de la sesión IP).	0x406
La dirección temporal expira (por ejemplo, la dirección IP asignada de forma dinámica expira).	0x407

En este paso, la orden de terminación de la sesión IP es remitida por el sistema de gestión de red o el servidor de políticas, o localmente en un instante determinado (por ejemplo, al agotarse el tiempo máximo permitido de la sesión). La orden de terminación de la sesión IP puede ser una orden de desconexión activa de la sesión del UE, por ejemplo, un mensaje DHCP de desconexión del UE.

En este paso, el mensaje de terminación de la sesión IP puede ser enviado al UE mediante un mensaje del protocolo BFD. La causa de terminación de la sesión IP puede ser transportada en el campo del código de Diagnóstico (Diag) del mensaje BFD de control; en otros términos, el dispositivo IP perimetral incluye la causa de terminación de la sesión IP en el campo del código Diag del mensaje BFD de control y, a continuación, envía al UE un mensaje BFD de control de cambio de estado.

Paso 1002: El dispositivo IP perimetral envía al servidor de políticas una orden de terminación de la sesión IP (por ejemplo, un mensaje de detención de la contabilización, o un mensaje de terminación de la sesión IP), e incluye la causa de terminación de la sesión IP en el mensaje de detención de la contabilización o en el mensaje de terminación de la sesión IP. Este paso es opcional, en función de la implementación que se haga.

Paso 1003: Después de recibir el mensaje de terminación de la sesión IP, el UE ejecuta el proceso correspondiente, por ejemplo, registra o muestra la causa de terminación de la sesión IP, o establece de nuevo una sesión IP.

En el proceso que se muestra en la FIG. 10, el paso 1001 puede ocurrir antes, simultáneamente o después del paso 1002.

Asumiendo que el receptor dispone de un UE o un controlador de políticas, a continuación se detallan el sistema y el dispositivo proporcionados en un modo de realización de la presente invención.

Como se muestra en la FIG. 11, un sistema para procesar la información de las solicitudes de acceso en una sesión IP incluye:

un dispositivo IP perimetral, configurado para: obtener información de las solicitudes de acceso en una sesión IP, incorporar la información de las solicitudes de acceso de la sesión IP a un mensaje de señalización de control de la sesión IP, y enviar el mensaje de señalización de control de la sesión IP a un UE y/o a un controlador de políticas;

el UE, configurado para: recibir el mensaje de señalización de control de la sesión IP enviado por el dispositivo IP perimetral, y ejecutar las operaciones correspondientes de acuerdo con la información de las solicitudes de acceso transmitida en el mensaje de señalización de control de la sesión IP; y

el controlador de políticas, configurado para: recibir el mensaje de señalización de control de la sesión IP enviado por el dispositivo IP perimetral y ejecutar las operaciones correspondientes de acuerdo con la información de las solicitudes de acceso transmitida en el mensaje de señalización de control de la sesión IP.

El sistema puede incluir, además, un servidor, configurado par enviar al dispositivo IP perimetral la información de las solicitudes de acceso de la sesión IP. En este caso, el dispositivo IP perimetral obtiene la información de las solicitudes de acceso a partir del servidor.

Como se muestra en la FIG. 12, un dispositivo para procesar la información de las solicitudes de acceso de una sesión IP (por ejemplo, in dispositivo IP perimetral) incluye:

una GSSMU, configurada para: gestionar el estado de una sesión IP durante el proceso de una sesión IP, y proporcionar la información de las solicitudes de acceso;

una AICU, configurada para: obtener de la GSSMU la información de las solicitudes de acceso y, a continuación, indicarle a una IMU que lleve a cabo la correspondiente asociación para la información de las solicitudes de acceso;

la IMU, configurada para: llevar a cabo la correspondiente asociación para la información de las solicitudes de acceso de modo que la información de las solicitudes de acceso quede asociada a unos códigos de información de las solicitudes de acceso, o asociar la información de las solicitudes de acceso a un mensaje de señalización de control de la sesión IP de un tipo especificado, y enviar a la GSSPU la información de las solicitudes de acceso asociada; y

la GSSPU, configurada para: incluir en el mensaje de señalización de control de la sesión IP la información de las solicitudes de acceso asociada, y enviar el mensaje de señalización de control de la sesión IP al UE y/o al servidor de políticas.

La información de las solicitudes de acceso asociada enviada por la IMU a la GSSPU puede indicarle a la GSSPU que incluya la información de las solicitudes de acceso en el mensaje de señalización de control de la sesión IP especificado.

Adicionalmente, los modos de realización de la presente invención proporcionan un método y un dispositivo para procesar la información de las solicitudes de acceso desde la perspectiva del UE o del servidor de políticas.

Un método para procesar la información de las solicitudes de acceso incluye: obtener un mensaje de señalización de control de la sesión IP que contenga información de una solicitud de acceso de una sesión IP; y ejecutar las operaciones correspondientes de acuerdo con la información de la solicitud de acceso contenida en el mensaje de señalización de control de la sesión IP.

Se proporciona un dispositivo para procesar la información de las solicitudes de acceso. El dispositivo puede ser un UE o un servidor de políticas. Como se muestra en la FIG. 13, el dispositivo incluye:

una Unidad de Proceso de Señalización de la Sesión (SSPU), configurada para: recibir un mensaje de señalización de control de la sesión IP que incluye información de las solicitudes de acceso, y enviar el mensaje de señalización de control de la sesión IP a una Unidad de Adopción de Información (IAU);

la IAU, configurada para: obtener la información de las solicitudes de acceso contenida en el mensaje de señalización de control de la sesión IP, y enviar la información de las solicitudes de acceso a una Unidad de Proceso de las Solicitudes de Información (IPU); y

la IPU, configurada para ejecutar las operaciones correspondientes de acuerdo con la información de las solicitudes de acceso recibida de la IAU.

Mediante el método, el sistema y el dispositivo que se proporcionan en la presente invención, el dispositivo IP perimetral obtiene la información de las solicitudes de acceso durante el proceso de la sesión IP, e incluye la información de las solicitudes de acceso obtenida durante el proceso de la sesión IP en un mensaje de señalización de control de la sesión IP que se envía en el momento preciso al UE y/o al servidor de políticas, mejorando de este modo la percepción del usuario en la sesión IP. Después de recibir el mensaje de señalización de control de la sesión IP, el UE y/o el servidor de políticas analizan el mensaje para obtener la información de las solicitudes de acceso, y registran una copia de seguridad de la información de las solicitudes de acceso obtenida, mejorando de este modo la eficiencia del mantenimiento de la sesión IP y reduciendo el coste de la operación. Adicionalmente, la información de las solicitudes de acceso puede contener alguna información aportada activamente por el servidor de políticas, por ejemplo, información de carácter comercial, incrementando de ese modo el coste de operación del

acceso de banda ancha.

Para aquellos experimentados en la técnica resulta entendible que todos o parte de los pasos de los modos de realización precedentes se puedan implementar mediante hardware controlado por un programa de ordenador. El programa puede encontrarse almacenado en un medio de almacenamiento legible por el ordenador. Al ser ejecutado, el programa ejecuta los procesos que se han cubierto en los modos de realización anteriores. El medio de almacenamiento puede ser un disco magnético, un Disco Compacto (CD), una Memoria de Sólo Lectura (ROM) o una Memoria de Acceso Aleatorio (RAM).

REIVINDICACIONES

1. Un método para procesar información de solicitudes de acceso, que comprende:

gestionar un estado de una sesión del Protocolo de Internet, IP, entre un Equipo de Usuario, UE, y un dispositivo IP perimetral durante el proceso de una sesión IP, y proporcionar información de las solicitudes de acceso de la sesión IP, donde la información de las solicitudes de acceso comprende una causa de terminación de la sesión IP; estando caracterizado el método por

incluir la información de las solicitudes de acceso en un campo Opción de un mensaje de Detección de Reenvío Bidireccional, BFD, de la sesión IP, siendo el mensaje BFD un mensaje BFD enviado desde el dispositivo IP perimetral al equipo de usuario, UE, y siendo incluid la causa de terminación de la sesión IP en un campo Opción o en un campo Diagnóstico del mensaje BFD; y

enviar al UE el mensaje BFD que incluye la información de las solicitudes de acceso, para que el UE pueda ejecutar las operaciones correspondientes de acuerdo con la información de las solicitudes de acceso.

2. El método de la reivindicación 1, donde la información de las solicitudes de acceso es un código de causa obtenido de acuerdo con una tabla en la que se registran las relaciones de asociación entre las causas de terminación de la sesión IP y los códigos de causa.

3. Un sistema de comunicación, que comprende un dispositivo perimetral (100B) del Protocolo de Internet, IP, y un equipo de usuario, UE, (100A),

estando configurado el dispositivo perimetral (100B) del Protocolo de Internet, IP, para gestionar un estado de una sesión IP entre el dispositivo IP perimetral y el Equipo de Usuario, UE, (100A), durante el proceso de una sesión IP, obtener información de las solicitudes de acceso de la sesión IP, donde la información de las solicitudes de acceso comprende una causa de terminación de la sesión IP, incluir la información de las solicitudes de acceso de la sesión IP en un campo Opción de un mensaje de Detección de Reenvío Bidireccional, BFD, de la sesión IP, siendo el mensaje BFD un mensaje BFD enviado desde el dispositivo IP perimetral al UE, y siendo incluida la causa de terminación de la sesión IP en un campo Opción o en un campo Diagnóstico del mensaje BFD, y enviar al UE el mensaje BFD que incluye la información de las solicitudes de acceso, y

el UE, configurado para recibir el mensaje BFD enviado por el dispositivo IP perimetral, y ejecutar las operaciones correspondientes de acuerdo con la información de las solicitudes de acceso incluida en el mensaje BFD.

4. El sistema de la reivindicación 3, donde el dispositivo IP perimetral está configurado para proporcionar una tabla que registra las relaciones de asociación entre las causas de terminación de la sesión IP y los códigos de causa, y para proporcionar el código de causa asociado a la información de las solicitudes de acceso obtenido de acuerdo con la tabla que registra las relaciones de asociación entre las causas de terminación de la sesión IP y los códigos de causa.

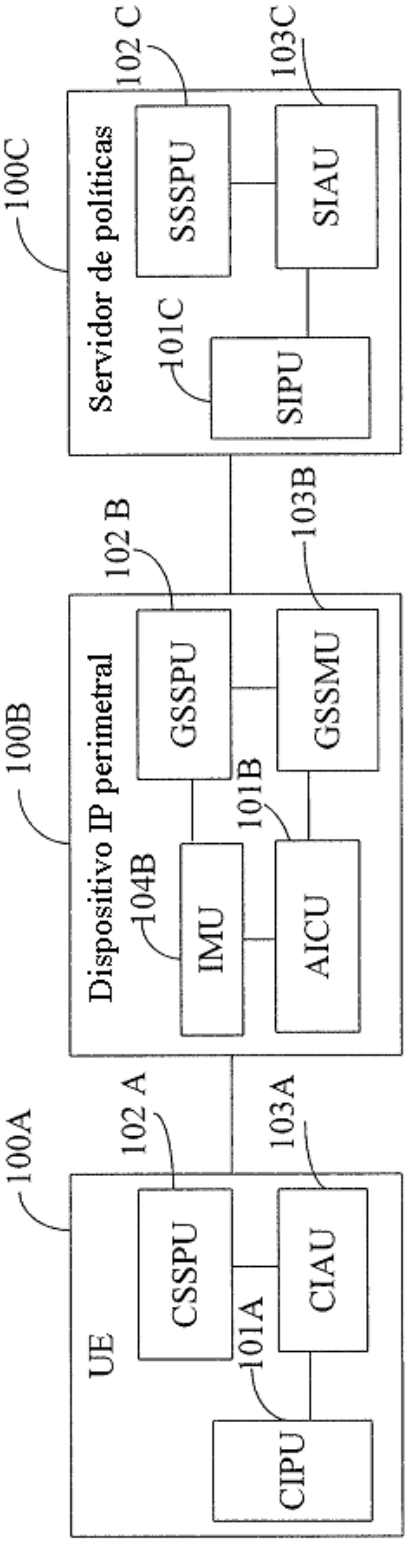
100A
UE
102 A
CSSPU
103A
CIAU
101A
CIPU
100B
Dispositivo IP perimetral
102 B
GSSPU
103B
GSSMU
101B
104B
IMU
AICU
100C
Servidor de políticas
102 C
SSSPU
103C
SIAU
101C
SIPU

FIG. 1

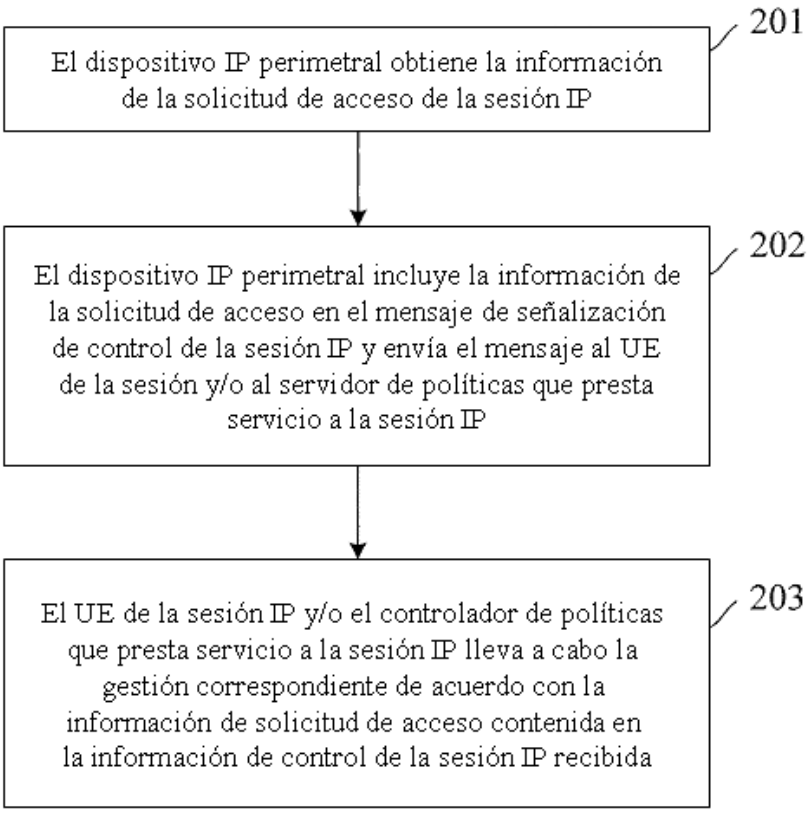
201
El dispositivo IP perimetral obtiene la información de la solicitud de acceso de la sesión IP
202
El dispositivo IP perimetral incluye la información de la solicitud de acceso en el mensaje de señalización de control de la sesión IP y envía el mensaje al UE de la sesión y/o al servidor de políticas que presta servicio a la sesión IP
203
El UE de la sesión IP y/o el controlador de políticas que presta servicio a la sesión IP lleva a cabo la gestión correspondiente de acuerdo con la información de solicitud de acceso contenida en la información de control de la sesión IP recibida

FIG. 2

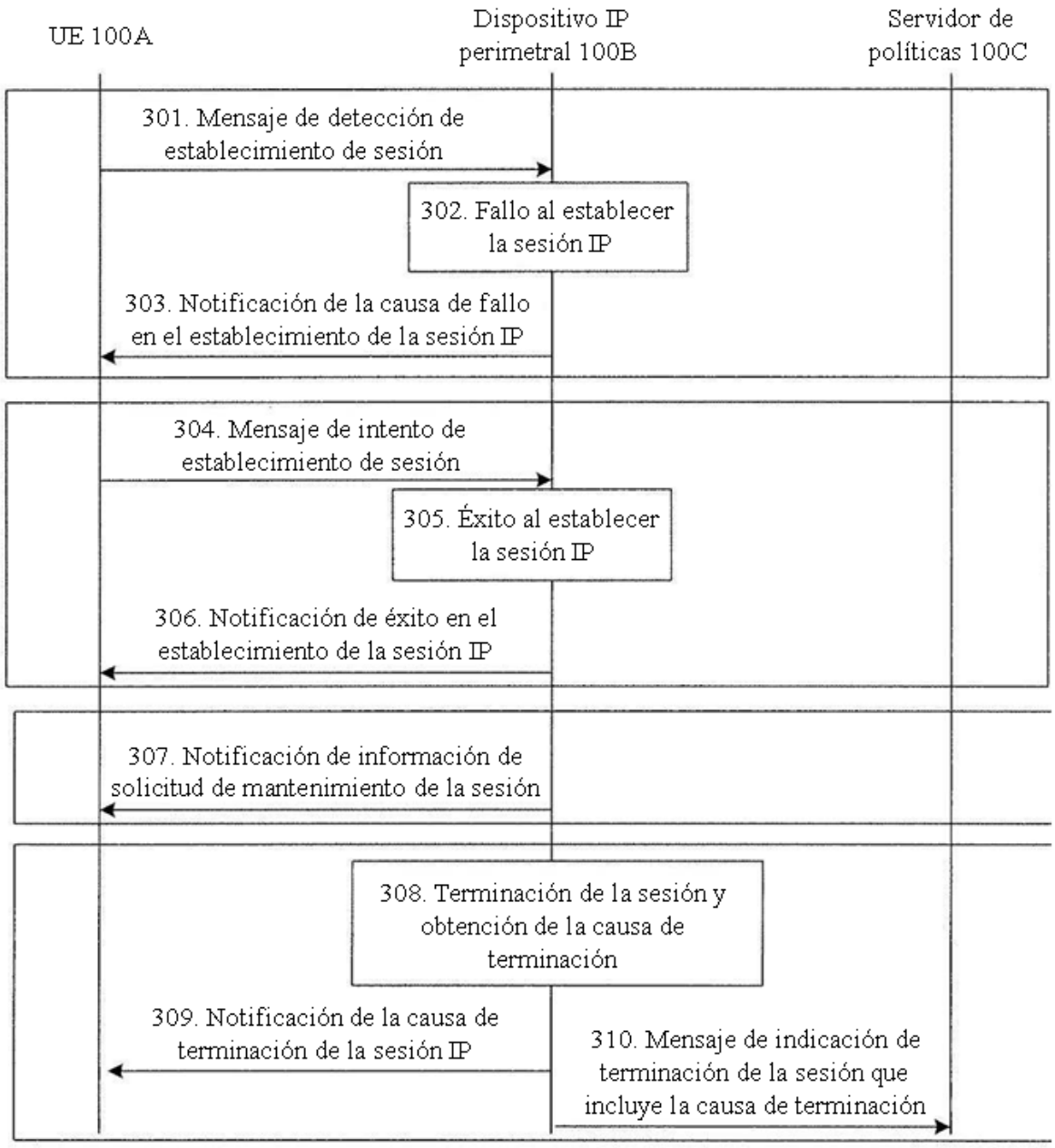
UE 100A
Dispositivo IP perimetral 100B
Servidor de políticas 100C
301. Mensaje de detección de establecimiento de sesión
302. Fallo al establecer la sesión IP
303. Notificación de la causa de fallo en el establecimiento de la sesión IP
304. Mensaje de intento de establecimiento de sesión
305. Éxito al establecer la sesión IP
306. Notificación de éxito en el establecimiento de la sesión IP
307. Notificación de información de solicitud de mantenimiento de la sesión
308. Terminación de la sesión y obtención de la causa de terminación
309. Notificación de la causa de terminación de la sesión IP
310. Mensaje de indicación de terminación de la sesión que incluye la causa de terminación

FIG. 3

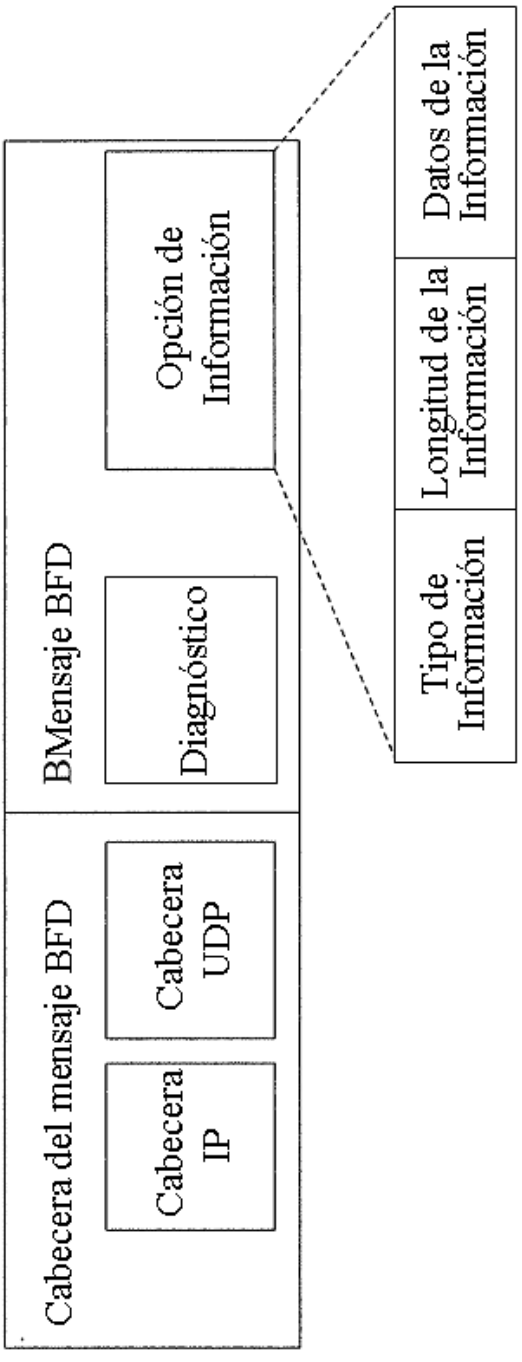
Cabecera del mensaje BFD
Cabecera IP
Cabecera UDP
BMensaje BFD
Diagnóstico
Opción de Información
Tipo de Información
Longitud de la Información
Datos de la Información

FIG. 4

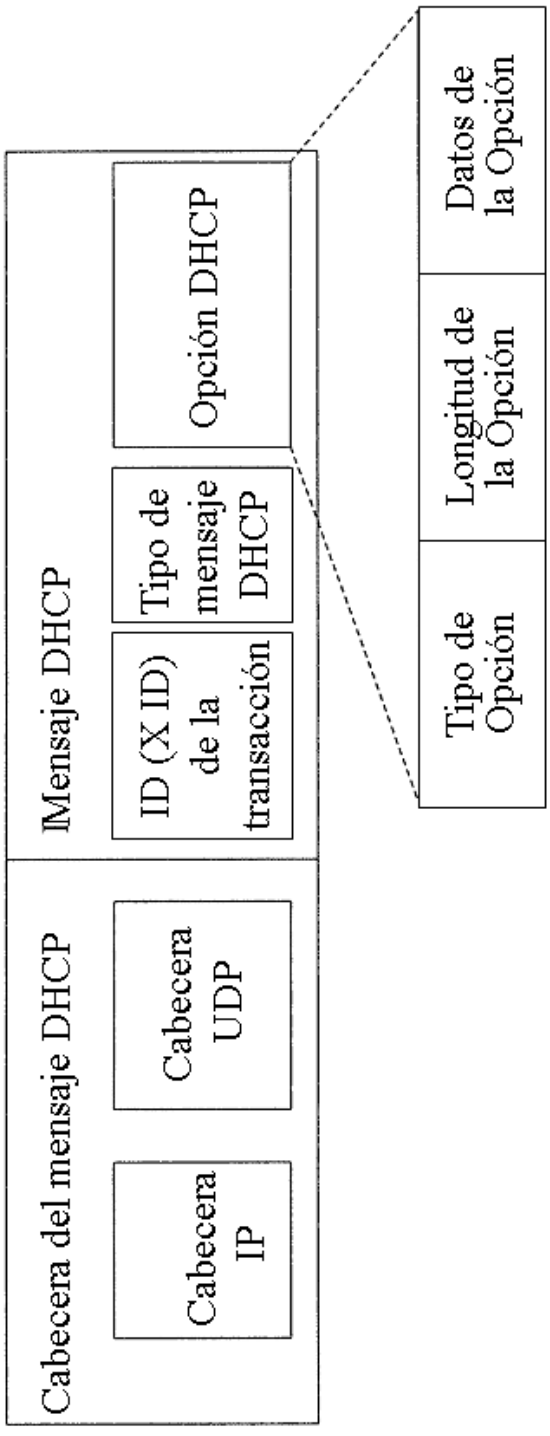
Cabecera del mensaje DHCP
Cabecera IP
Cabecera UDP
Mensaje DHCP
ID (X ID) de la transacción
Tipo de mensaje DHCP
Opción DHCP
Tipo de Opción
Longitud de la Opción
Datos de la Opción

FIG. 5

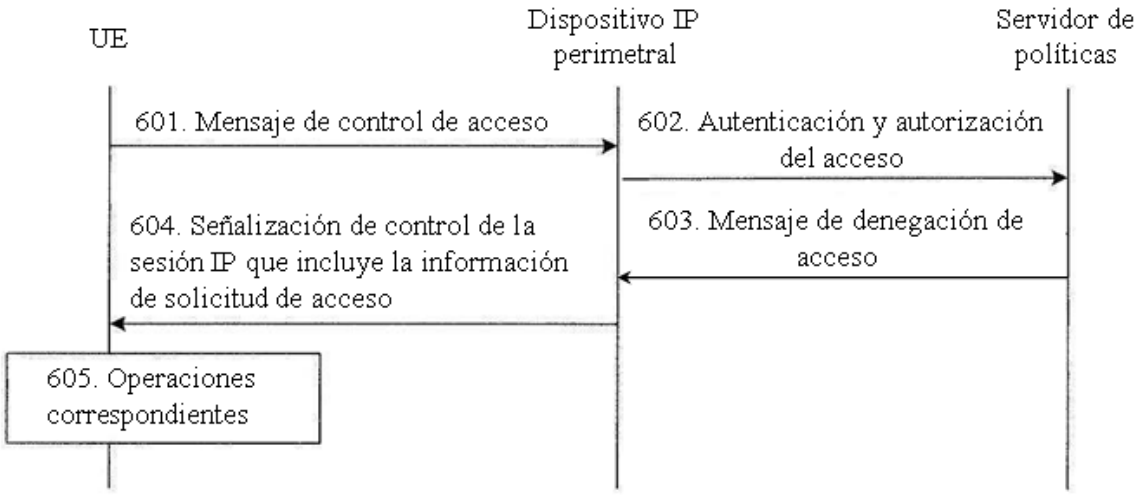
UE
Dispositivo IP perimetral
Servidor de políticas
601. Mensaje de control de acceso
602. Autenticación y autorización del acceso
603. Mensaje de denegación de acceso
604. Señalización de control de la sesión IP que incluye la información de solicitud de acceso
605. Operaciones correspondientes

FIG. 6

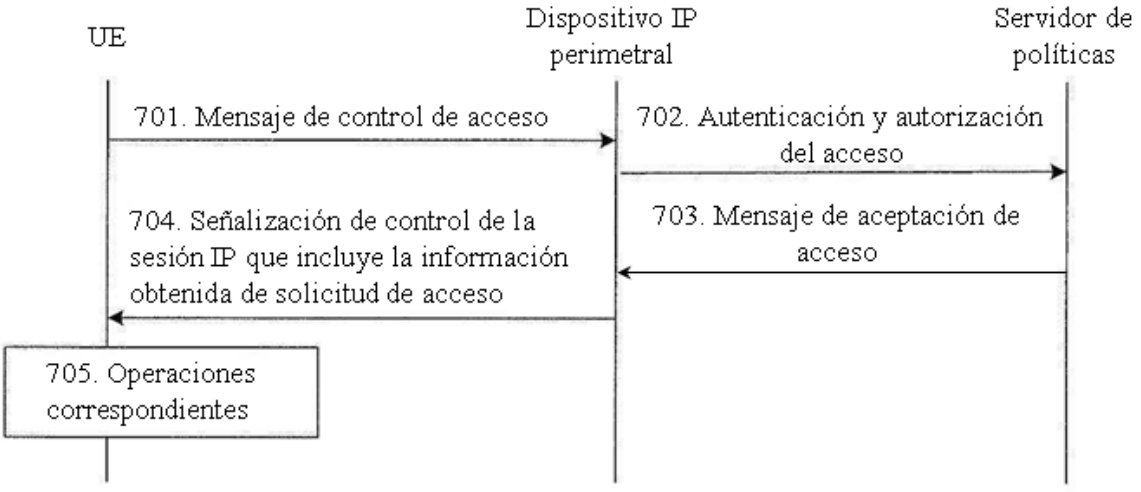
UE
Dispositivo IP perimetral
Servidor de políticas
701. Mensaje de control de acceso
702. Autenticación y autorización del acceso
703. Mensaje de aceptación de acceso
704. Señalización de control de la sesión IP que incluye la información obtenida de solicitud de acceso
705. Operaciones correspondientes

FIG. 7

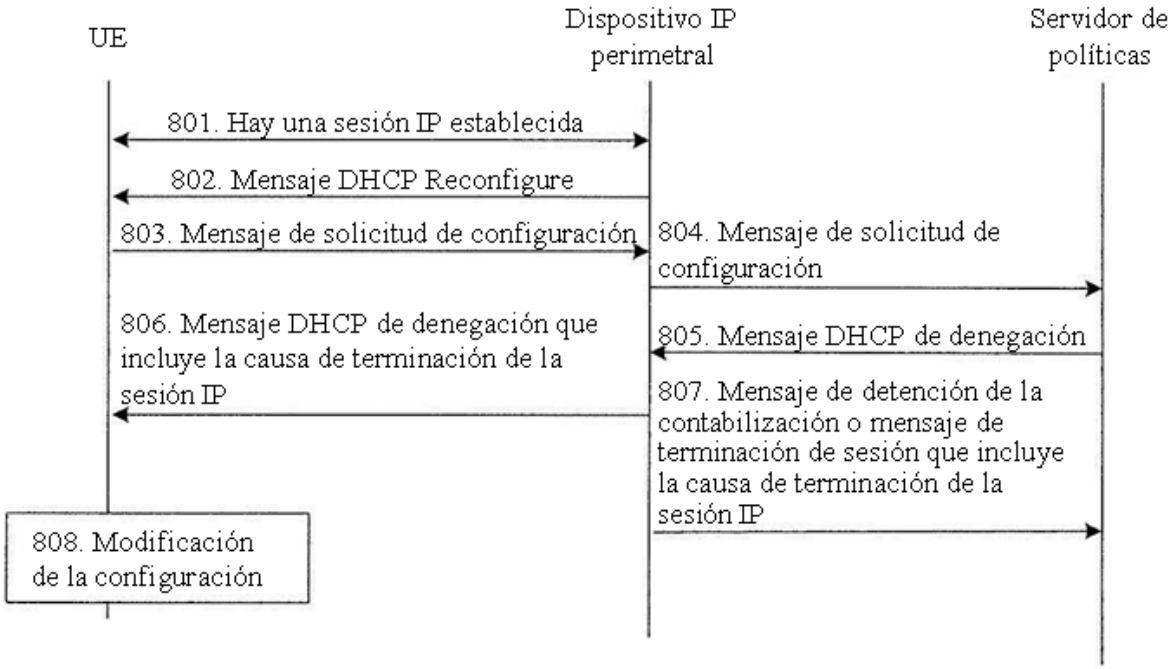
UE
Dispositivo IP perimetral
Servidor de políticas
801. Hay una sesión IP establecida
802. Mensaje DHCP Reconfigure
803. Mensaje de solicitud de configuración
804. Mensaje de solicitud de configuración
806. Mensaje DHCP de denegación que incluye la causa de terminación de la sesión IP
805. Mensaje DHCP de denegación
807. Mensaje de detención de la contabilización o mensaje de terminación de sesión que incluye la causa de terminación de la sesión IP
808. Modificación de la configuración

FIG. 8

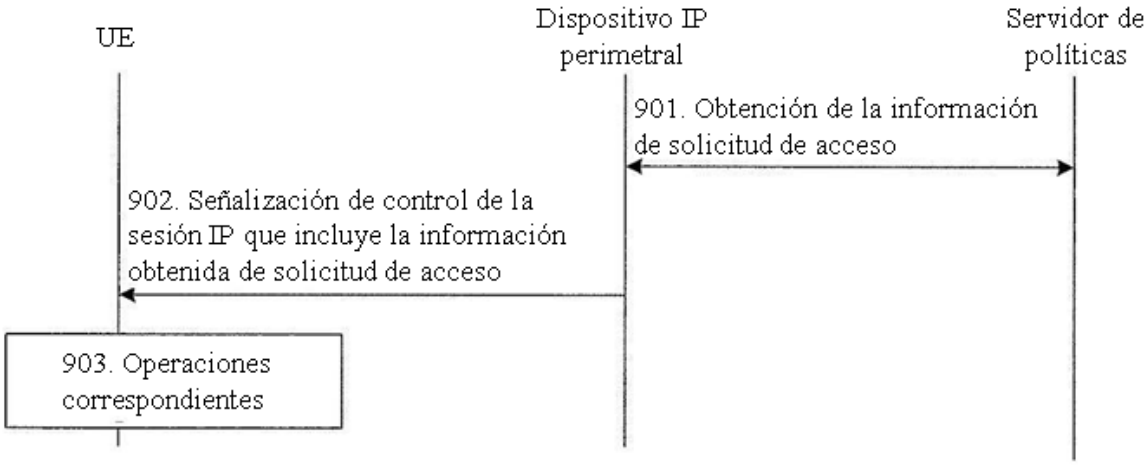
UE
Dispositivo IP perimetral
Servidor de políticas
901. Obtención de la información de solicitud de acceso
902. Señalización de control de la sesión IP que incluye la información obtenida de solicitud de acceso
903. Operaciones correspondientes

FIG. 9

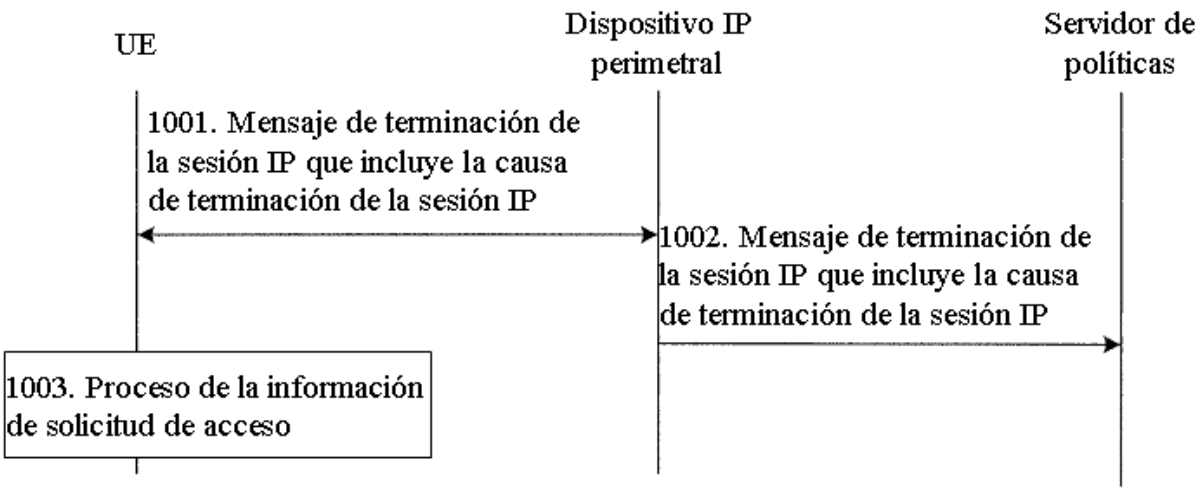

FIG. 10

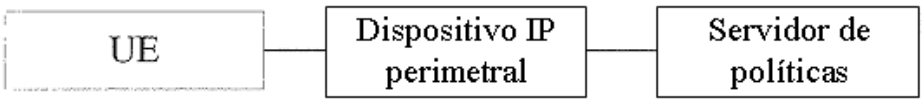

FIG. 11

FIG. 12

FIG. 13