(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 381 857**

(51) Int. CI.:
H04L 12/24 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06741751 .9**
(96) Fecha de presentación: **28.04.2006**
(97) Número de publicación de la solicitud: **1876754**
(97) Fecha de publicación de la solicitud: **09.01.2008**

(54) Título: **Método, sistema y servidor para poner en práctica la asignación de seguridad de dirección de protocolo DHCP**

(30) Prioridad:
29.04.2005 CN 200510069417

(45) Fecha de publicación de la mención BOPI:
01.06.2012

(45) Fecha de la publicación del folleto de la patente:
01.06.2012

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

(72) Inventor/es:
WEI, Jiahong;
LI, Jun y
CHEN, Wumao

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Método, sistema y servidor para poner en práctica la asignación de seguridad de dirección de protocolo DHCP.

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo técnico de comunicaciones de redes, en particular, a un método, un sistema y un servidor para realizar una asignación segura de una dirección de protocolo de Configuración Dinámica de Concentrador (DHCP).

ANTECEDENTES DE LA INVENCIÓN

A medida que se desarrollan, cada vez más, las tecnologías de acceso tales como ADSL (Línea de Abonado Digital Asimétrica) y Ethernet, el acceso de banda ancha se hace cada vez más popular y los servicios de vídeo de IPTV (Televisión de Protocolo Internet) y VoIP (Protocolo de Voz sobre Internet) desarrollados, basándose en la red de acceso de banda ancha, tienen una aplicación más amplia. El desarrollo de cada servicio necesita utilizar un terminal dedicado; por ejemplo, el servicio de vídeo necesita utilizar un STB (Caja Decodificadora) y el servicio de voz necesita utilizar IAD (Dispositivo de Acceso Integrado). Cada terminal dedicado necesita obtener una dirección local antes de que se realice un servicio y luego, cada servicio se puede prestar utilizando la dirección local.

En una red de comunicación, cada terminal suele obtener una dirección de IP (Protocolo de Internet) sobre la base de un protocolo DHCP. Sin embargo, en un servicio en línea tradicional, se suele utilizar el protocolo PPPoE (Protocolo Punto a Punto sobre Ethernet) y un servidor de AAA (Autenticación, Autorización y Contabilización) se necesita para autenticar un abonado de acceso y asignar la dirección de IP. En condiciones normales, el servidor AAA puede ser un servidor RADIUS (Servicio de Usuario de Marcación de Autenticación Remota) u otros servidores de autenticación.

La Figura 1 representa una estructura de un sistema de comunicación de red en donde se realiza una autenticación por un servidor RADIUS y la dirección de IP se obtiene por intermedio de un servidor de protocolo DHCP.

El servidor de protocolo DHCP es un servidor para gestionar la dirección de IP y está adaptado para dar respuesta a una demanda de asignación de dirección procedente de un ordenador y para asignar una dirección de IP adecuada al ordenador.

El cliente de DHCP es un terminal adaptado para obtener parámetros de red tales como la dirección de IP utilizando un protocolo DHCP, que incluye un ordenador, STB e IAD.

El servidor RADIUS está adaptado para gestionar la cuenta y la contraseña de un abonado y para realizar una autenticación de un abonado de acceso.

El servidor BRAS (Servidor de Acceso Remoto de Banda Ancha) está adaptado para gestionar el acceso de un abonado de banda ancha; para un abonado de protocolo PPPoE, el servidor BRAS actúa como un cliente de RADIUS e inicia una demanda de autenticación al servidor de RADIUS y para un abonado de protocolo DHCP, el servidor BRAS pone en práctica la función de retransmisión de relé de DHCP.

La red de acceso es una red intermedia entre la vivienda del abonado y el servidor BRAS.

El nodo de acceso es un dispositivo que conecta con una línea de abonado directamente en una red de acceso, tal como un dispositivo de acceso ADSL del multiplexor DSLAM (Multiplexor de Acceso de Línea de Abonado Digital).

OSS (Sistemas de Soporte de Operaciones) es un sistema para que el operador libere y gestione un servicio.

En la Figura 1, un cliente de DHCP, tal como un STB e IAD se pueden asignar con una dirección de IP correspondiente utilizando el protocolo DHCP mediante un servidor de protocolo DHCP dispuesto en la red.

El proceso específico en el que cada cliente de DHCP, representado en la Figura 1, obtiene la dirección es como se representa en la Figura 2, incluyendo las etapas siguientes.

Etapa 21: Un cliente de DHCP se activa y envía un mensaje de descubrimiento de protocolo DHCP para la búsqueda de un servidor capaz de proporcionar el servicio de protocolo DHCP.

Etapa 22: Como un relé de DHCP, un servidor BRAS retransmite el mensaje de descubrimiento de protocolo DHCP al servidor de DHCP designado.

Etapa 23: El servidor DHCP reenvía un mensaje de oferta de protocolo DHCP para indicar que el servidor DHCP es capaz de asignar una dirección de IP al cliente.

Etapa 24: El cliente de DHCP envía un mensaje de demanda de DHCP y el servidor BRAS retransmite el mensaje de demanda de DHCP al servidor de DHCP.

Etapa 25: El servidor de DHCP asigna una dirección de IP adecuada y reenvía un mensaje de respuesta de protocolo DHCP.

Por lo tanto, el cliente de DHCP puede obtener la dirección de IP y de este modo, acceder a la red y obtener el servicio de la red.

Se puede deducir del anterior proceso de asignación de dirección de protocolo DHCP que: durante el proceso en el que el cliente de DHCP obtiene la dirección de IP en un modo de protocolo DHCP, un abonado no válido puede obtener fácilmente la correspondiente dirección de IP y de este modo, obtener el servicio de la red. Por lo tanto, el problema de que un *hacker* utilice, de forma malintencionada, los recursos de dirección de IP y ataque una red es fácil de que ocurra. Además, después de que el *hacker* ataque la red, no se podrá realizar su seguimiento.

Además, el operador necesita utilizar un servidor de DHCP para gestionar la dirección de IP del usuario del cliente de DHCP y utilizar un servidor RADIUS para gestionar la dirección de IP del usuario del cliente de protocolo PPPoE. En consecuencia, existen dos conjuntos de mecanismos de gestión de recursos de direcciones de IP, los datos están descentralizados y el coste de la gestión es alto.

Además, el documento WO 99/16266 A da a conocer los contenidos siguientes. Las aplicaciones que se ejecutan en una estación móvil o en una entidad de red externa, tal como un proveedor de servicios de Internet, puede especificar, sobre una base de flujo de aplicación individual, una calidad de servicio demandada. A partir de esa calidad de servicio demandada, se determina un tipo óptimo de portador para transferir el flujo de aplicación a través de la red de comunicaciones móviles. Por ejemplo, un portador de circuitos conmutados se puede asignar si la demanda es para un servicio en tiempo real y un portador de paquetes conmutados se puede asignar si la demanda es para un tipo de servicio no en tiempo real. Se pueden utilizar otros varios criterios para la toma de decisiones. Una estación móvil y un nodo de pasarela de red móvil incluyen, cada uno, un dispositivo de mapeado para establecer una correspondencia mapeada de un flujo de aplicación individual con uno de una red de circuitos conmutados y un portador de red de paquetes conmutados, que depende de la calidad de servicio demandada para el flujo de aplicación individual. Los parámetros de la calidad de servicio de la capa de red, que corresponden a un flujo de aplicación individual, son objeto de mapeado para los parámetros de portador de circuitos conmutados si el flujo de aplicación es mapeado para la red de circuitos conmutados y para los parámetros del portador de paquetes conmutados si el flujo de aplicación es objeto de mapeado para la red de paquetes conmutados. El nodo de pasarela incluye un servidor de acceso común, que permite a una estación móvil establecer inicialmente una sesión de comunicación con una entidad de red externa para realizar solamente un procedimiento de acceso común único para posteriores comunicaciones utilizando una de las redes de circuitos conmutados y de paquetes conmutados. Una vez concluido dicho procedimiento de acceso común, se establecen flujos de aplicación posteriores entre la estación móvil y la entidad de red externa utilizando procedimientos abreviados sin tener que acceder a la entidad de red externa.

Además, el documento IETF STANDARD “Opción de información de agente de retransmisión DHCP; rfc 3046.txt” da a conocer contenidos técnicos en relación con el agente de retransmisión de DHCP.

Además, una solicitud de patente (WO/2004/006503) da a conocer una disposición y un método con configuración dinámica de puertos de equipos de red para comunicación en una red de banda ancha. Una base de datos de gestión central en conexión con un servidor de Protocolo de Configuración Dinámica de Concentrador está manteniendo plantillas modelo con registros de parámetros de equipos de redes para sus configuraciones de puertos físicos y servicios desplegados. En consecuencia, se habilita la actualización dinámica de las configuraciones de puertos transmitiendo registros de parámetros desde el servidor de protocolo de configuración dinámica de concentrador. Los ajustes de parámetros se actualizan en el medio intermedio. Sin embargo, en la solución técnica de D3, puesto que la base de datos está situada fuera del servidor de protocolo DHCP, el coste de la gestión de datos es alto y la seguridad para la transmisión de datos es baja.

SUMARIO DE LA INVENCIÓN

Considerando los problemas antes citados en la técnica anterior, un objetivo de la presente invención es dar a conocer un método, un sistema y un servidor para realizar una asignación segura de una dirección de protocolo DHCP. Y, por lo tanto, la seguridad del proceso de asignación de dirección del servidor de DHCP se puede garantizar efectivamente y el coste de la gestión de datos es bajo.

El objetivo de la presente invención se realiza mediante las siguientes soluciones técnicas.

Un método para realizar una asignación segura de una dirección de protocolo DHCP, que comprende:

la recepción, por un servidor de acceso, de un mensaje de descubrimiento de protocolo DHCP;

la inserción, por el servidor de acceso, de información de localización del cliente de DHCP en el mensaje de descubrimiento de protocolo DHCP;

el envío, por el servidor de acceso, del mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP a un servidor de autenticación de protocolo DHCP;

la recepción, por el servidor de autenticación de protocolo DHCP, del mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP, en donde el servidor de autenticación de protocolo DHCP es un servidor DHCP que tiene una función de autenticación configurada a nivel local, comprendiendo el servidor de autenticación de protocolo DHCP una base de datos local que comprende información de identificación memorizada para un abonado válido a nivel local;

la realización de una autenticación del cliente de DHCP en función de la información de localización y de la información de identificación memorizadas para el abonado válido a nivel local por el servidor de autenticación de protocolo DHCP y

el envío, por el servidor de autenticación de protocolo DHCP, de un mensaje de protocolo DHCP con información de dirección que se asigna al cliente de DHCP que ha tenido éxito operativo en la autenticación por intermedio del servidor de acceso, después de que se haya realizado la autenticación del cliente de DHCP.

Un servidor de autenticación de protocolo DHCP para realizar una asignación segura de una dirección de DHCP, teniendo el servidor de autenticación de protocolo DHCP una función de autenticación configurada a nivel local y comprendiendo un módulo de procesamiento de autenticación, un servidor DHCP para asignar una dirección de IP a un cliente de DHCP que demanda una dirección de IP y una base de datos local que comprende información de identificación memorizada para un abonado válido a nivel local, en donde:

el módulo de procesamiento de autenticación está adaptado para obtener información de localización de un cliente que inicia un proceso de protocolo DHCP, para realizar una autenticación de validez del cliente en función de la información de localización y de la información de identificación memorizadas para el abonado válido y para enviar un mensaje de descubrimiento de protocolo DHCP de un cliente de DHCP que ha tenido éxito operativo en la autenticación de validez al servidor DHCP y

el servidor DHCP está adaptado para recibir el mensaje de descubrimiento de protocolo DHCP enviado por el módulo de procesamiento de autenticación y para enviar un mensaje de oferta de protocolo DHCP al cliente de DHCP y para asignar una dirección de IP a un cliente de DHCP correspondiente en un conjunto de direcciones del servidor de DHCP cuando el cliente de DHCP envía un mensaje de demanda de protocolo DHCP.

Un sistema para realizar una asignación segura de una dirección de DHCP, que comprende un servidor de acceso y un servidor de autenticación de protocolo DHCP, en donde

el servidor de acceso está adaptado para recibir el mensaje de descubrimiento de protocolo DHCP enviado desde el cliente de DHCP, para insertar información de localización del cliente de DHCP en el mensaje de descubrimiento de protocolo DHCP y para enviar el mensaje de descubrimiento de DHCP, con la información de localización, al servidor de autenticación de protocolo DHCP y

el servidor de autenticación de protocolo DHCP tiene una función de autenticación configurada a nivel local y está adaptado para recibir el mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP y para realizar una autenticación del cliente de DHCP en función de la información de localización y de la información de identificación memorizadas para un abonado válido a nivel local y para enviar un mensaje de protocolo DHCP con la información de dirección que es asignada al cliente de DHCP que ha tenido éxito operativo en la autenticación por intermedio del servidor de acceso.

Además, en la presente invención, se pueden gestionar direcciones por un servidor RADIUS de forma unificada; dicho de otro modo, el servidor de DHCP y el servidor RADIUS gestionan, de forma unificada, las direcciones de IP, con lo que se puede reducir el coste de la gestión de la red. Además, las medidas de seguridad originales del servidor RADIUS se pueden utilizar para controlar el número de direcciones de IP a obtenerse por un abonado, de modo que el ataque de quienes utilizan direcciones de forma malintencionada se puede evitar de forma eficiente. Aún cuando se produzca el ataque a la red u otros problemas de seguridad de la red, la localización física del abonado puede ser objeto de seguimiento según la dirección de IP, de modo que un *hacker* pueda disuadirse efectivamente de realizar una actividad de ataque.

La presente invención presenta una buena compatibilidad; dicho de otro modo, durante la puesta en práctica de la presente invención, no se añade ninguna interfaz ni orden extraordinaria al sistema OSS y el proceso de gestión del servicio en el usuario del cliente de DHCP es compatible con el proceso de gestión de liberación del servicio original en el cliente de protocolo PPPoE. Como resultado, se puede proteger la inversión del operador.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es una representación estructural de un sistema de acceso de banda ancha;

La Figura 2 es un diagrama esquemático que muestra un proceso en el que un servidor de protocolo DHCP obtiene una dirección;

La Figura 3 es una representación estructural del servidor de autenticación de protocolo DHCP según la presente invención;

La Figura 4 es otro sistema de representación estructural según la presente invención y

La Figura 5 es un diagrama esquemático de un proceso de asignación de dirección de protocolo DHCP basándose en el sistema representado en la Figura 4.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

El concepto principal de la presente invención reside en que: durante el proceso en el que un cliente de DHCP obtiene una dirección desde un servidor de DHCP, se añade un proceso de autenticación de la validez en el cliente de DHCP, de modo que pueda evitarse que un abonado no válido ataque al servidor de protocolo DHCP. Además, basándose en el concepto anterior, la gestión de direcciones del servidor de DHCP y el servidor de autenticación pueden estar operativamente unificados, de modo que sea fácil realizar la gestión de las direcciones. El servidor de autenticación incluye un servidor AAA tal como un servidor RADIUS. De forma opcional, el servidor de autenticación puede ser otros servidores de autenticación con la función similar.

Una forma de realización de la presente invención da a conocer un método para realizar una asignación segura de una dirección de DHCP, incluyendo principalmente lo siguiente.

(1) Un cliente de DHCP envía un mensaje de descubrimiento de protocolo DHCP a través de una red de acceso.

(2) El servidor de acceso en el lado de la red (tal como un servidor BRAS y un nodo de acceso) determina la información de identificación del cliente de DHCP, tal como el número de puerto, VPI (identificadores de ruta virtual) / VCI (identificadores de canal virtual) y VLAN ID (identificador de red de área local virtual) en función de la información del puerto de entrada del mensaje de descubrimiento de protocolo DHCP y realiza una autenticación del cliente de DHCP en función de la información de identificación del cliente de DHCP y de la información de identificación preconfigurada para un abonado válido.

(3) El mensaje de descubrimiento de protocolo DHCP del cliente de DHCP que ha tenido éxito operativo en la autenticación se envía al servidor de DHCP y la dirección se asigna al cliente de DHCP por intermedio del servidor de DHCP. El proceso de asignación de dirección específico es el mismo que un proceso de asignación de dirección convencional y se omite la repetición de su descripción.

Además, un servidor de DHCP correspondiente, con una función de autenticación, se puede configurar en la red, de modo que el servidor de DHCP pueda realizar primero un proceso de autenticación después de recibir un mensaje de descubrimiento de protocolo DHCP enviado desde un cliente de DHCP y la dirección correspondiente solamente se asignará después de que tenga éxito operativo la autenticación.

La presente invención da a conocer un servidor de autenticación de protocolo DHCP con la función de autenticación. Descripciones del servidor de autenticación de protocolo DHCP se ilustrarán ahora haciendo referencia a los dibujos respectivos.

Para el servidor de autenticación de protocolo DHCP con la función de autenticación, la función de autenticación está configurada y puesta en práctica al nivel local. La estructura específica del servidor de autenticación de protocolo DHCP es según se representa en la Figura 3, incluyendo un módulo de procesamiento de autenticación y un módulo de servidor DHCP.

El módulo de procesamiento de autenticación está adaptado para obtener la información de identificación del cliente de DHCP durante la iniciación del proceso de DHCP, para realizar una autenticación de la validez del cliente en función de la información de identificación memorizada para abonados válidos y luego, para enviar un resultado de la autenticación al módulo del servidor de DHCP, en donde la información de identificación del abonado válido es memorizada en un módulo de almacenamiento correspondiente (no ilustrado).

El módulo del servidor de DHCP está adaptado para obtener el resultado de la autenticación en el cliente DHCP a partir del módulo de procesamiento de la autenticación, para enviar un mensaje de oferta de protocolo DHCP al cliente DHCP con el resultado de autenticación de éxito operativo (PASSED) para indicar que el servidor de DHCP pueda asignar una dirección de IP correspondiente al cliente de DHCP y luego, para asignar la dirección de IP correspondiente al cliente de

DHCP después de que el cliente de DHCP envíe un mensaje de demanda de DHCP. De este modo, se pone en práctica la función del servidor de DHCP.

En este punto operativo, el servidor de autenticación de protocolo DHCP funciona en un modo de servidor, está en correspondencia con un servidor de DHCP con una función de autenticación segura y puede poner en práctica la autenticación y la asignación de dirección para un cliente de forma independiente.

El servidor de autenticación de protocolo DHCP anterior, con la función de autenticación, puede configurarse en cualquier red, con necesidad de un servidor de DHCP, para realizar la correspondiente función de asignación de dirección.

La presente invención da a conocer, además, un sistema correspondiente con una función de autenticación y asignación de dirección de protocolo DHCP para realizar una asignación segura de una dirección de DHCP. La estructura del sistema se representa en la Figura 4, incluyendo concretamente un cliente de DHCP, una red de acceso y un servidor de autenticación de DHCP. El servidor de autenticación de DHCP está adaptado para realizar una autenticación de validez de un mensaje de descubrimiento de protocolo DHCP del cliente de DHCP obtenido por la red de acceso y para realizar una asignación de dirección al cliente de DHCP que ha tenido éxito operativo en la autenticación.

En el sistema según la presente invención, el servidor de autenticación de protocolo DHCP puede realizar la autenticación del cliente de DHCP y asignar una dirección de IP correspondiente en el modo siguiente.

Según se ilustra en la Figura 5, la autenticación de validez se realiza sobre la información de identificación del cliente de DHCP en función de la información de identificación del abonado válido memorizada a nivel local y el servidor de DHCP puede asignar la dirección de IP correspondiente al cliente de DHCP que ha tenido éxito operativo en la autenticación.

Más concretamente, en el sistema, el nodo de acceso y el servidor BRAS soportan la captura de un mensaje de protocolo DHCP e insertan una opción 82 en el en el mensaje DHCP, de modo que el servidor de autenticación de protocolo DHCP pueda obtener la información de identificación correspondiente del cliente de DHCP después de recibir el mensaje de protocolo DHCP. En la opción 82, la información de localización del abonado, que actúa como la información de identificación, es objeto de identificación. Más concretamente, la información de localización del abonado incluye información del puerto, información de VPI/VCI y el identificador de red VLAN. La opción 82 se puede insertar en el mensaje de DHCP en el nodo de acceso o la opción 82 se puede insertar en el mensaje de DHCP en el servidor BRAS.

La presente invención da a conocer, además, un método correspondiente para realizar una asignación segura de una dirección de DHCP basándose en el sistema anterior. Una descripción detallada se ilustrará ahora a continuación.

Por ejemplo, el método se describe en el caso de que el servidor de autenticación de protocolo DHCP funcione en un modo de servidor, según se ilustra en la Figura 4 y en la Figura 5.

Etapa 91: Cuando un abonado abre una cuenta, el operador añade un elemento de datos a un servidor de autenticación de protocolo DHCP y registra la información de localización del abonado, siendo el modo de codificación compatible con la opción 82 insertada por el nodo de acceso o el servidor BRAS y la dirección de MAC de un terminal (STB, IAD) se puede registrar de forma selectiva.

Etapa 92: Cuando un cliente de DHCP necesita obtener la dirección de IP, el cliente de DHCP necesita enviar un mensaje de descubrimiento de protocolo DHCP al servidor BRAS.

Etapa 93: Como un relé de DHCP, el servidor BRAS captura el mensaje de protocolo DHCP e inserta la opción 82 en el mensaje y luego, envía el mensaje de descubrimiento de protocolo DHCP que transmite la información de localización del abonado al servidor de autenticación de protocolo DHCP. La información de localización del abonado, tal como información del puerto, VPI/VCI y el identificador de red VLAN, se identifica en la opción 82.

El servidor de autenticación de protocolo DHCP recibe el mensaje de DHCP retransmitido por el servidor BRAS, extrae la opción 82 y la dirección de MAC del terminal como la información de identificación, consulta una base de datos local y realiza una autenticación de la información de identificación del cliente de DHCP en función de la información de identificación memorizada para un abonado válido a nivel local. Si la autenticación se realiza con éxito operativo, el servidor de autenticación de protocolo DHCP reenvía un mensaje de oferta de protocolo DHCP al cliente de DHCP, según se describe en la etapa 94.

Etapa 94: El servidor de autenticación de protocolo DHCP envía un mensaje de oferta de protocolo DHCP al cliente de DHCP.

Etapa 95: Después de recibir el mensaje de oferta de protocolo DHCP, el cliente de DHCP envía un mensaje de demanda de DHCP al servidor de autenticación de protocolo DHCP.

Etapa 96: El servidor de autenticación de protocolo DHCP asigna la dirección de IP al cliente de DHCP y envía la dirección de IP al cliente de DHCP por intermedio de un mensaje de respuesta de protocolo DHCP.

De forma similar, según se describe en la etapa 93 de la Figura 5, el servidor BRAS inserta la opción 82. En la aplicación práctica, la opción 82 se puede insertar también por un nodo de acceso tal como DSLAM, mientras el servidor BRAS solamente actúa como el relé de DHCP. Otros procesos son los mismos que los anteriormente descritos.

En conclusión, la presente invención puede mejorar la seguridad de la asignación de dirección en el modo DHCP en gran medida y puede realizar una autenticación del acceso de un abonado en función de la información de localización y sólo puede asignar una dirección de IP a un abonado válido o un terminal válido. Por lo tanto, el ataque de un usuario de dirección malintencionada se puede evitar de forma efectiva. Además, cuando ocurra el ataque de la red u otro problema de seguridad de la red, la localización física del abonado puede ser objeto de seguimiento según la dirección de IP, de modo que un hacker pueda disuadirse efectivamente de realizar una actividad de ataque.

Otras ventajas y modificaciones adicionales serán evidentes para los expertos en esta materia. Por lo tanto, la presente invención, en sus aspectos de la idea inventiva más amplios, no está limitada a los detalles concretos y modos de realización representativos mostrados e ilustrados en la presente descripción. En consecuencia, se pueden realizar diversas modificaciones y variaciones sin desviarse, por ello, del alcance de protección de la presente invención, según se define por las reivindicaciones adjuntas y sus equivalentes.

REIVINDICACIONES

1. Un método para realizar una asignación segura de una dirección de protocolo DHCP, que comprende:

la recepción, por un servidor de acceso, de un mensaje de descubrimiento en el protocolo DHCP (91);

la inserción, por el servidor de acceso, de información de localización del cliente de DHCP en el mensaje de descubrimiento de protocolo DHCP (93);

el envío, por el servidor de acceso, del mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP a un servidor de autenticación de protocolo DHCP (93);

la recepción, por el servidor de autenticación de protocolo DHCP, del mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP (93);

caracterizado porque:

el servidor de autenticación de protocolo DHCP es un servidor de protocolo DHCP que tiene una función de autenticación configurada localmente, comprendiendo el servidor de autenticación de protocolo DHCP una base de datos local que comprende información de identificación memorizada para un abonado válido a nivel local;

en donde el método comprende, además:

la realización, por el servidor de autenticación de protocolo DHCP, de una autenticación del cliente de DHCP en función de la información de localización y de la información de identificación memorizadas para el abonado válido a nivel local y

el envío, por el servidor de autenticación de protocolo DHCP, de un mensaje de protocolo DHCP con información de dirección que se asigna al cliente de DHCP que ha transmitido la autenticación a través del servidor de acceso, después de que haya tenido éxito operativo la autenticación del cliente del servidor DHCP (96).

2. El método para realizar la asignación segura de la dirección de protocolo DHCP, según la reivindicación 1, en donde la información de localización comprende:

un número de puerto, un número de circuito y un número de conexión del cliente de DHCP.

3. El método para realizar la asignación segura de la dirección de protocolo DHCP según la reivindicación 1 o 2, en donde, la recepción del mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP por el servidor de autenticación de protocolo de DHCP y la realización de la autenticación del cliente de DHCP en función de la información de localización y de la información de identificación memorizadas para el abonado válido, a nivel local, por el servidor de autenticación de protocolo DHCP, comprende:

la recepción, por el servidor de autenticación de protocolo DHCP, del mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP y la realización de una autenticación de validez del cliente de DHCP en función de la información de localización y de la información de identificación memorizadas para el abonado válido al nivel local.

4. El método para realizar la asignación segura de la dirección de protocolo DHCP según la reivindicación 3 que comprende, además:

la asignación, por el servidor de autenticación de protocolo DHCP, de la información de dirección al cliente de DHCP que ha realizado la autenticación después de recibir la información del éxito operativo de la autenticación.

5. Un servidor de autenticación de protocolo DHCP para realizar una asignación segura de una dirección de protocolo DHCP, que comprende un servidor de protocolo DHCP para asignar una dirección de IP a un cliente de DHCP, que solicita una dirección de IP, caracterizado porque:

el servidor de autenticación de protocolo DHCP tiene una función de autenticación configurada a nivel local y el servidor de autenticación de protocolo DHCP comprende, además: un módulo de procesamiento de la autenticación y una base de datos local que comprende información de identificación memorizada para un abonado válido al nivel local, en donde:

el módulo de procesamiento de la autenticación está adaptado para obtener información de localización de un cliente que inicia un proceso de protocolo DHCP, para realizar una autenticación de validez del cliente en función de la información de localización y de la información de identificación memorizadas para el abonado válido y para enviar un mensaje de descubrimiento de protocolo DHCP de un cliente de DHCP que ha tenido éxito operativo en la autenticación de validez para el servidor de protocolo DHCP y

el servidor de protocolo DHCP está adaptado para recibir el mensaje de descubrimiento de protocolo DHCP enviado por el módulo de procesamiento de autenticación y para enviar un mensaje de oferta de protocolo DHCP al cliente de DHCP y para asignar una dirección de IP a un cliente de DHCP correspondiente en un conjunto de direcciones del servidor de protocolo DHCP cuando el cliente de DHCP envía un mensaje de demanda de protocolo DHCP.

6. El servidor de autenticación de protocolo DHCP, según la reivindicación 5, en donde la información de localización comprende:

un número de puerto, un número de circuito y un número de conexión del cliente de DHCP.

7. Un sistema para realizar una asignación segura de una dirección de protocolo DHCP, que comprende un servidor de acceso y un servidor de autenticación de protocolo DHCP, en donde:

el servidor de acceso está adaptado para recibir el mensaje de descubrimiento de protocolo DHCP enviado desde el cliente de DHCP, para insertar la información de localización del cliente de DHCP en el mensaje de descubrimiento de protocolo DHCP y para enviar el mensaje de descubrimiento de DHCP con la información de localización al servidor de autenticación de protocolo DHCP;

caracterizado porque:

el servidor de autenticación de protocolo DHCP tiene una función de autenticación configurada a nivel local y está adaptado para recibir el mensaje de descubrimiento de protocolo DHCP con la información de localización del cliente de DHCP y para realizar una autenticación del cliente de DHCP en función de la información de localización y de la información de identificación memorizadas para un abonado válido a nivel local y para enviar un mensaje de protocolo DHCP con la información de dirección que se asigna al cliente de DHCP que ha tenido éxito operativo en la autenticación por intermedio del servidor de acceso.

8. El sistema según la reivindicación 7, en donde el servidor de autenticación de DHCP es el servidor de autenticación de protocolo DHCP según se establece en la reivindicación 5.

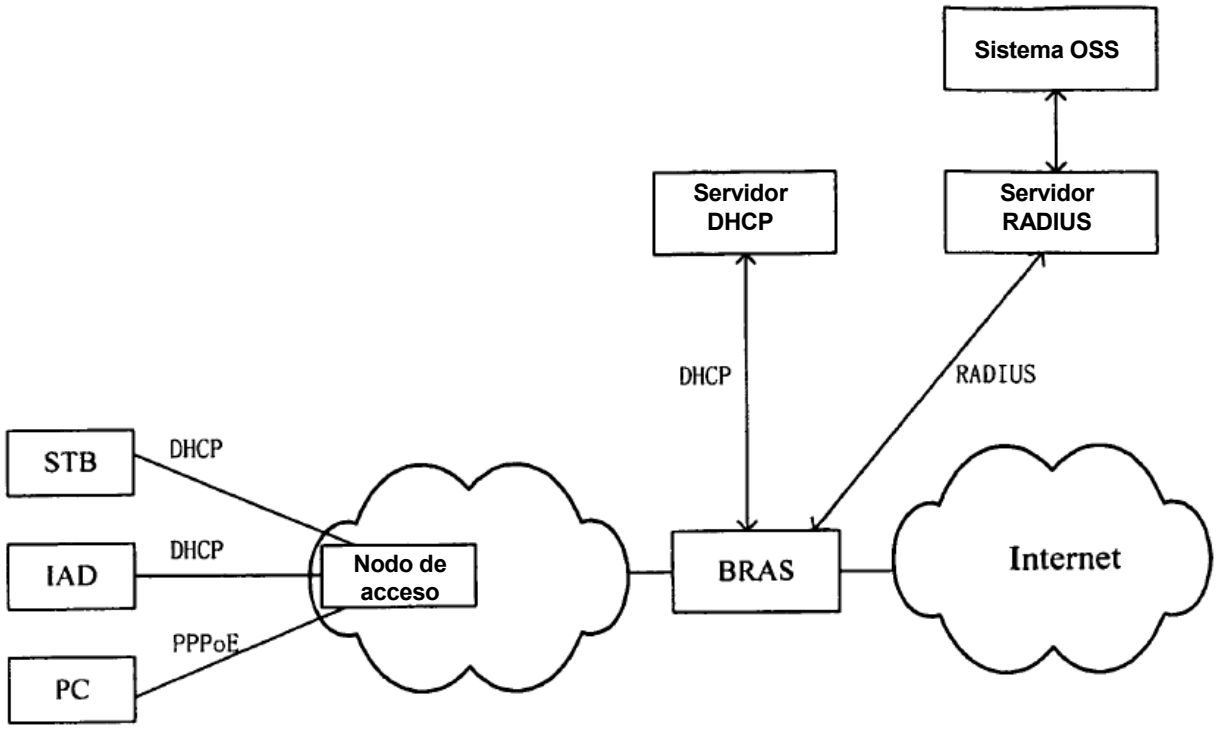

Figura 1

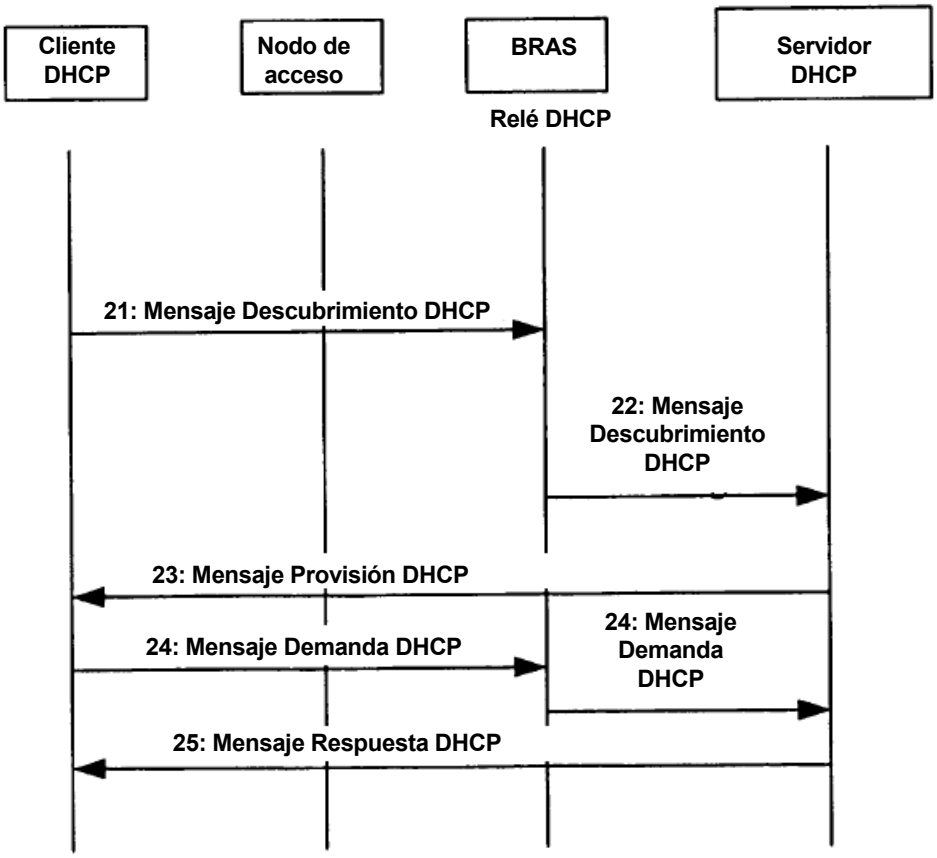

Figura 2

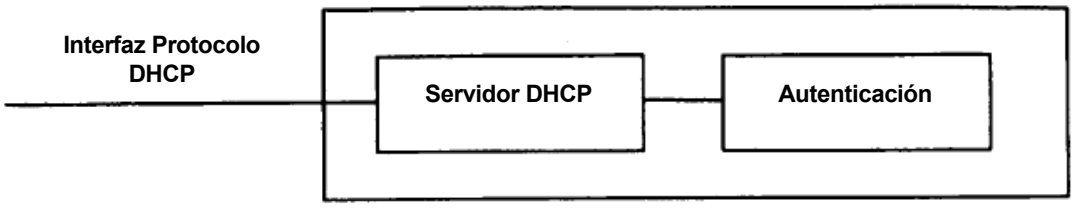

Figura 3

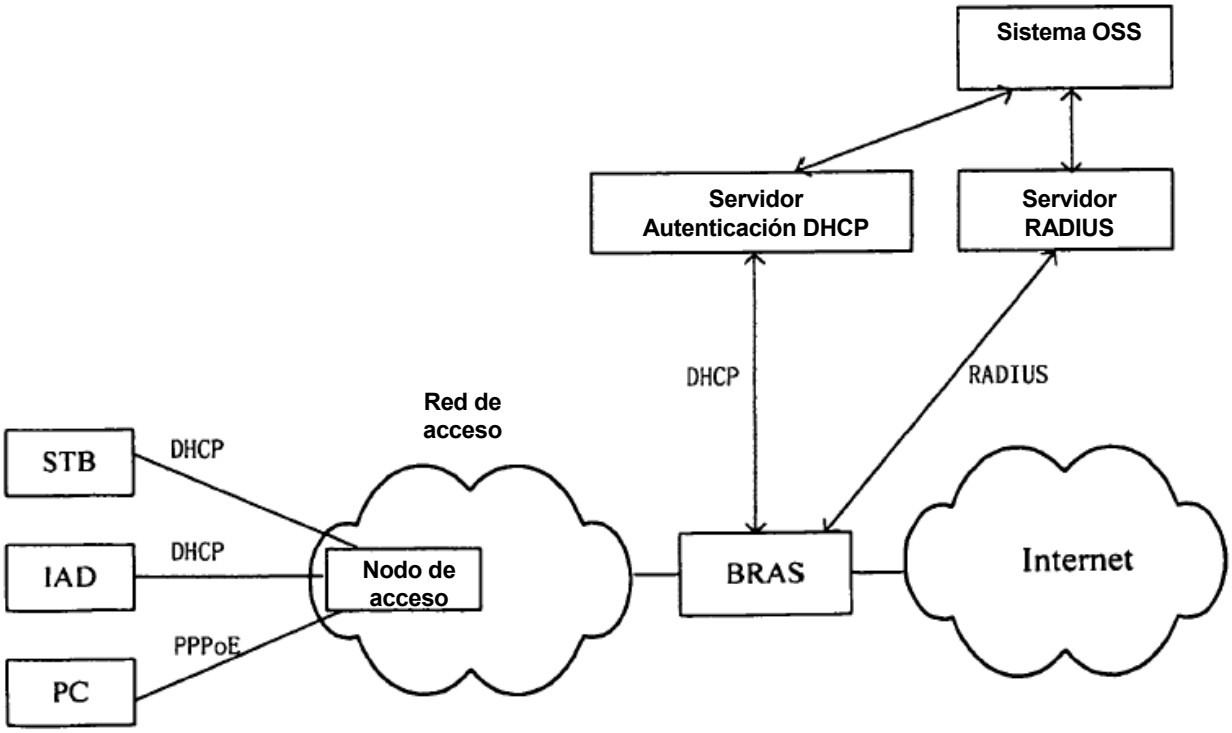

Figura 4

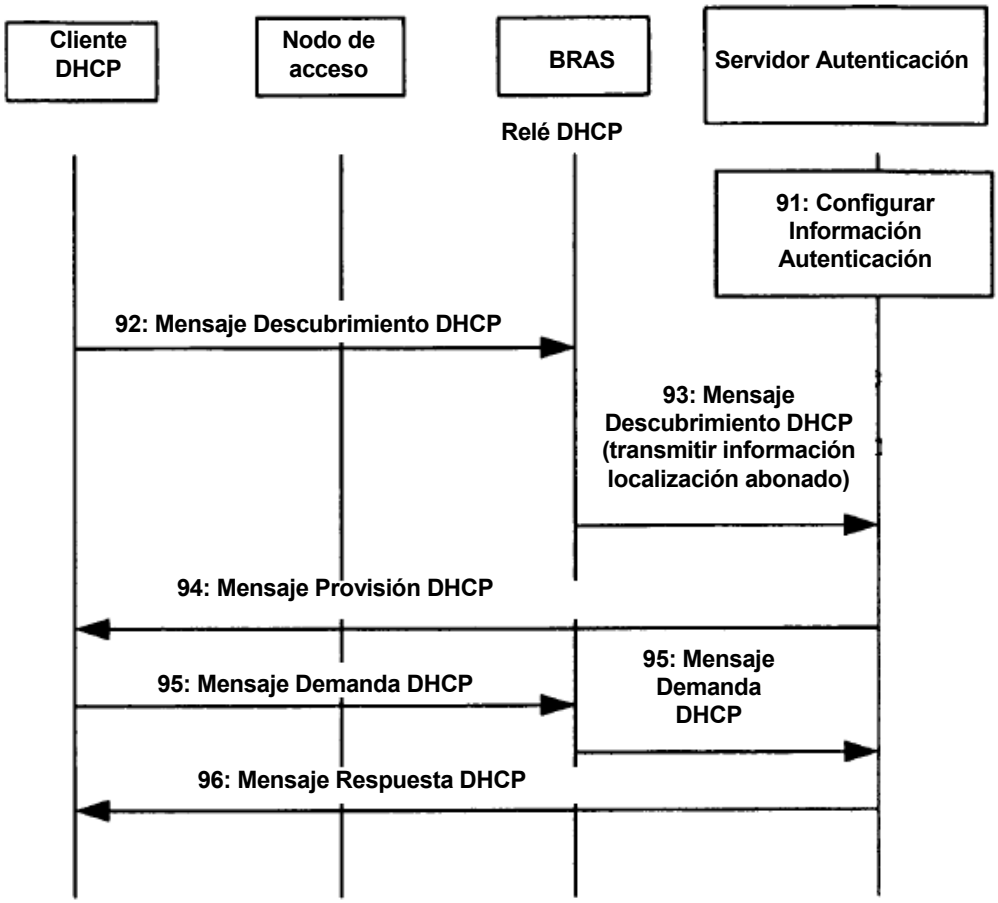
Cliente DHCP
Nodo de acceso
BRAS
Servidor Autenticación
Relé DHCP
91: Configurar Información Autenticación
92: Mensaje Descubrimiento DHCP
93: Mensaje Descubrimiento DHCP (transmitir información localización abonado)
94: Mensaje Provisión DHCP
95: Mensaje Demanda DHCP
95: Mensaje Demanda DHCP
96: Mensaje Respuesta DHCP

Figura 5