(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 407 258**

(51) Int. CI.:

H04L 29/12 (2006.01)
H04L 29/06 (2006.01)
H04W 12/10 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.04.2007 E 07007443 (0)**

(97) Fecha y número de publicación de la concesión europea: **09.01.2013 EP 1914960**

(54) Título: **Método para la transmisión de mensajes de DHCP**

(30) Prioridad:

16.10.2006 EP 06021659

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.06.2013

(73) Titular/es:

NOKIA SIEMENS NETWORKS GMBH & CO. KG (100.0%)
St. Martinstrasse 76
81541 München , DE

(72) Inventor/es:

PREMEC, DOMAGOJ y
RIEGEL, MAXIMILIAN

(74) Agente/Representante:

ZUAZO ARALUZE, Alexander

DESCRIPCIÓN

Método para la transmisión de mensajes de DHCP.

La invención se refiere a un método para la transmisión de un mensaje de DHCP entre una red de telecomunicaciones, especialmente a una red de telecomunicaciones según la norma WiMAX, y un abonado de protocolo de Internet (IP) de la red de telecomunicaciones.

En la siguiente descripción, se hace referencia a una red de telecomunicaciones WiMAX para explicar el problema que subyace a la presente invención. Esta referencia a una red de telecomunicaciones WiMAX es sólo un ejemplo. De hecho, la invención se refiere a cualquier clase de red de telecomunicaciones.

La red WiMAX consiste en una red de servicio de conectividad (CSN) de WiMAX que es comparable a una red central y una red de servicio de acceso (ASN) de WiMAX que desempeña el papel de una red de acceso inalámbrica. La ASN y la CSN pueden operarse por entidades comerciales u operadores diferentes. La arquitectura global de una red WiMAX se muestra en la figura 1 que representa un modelo de referencia de la red WiMAX. Puede encontrarse una descripción detallada del modelo de referencia de red en www.wimaxforum.org/technology/documents/ en la especificación “WiMAX end-to-end network systems architecture”, capítulo 6, “Network Reference Model”.

La CSN siempre contiene un agente doméstico de un abonado de WiMAX. El agente doméstico no puede estar ubicado en la ASN. El agente doméstico tiene la tarea de defender la dirección doméstica del abonado en su red doméstica (CSN) mientras el abonado está fuera de casa. Esto significa que la dirección doméstica del abonado es topológicamente correcta en la subred en la que está ubicado el agente doméstico, y como tal la dirección doméstica debe asignarse por el dominio de CSN. La red doméstica del abonado de WiMAX puede asignarse de manera dinámica y puede estar o bien en una CSN doméstica (H-CSN) o una CSN visitada (V-CSN) dependiendo de un acuerdo de itinerancia entre el proveedor de servicios de red (NSP) WiMAX doméstico y visitado.

Una característica de la arquitectura de red WiMAX es el soporte de denominados terminales de “protocolo de Internet (IP) simple” como abonado que no contienen una implementación de un pila de IP móvil. La movilidad en la capa (IP) de red para estos dispositivos se gestiona por la ASN por medio de un IP móvil proxy.

Los terminales de IP simple usan DHCP para adquirir una dirección IP y otros parámetros de configuración de IP. La dirección IP para el terminal de IP simple se asigna por la CSN (o bien H-CSN o bien V-CSN) pero la asignación de esta dirección al terminal se realiza por la red de acceso ASN. Para la asignación de esta dirección debe estar previsto un retransmisor de DHCP en la ASN. En contraposición a esto, un servidor de DHCP está ubicado en la CSN, y el retransmisor de DHCP en la ASN retransmite mensajes de DHCP desde el terminal de IP simple al servidor de DHCP en la CSN. En este escenario, durante la autenticación de abonado la CSN proporciona a la ASN la dirección IP del servidor de DHCP en la CSN. Esta dirección se usa posteriormente por el retransmisor de DHCP en la ASN para retransmitir los mensajes de DHCP desde el terminal al servidor de DHCP correcto. El servidor de DHCP puede estar ubicado o bien en la V-CSN o bien en la H-CSN. En esos casos, se supone que la ASN y la CSN pueden estar separadas por una nube IP desconocida, por ejemplo Internet público. Haciendo referencia a la figura 1, los puntos de referencia R3 y R5 pueden discurrir a través de una infraestructura de IP no confiable de este tipo.

Debido a esta topología de la red de telecomunicaciones, el servidor de DHCP en la CSN es vulnerable a diversos tipos de ataques. Los ataques pueden originarse tanto de la red no confiable que conecta la ASN y la CSN así como de abonados de WiMax autenticados pero que no se comportan correctamente. Estos ataques pueden evitarse si el retransmisor de DHCP en la ASN y el servidor de DHCP en la CSN implementan una subopción de autenticación de agente de retransmisión tal como se define en RFC 4030 (http://rfc.net/rfc4030.html). Los métodos definidos en RFC 4030 proporcionan una autenticación, protección de integridad y protección de reproducción de mensajes de DHCP. De ese modo, se supone que el retransmisor de DHCP y el servidor de DHCP comparten una clave secreta que se usa para calcular la suma de comprobación criptográfica que proporciona la protección mencionada anteriormente.

El borrador de Internet “Bootstrapping RFC3118 delayed DHCP authentication using EAP-based Network Access Authentication” (www.ietf.org) de febrero de 2006 proporciona un método de cómo generar y distribuir una clave compartida usando un procedimiento de autenticación de acceso basado en EAP.

Por tanto, un objeto de la presente invención es mejorar la seguridad cuando se intercambian mensajes de DHCP entre una red de telecomunicaciones y un abonado de IP.

Este objeto se resuelve mediante la invención según las reivindicaciones independientes. Realizaciones preferidas se definen mediante las reivindicaciones dependientes.

Según el ejemplo, se proporciona un método para la transmisión de un mensaje de DHCP entre un servidor de DHCP de una red de telecomunicaciones, especialmente una red de telecomunicaciones según la norma WiMAX, y un abonado de protocolo de Internet (IP) conectado a la red de telecomunicaciones, en el que se añade una

información protegida con una clave de cifrado al mensaje de DHCP por el servidor de DHCP o por un retransmisor de DHCP ubicado entre el dispositivo de abonado de protocolo de Internet y el servidor de DHCP que retransmite el mensaje de DHCP desde el dispositivo de abonado de protocolo de Internet (IP) al servidor de DHCP, y en el que la clave de cifrado se deriva de una clave básica que se proporciona por un servidor adicional de la red de telecomunicaciones y en el que la clave básica es una clave específica para el servidor de DHCP.

Según un ejemplo adicional, se proporciona un componente de red de telecomunicaciones para la transmisión de un mensaje de DHCP entre un servidor de DHCP de una red de telecomunicaciones y un dispositivo de abonado de protocolo de Internet (IP) conectado a la red de telecomunicaciones, en el que se añade una información protegida con una clave de cifrado por el componente de red de telecomunicaciones al mensaje de DHCP recibido desde el dispositivo de abonado de protocolo de Internet (IP), en el que la clave de cifrado se deriva por el componente de telecomunicaciones a partir de una clave básica que se proporciona por un servidor adicional de la red de telecomunicaciones y en el que la clave básica es una clave específica para el servidor de DHCP.

Protegiendo cierta información con una clave de cifrado que se deriva de una clave básica, puede proporcionarse máxima seguridad frente a un uso incorrecto. La clave de cifrado sólo se usa para proteger una información que se añade al mensaje de DHCP pero no el propio mensaje de DHCP. Esto significa que la clave de cifrado se usa para firmar digitalmente el mensaje. Sólo una entidad en posesión de la clave de cifrado puede calcular la firma, verificando de ese modo la autenticidad del mensaje. La entidad de envío calcula la firma de mensaje (usando la clave de cifrado como parte del cálculo) y añade la firma al mensaje. La entidad de recepción (también en posesión de la clave de cifrado) calcula por su parte de nuevo la firma y compara el resultado con la firma recibida en el mensaje. Si coinciden, la entidad de recepción puede garantizar que el mensaje recibido se firmó por la entidad en posesión de la clave de cifrado (y que el mensaje no se ha alterado en el trayecto). Las claves de cifrado pueden derivarse de manera dinámica de la clave básica para proteger los mensajes de DHCP.

Según un ejemplo adicional, se usa la clave de cifrado para proteger los mensajes de DHCP intercambiados entre un servidor de DHCP y un retransmisor de DHCP, que están ubicados opcionalmente en redes (subredes) diferentes de la red de telecomunicaciones. El servidor de DHCP puede estar ubicado en una red central, tal como la CSN, mientras que el retransmisor de DHCP puede estar ubicado en una red de acceso, tal como la ASN en la red de telecomunicaciones WiMAX. Debido al uso de la clave de cifrado para proteger los mensajes de DHCP intercambiados entre el servidor de DHCP y el retransmisor de DHCP, los mensajes pueden transferirse a través de una infraestructura de IP no confiable sin el peligro de que el servidor de DHCP pueda ser objeto de ataques.

Según un ejemplo adicional, el mensaje de DHCP generado por el abonado se intercepta por la red de telecomunicaciones, añadiéndose la información cifrada con la clave de cifrado cuando el mensaje de DHCP cumple con las comprobaciones de seguridad y/o credibilidad. El retransmisor de DHCP puede realizar la intercepción y comprobación del mensaje de DHCP. La intercepción y comprobación incluyen el tráfico de unidifusión dirigido al servidor de DHCP. De ese modo, puede realizarse una verificación del contenido de cada mensaje de DHCP. En caso de que el mensaje de DHCP pase las diversas comprobaciones de seguridad y/o credibilidad con respecto a suplantación de identidad (*spoofing*), ataques de DoS, etc., se añadirá la información cifrada con la clave de cifrado al mensaje, garantizando de ese modo a la red de telecomunicaciones, especialmente al servidor de DHCP, que se trata de un mensaje de DHCP legítimo.

Según un ejemplo adicional, la clave básica puede generarse usando un valor aleatorio generado. El valor aleatorio puede generarse por un servidor de AAA en una red doméstica del abonado. El servidor de AAA puede estar ubicado en la red central, por ejemplo la CSN. Por motivos de seguridad, la clave básica puede ser específica para un servidor de DHCP. Las claves generadas por el servidor de AAA pueden transportarse al servidor de DHCP usando un protocolo RADIUS. El protocolo RADIUS puede usarse adicionalmente para transportar la clave básica a un protocolo de autenticación extensible o autenticador (IAP) tal como se describirá más adelante.

Según un ejemplo adicional, la clave básica y un identificador de clave asociado, identificando la clave asociada respectivamente una clave básica, se transfieren desde el servidor de AAA de la red doméstica del abonado, preferiblemente en un mensaje de petición de acceso, a la red de acceso que da servicio al abonado. El identificador de clave asociado puede generarse por el servidor de AAA.

Según la invención, la clave de cifrado se deriva de manera específica para cada pasarela de red de acceso en una red de servicio de acceso respectiva, actuando la pasarela de red de acceso como retransmisor de DHCP para el abonado. Esto significa que a partir de la clave básica se derivan claves de cifrado adicionales que son específicas para cada par de retransmisor de DHCP / servidor de DHCP, usándose estas claves para proteger los mensajes de DHCP intercambiados entre la red de telecomunicaciones y el abonado, especialmente entre los retransmisores de DHCP y el servidor de DHCP. La clave básica y las claves derivadas no están ligadas a un usuario o sesiones de autenticación individuales sino a un servidor de DHCP específico y a un par de retransmisor de DHCP / servidor de DHCP.

La clave de cifrado específica para la pasarela de red de acceso se genera usando la clave básica.

En un ejemplo adicional, la clave de cifrado específica para pasarela de red de acceso se usa para calcular una subopción de autenticación de agente de retransmisión como información de protección. Esto significa que, para un cálculo de la subopción de autenticación de agente de retransmisión, no se usa la clave básica sino en su lugar la clave de cifrado que se deriva de la clave básica y que es específica para una pasarela de red de acceso. La pasarela de red de acceso actúa como retransmisor de DHCP para el abonado. La manera propuesta para hacer que la clave de cifrado derivada sea específica para cada pasarela de red de aplicación es incluir la dirección IP de la pasarela de red de aplicación en el proceso de derivación de clave.

Cuando el servidor de DHCP en la red central recibe un mensaje de DHCP que contiene la subopción de autenticación de agente de retransmisión, debe verificar la subopción de autenticación. En caso de que el servidor de DHCP no tenga todavía la clave básica que corresponde al identificador de clave contenido en la subopción de autenticación recibida, el servidor de DHCP solicitará la clave básica al servidor de AAA. Esto puede llevarse a cabo de la misma manera en la que un agente doméstico solicita una clave raíz de agente doméstico (HA-RK) cuando tiene que verificar una extensión de autenticación de agente externo - agente doméstico (FA-HA) en el mensaje de petición de registro de IP móvil. El servidor de DHCP puede usar el mensaje de petición de acceso para solicitar la clave básica al servidor de AAA. El servidor de DHCP debe incluir el valor del campo de identificador de clave de la subopción de autenticación del mensaje de DHCP recibido en el mensaje de excepción de acceso. El servidor de AAA entrega la clave básica correspondiente al servidor de DHCP y el identificador de clave indicado al servidor de DHCP que lo solicita en el mensaje de aceptación de acceso. En caso de que el identificador de clave sea desconocido para el servidor de AAA, el servidor de AAA envía denegación de acceso al servidor de DHCP. Por otro lado, si la clave básica asociada con el identificador de clave recibido ya estaba disponible en el servidor de DHCP, no es necesario que el servidor de DHCP pida al servidor de AAA la clave básica. En este caso, el servidor de DHCP usará la clave básica ya disponible. Una vez que la clave básica está disponible en el servidor de DHCP, éste genera la clave de cifrado específica para este retransmisor de DHCP y usa la clave generada para verificar la subopción de autenticación. El servidor de DHCP también incluye la subopción de autenticación de agente de retransmisión en su respuesta usando la clave de cifrado requerida para calcularla.

En un ejemplo adicional de la invención, la clave básica, el identificador de clave asociado y un periodo de validez de la clave básica se mantendrán en la pasarela de red de acceso que actúa como autenticador de protocolo de autenticación extensible (EAP) hasta que expire el periodo de validez de la clave básica.

Según un ejemplo adicional, se mantendrán la clave de cifrado, el identificador de clave y un contador de detección de reproducción en la pasarela de red de acceso que actúa como retransmisor de DHCP para el abonado.

Según un ejemplo adicional, se transfieren el identificador de clave y los valores de detección de reproducción desde un retransmisor de DHCP antiguo a un retransmisor de DHCP nuevo como parte del contexto a través de mensajes de señalización específicos, especialmente WiMAX.

En cualquier instancia de tiempo, el servidor de AAA puede tener varias claves básicas válidas que son específicas para un único servidor de DHCP. Estas claves básicas deben tener identificadores de clave diferentes y pueden tener periodos de validez diferentes. De ese modo, se garantiza una actualización sin interrupción de las claves básicas lo que permite que coexistan tanto una clave básica antigua como una nueva y que se usen simultáneamente durante algún tiempo.

En un ejemplo adicional, cuando un servidor de DHCP en la red doméstica del abonado recibe un mensaje de DHCP desde un retransmisor de DHCP de la red de acceso para el que no está disponible todavía ninguna clave de cifrado, pero la subopción de autenticación indica que el servidor de DHCP ya conoce el identificador de clave, el servidor de DHCP genera una clave de cifrado nueva a partir de la clave básica conocida asociada con el identificador de clave recibido.

Según un ejemplo adicional, se usan reglas de derivación para claves de cifrado y para claves básicas.

La invención permite conectar un retransmisor de DHCP en una red de acceso y un servidor de DHCP en una red central a través de una red IP no confiable, tal como Internet. Proporcionando un mecanismo de gestión de claves eficaz es posible proporcionar una subopción de autenticación de agente de retransmisión en mensajes de DHCP que impide que el servidor de DHCP en la red central sea objeto de diversos tipos de ataques. Puesto que las claves de cifrado usadas para proteger los mensajes de DHCP se derivan dinámicamente y tienen un periodo de validez limitado ligado al periodo de validez de una sesión de abonado, el método proporcionado puede realizar implementaciones muy amplias.

La invención se describirá adicionalmente a modo de ejemplo y con referencia a las figuras adjuntas.

La figura 1 muestra una modelo de referencia de red según la red de telecomunicaciones WiMAX,

la figura 2 muestra una jerarquía de claves de WiMAX,

la figura 3 muestra el proceso de distribución de claves de DHCP inicial, y

la figura 4 muestra una vista esquemática de la distribución de claves de DHCP en caso de que un autenticador y un retransmisor de DHCP no estén coubicados.

La presente invención se describirá con referencia a una red de telecomunicaciones WiMAX. El modelo de referencia de red WiMAX conocido está ilustrado en la figura 1. Una característica de la arquitectura de red de telecomunicaciones WiMAX es el soporte de terminales SS/MS de "IP simple". Estos terminales SS/MS de IP simple usan DHCP (protocolo de configuración dinámica de *host*) para adquirir una dirección IP y otros parámetros de configuración de IP. La dirección IP para el terminal SS/MS de IP, que se denominará abonado, se asigna por una red de servicio de conectividad (CSN) de WiMAX, o bien una CSN doméstica (VSP doméstico) o bien una CSN visitada (CSN visitada). La asignación de la dirección IP al abonado SS/MS se realiza por una red de servicio de acceso (ASN) de WiMAX que se denomina red de acceso.

Según la invención, la asignación de la dirección IP se realizará usando una retransmisor de DHCP en la ASN. De ese modo, se supone que un servidor de DHCP está ubicado en la CSN y la ASN proporciona el retransmisor de DHCP. El objeto del retransmisor de DHCP es retransmitir mensajes de DHCP desde el abonado SS/MS al servidor de DHCP en la CSN. Durante la autenticación de abonado, la CSN proporciona a la ASN la dirección IP del servidor de DHCP en la CSN. Esta dirección IP se usa posteriormente por el retransmisor de DHCP para retransmitir los mensajes de DHCP desde el terminal al servidor de DHCP correcto. Puesto que la CSN y la ASN pueden estar ubicadas en subredes diferentes que están conectadas a través de una red IP desconocida, por ejemplo Internet público. Como resultado, los datos intercambiados entre el elemento retransmisión de DHCP y el servidor de DHCP pueden discurrir a través de una infraestructura de IP no confiable (véanse los nodos R3 y R5).

Para evitar un posible ataque al servidor de DHCP, la invención sugiere usar claves de cifrado, a continuación en el presente documento denominadas claves de DHCP, para proteger los mensajes de DHCP entre el retransmisor de DHCP y el servidor de DHCP. Ya se usa un enfoque similar en las normas de NWG del foro de WiMAX para generar la HA-RK usada para la autenticación de la señalización de IP móvil entre el HA y el FA. La figura 2 ilustra la jerarquía de claves de WiMAX con diversas claves y cómo se derivan. Puede hallarse una explicación de esta ilustración conocida en RFC 4030. Las claves de DHCP se generan a partir de una clave básica que se denominará DHCP-RK (clave raíz). La clave DHCP-RK se genera por un servidor de AAA que está ubicado en la CSN. La clave se transporta al retransmisor de DHCP y al servidor de DHCP usando el protocolo de AAA. A partir de la DHCP-RK se derivan las claves de DHCP adicionales que son específicas para cada par de retransmisor de DHCP / servidor de DHCP y estas claves de DHCP se usan para proteger mensajes de DHCP intercambiados entre el / los retransmisor(es) de DHCP y el servidor de DHCP.

La DHCP-RK y las claves de DHCP derivadas de la misma no dependen de una clave de sesión maestra (MSK) o una clave de sesión maestra extendida (EMSK) generada como resultado de una autenticación EAP específica. Por tanto, la DHCP-RK y las claves de DHCP derivadas no están ligadas a un usuario o sesiones de autenticación individuales sino a un servidor de DHCP específico y a pares de retransmisor de DHCP / servidor de DHCP. La DHCP-RK se generará sólo a petición pero no para cada (re)autenticación EAP que se produzca. No obstante, la clave DHCP-RK junto con el identificador de clave y valores de periodo de validez se entregan al autenticador durante una autenticación de acceso de red de un abonado. El periodo de validez y un identificador de clave generados por el servidor de DHCP y que identifican una DHCP-RK específica se gestionan por el servidor de AAA. La responsabilidad del servidor de AAA es entregar una DHCP-RK nueva al autenticador antes de la expiración de la DHCP-RK.

La DHCP-RK se genera por el servidor de AAA asignando el servidor de DHCP a un abonado de autenticación. Se genera una DHCP-RK diferente para cada servidor de DHCP. Puede generarse una DHCP-RK por el servidor de AAA tal como sigue:

DHCP-RK = HMAC-SHA1 (RAND, "CLAVE RAÍZ DE APLICACIÓN DE DHCP").

De ese modo, RAND es un valor aleatorio generado por el servidor de AAA. El servidor de AAA también asocia cada DHCP-RK con un identificador de clave único. El identificador de clave se define en RFC 4030. El identificador de clave es único dentro del alcance de un único servidor de DHCP. En caso de que existan varias DHCP-RK para un único servidor de DHCP al mismo tiempo, deben tener identificadores de clave diferentes. DHCP-RK que pertenecen a servidores de DHCP diferentes pueden usar el mismo identificador de clave. El servidor de AAA entrega la DHCP-RK al autenticador de EAP y al servidor de DHCP.

El autenticador de EAP genera a partir de la DHCP-RK una clave de DHCP para un par de retransmisor de DHCP / servidor de DHCP específico si se solicita por el retransmisor de DHCP específico. Puede derivarse una clave de DHCP específica para un retransmisor de DHCP, que también se denomina pasarela de red de aplicación ASN-GW, tal como sigue:

Clave-DHCP = HMAC SHA1 (DHCP-RK, "DHCP AUTH", IP-retransmisor-DHCP, IP-servidor-DHCP).

Esta clave se deriva por el autenticador de EAP y el servidor de DHCP. Se transfiere por el autenticador de EAP al retransmisor de DHCP.

En cualquier instancia de tiempo, el servidor de AAA puede tener varias claves DHCP-RK válidas específicas para un único servidor de DHCP. Estas claves DHCP-RK deben tener identificadores de clave diferentes y pueden tener periodos de validez diferentes. Esto es necesario para permitir una actualización sin interrupción de la DHCP-RK, lo que permite que tanto una DHCP-RK antigua como una nueva coexistan y se usen simultáneamente durante algún tiempo.

Las claves generadas por el servidor de AAA pueden transportarse al servidor de DHCP y al autenticador usando el protocolo RADIUS. Las claves de DHCP generadas por el autenticador (derivadas de una DHCP-RK) se transportan al retransmisor de DHCP, por ejemplo a través de una señalización R4 específica de WiMAX. Las claves generadas por el servidor de DHCP nunca se transportan fuera del servidor de DHCP.

Haciendo referencia a la figura 3, se muestra la distribución de claves de DHCP para el caso en el que el retransmisor de DHCP está coubicado con el autenticador de EAP.

Tal como se describió anteriormente, el autenticador y el retransmisor de DHCP están ubicados en la ASN mientras que el servidor de AAA, un servidor de EAP y un contenedor de claves junto con el servidor de DHCP están ubicados en la CSN. El abonado de la red de telecomunicaciones se representa con MN.

La distribución de claves se ejecutará durante un proceso de autenticación del abonado MN de la red de telecomunicaciones. Por tanto, el abonado MN envía un mensaje de petición a la pasarela de red de acceso ASN-GW que actúa como autenticador y retransmisor de DHCP. La pasarela de red de acceso transfiere un mensaje de petición de acceso a la CSN, especialmente al servidor de AAA. El autenticador recibe una dirección de servidor de DHCP en un mensaje de aceptación de acceso según el protocolo RADIUS como resultado de una autenticación de abonado satisfactoria. En caso de que varias DHCP-RK asociadas con el servidor de DHCP estén disponibles en el servidor de AAA, el servidor de AAA debe incluir la DHCP-RK con el periodo de validez restante más largo en el mensaje de aceptación de acceso. Además de la DHCP-RK, el mensaje de aceptación de acceso contiene también el periodo de validez y un identificador de clave de la DHCP-RK, proporcionándose este último por el servidor de DHCP. La DHCP-RK se transporta a través de RADIUS y se cifra, por ejemplo usando el método definido en la sección 3.5 de RFC-2868. Las claves generadas por el servidor de AAA se almacenan en un contenedor de claves en el autenticador en la ASN (no mostrado). En el momento de los procedimientos de DHCP, el retransmisor de DHCP obtiene la clave de DHCP derivada desde el contenedor de claves en el autenticador. El contenedor de claves deriva la clave de DHCP específica para el retransmisor de DHCP que la solicita a partir de la DHCP-RK y entrega la clave derivada, su periodo de validez y el identificador de clave asociado con la DHCP-RK al retransmisor de DHCP. El retransmisor de DHCP usa la clave de DHCP recibida para calcular la subopción de autenticación e incluye la subopción en el mensaje de DHCP. Cuando el servidor de DHCP recibe un mensaje con subopción de autenticación, busca la clave de DHCP correspondiente en su memoria caché local mediante la dirección de retransmisor de DHCP y el identificador de clave recibido. Si no se halla la clave correspondiente, el servidor de DHCP deriva una clave de DHCP nueva específica para este retransmisor de DHCP a partir de la DHCP-RK. Si están disponibles varias DHCP-RK en el servidor de DHCP, usa el identificador de clave recibido para seleccionar la DHCP-RK correcta. Si no se halla ninguna DHCP-RK que esté asociada con el identificador de clave recibido, el servidor de DHCP adquiere la DHCP-RK del servidor de AAA. Esto puede producirse de la misma manera que un agente doméstico adquiere una clave raíz de agente doméstico. El servidor de DHCP debe incluir el identificador de clave recibido en el mensaje de petición de acceso. Esto permitirá al servidor de AAA localizar la DHCP-RK correcta en caso de que estén disponibles varias DHCP-RK para este servidor de DHCP particular en el servidor de AAA.

La figura 4 describe la distribución de las claves de DHCP en el caso en el que el retransmisor de DHCP y el autenticador no estén coubicados. Cuando el retransmisor de DHCP intercepta un mensaje de DHCP desde el abonado debe proporcionarle la subopción de autenticación, tal como se menciona en RFC 4030. Si la clave correspondiente al servidor de DHCP no está disponible en el retransmisor de DHCP, el retransmisor de DHCP solicitará una clave al autenticador enviando un mensaje de petición de contexto con un TLV de clave de DHCP vacío. El autenticador derivará la clave necesaria y entregará la clave derivada, su periodo de validez y el identificador de clave asociado al elemento retransmisión de DHCP en un mensaje de informe de contexto. Habiendo adquirido la clave de DHCP, el retransmisor de DHCP procede tal como se describió anteriormente en la realización de la figura 3 cuando el retransmisor de DHCP y el autenticador están coubicados.

REIVINDICACIONES

1. Método para la transmisión de un mensaje de protocolo de configuración dinámica de *host*, DHCP, entre un servidor de DHCP de una red de telecomunicaciones y un dispositivo de abonado (SS/MS; MN) de protocolo de Internet, IP, conectado a la red de telecomunicaciones,

en el que un retransmisor de DHCP, que retransmite el mensaje de DHCP entre el dispositivo de abonado de protocolo de Internet y el servidor de DHCP, está ubicado entre el dispositivo de abonado de protocolo de Internet y el servidor de DHCP,

se añade una información protegida con una clave de cifrado al mensaje de DHCP por el servidor de DHCP o por el retransmisor de DHCP,

la clave de cifrado se deriva de una clave básica que se proporciona por un servidor adicional de la red de telecomunicaciones,

caracterizado porque

la clave básica es una clave única para el servidor de DHCP, y

la clave de cifrado se genera usando la clave básica única para el servidor de DHCP, para cada par específico de un servidor de DHCP y un retransmisor de DHCP.

2. Método según la reivindicación 1, caracterizado porque

el mensaje de DHCP generado por el dispositivo de abonado se intercepta por el retransmisor de DHCP, y la información cifrada con la clave de cifrado se añade por el retransmisor de DHCP.

3. Método según cualquiera de las reivindicaciones anteriores, caracterizado porque

la clave básica única para el servidor de DHCP es una clave raíz específica para el servidor de DHCP.

4. Método según cualquiera de las reivindicaciones anteriores, caracterizado porque

el servidor adicional es un servidor de AAA de la red doméstica del abonado, y porque

la clave básica y un identificador de clave asociado, identificando el identificador de clave asociado respectivamente una clave básica, se transfieren desde el servidor de AAA de la red doméstica del abonado, preferiblemente en un mensaje de petición de acceso, a una red de acceso (ASN) que da servicio al abonado (SS/MS; MN).

5. Método según cualquiera de las reivindicaciones anteriores, caracterizado porque

se deriva la clave de cifrado, clave de DHCP, específica para cada pasarela de red de acceso (ASN-GW) en una red de servicio de acceso (ASN) respectiva que actúa como retransmisor de DHCP para el dispositivo de abonado (SS/MS; MN).

6. Método según cualquiera de las reivindicaciones anteriores, caracterizado por una transferencia del identificador de clave y valores de detección de reproducción desde un retransmisor de DHCP antiguo a un retransmisor de DHCP nuevo como parte del contexto a través de mensajes de señalización específicos, especialmente WiMAX.

7. Método según cualquiera de las reivindicaciones anteriores, caracterizado porque

cuando el servidor de DHCP en la red doméstica del abonado recibe un mensaje de DHCP desde un retransmisor de DHCP de la red de acceso para el que no está disponible todavía ninguna clave de cifrado, pero una subopción de autenticación indica que el servidor de DHCP ya conoce el identificador de clave, el servidor de DHCP genera una clave de cifrado nueva a partir de la clave básica conocida asociada con el identificador de clave recibido.

8. Método según cualquiera de las reivindicaciones anteriores, caracterizado porque

la red de telecomunicaciones es una red según la norma WiMAX.

9. Componente de red de telecomunicaciones para la transmisión de un mensaje de protocolo de configuración dinámica de *host*, DHCP, entre un servidor de DHCP de una red de telecomunicaciones y un

dispositivo de abonado (SS/MS; MN) de protocolo de Internet, IP, conectado a la red de telecomunicaciones, en el que

se añade una información protegida con una clave de cifrado por el componente de red de telecomunicaciones al mensaje de DHCP transmitido entre el dispositivo de abonado (SS/MS; MN) de protocolo de Internet, IP, y el servidor de DHCP,

la clave de cifrado se deriva por el componente de red de telecomunicaciones a partir de una clave básica que se proporciona por un servidor adicional de la red de telecomunicaciones, y

dicho componente de red está caracterizado porque

la clave básica es una clave única para el servidor de DHCP, y porque

la clave de cifrado se genera usando la clave básica única para el servidor de DHCP, para cada par específico de un servidor de DHCP y un retransmisor de DHCP.

10. Componente de red de telecomunicaciones según la reivindicación 9, caracterizado porque

la clave básica única para el servidor de DHCP es una clave raíz específica para el servidor de DHCP.

11. Componente de red de telecomunicaciones según la reivindicación 9 ó 10, caracterizado porque

el servidor adicional es un servidor de AAA de la red doméstica del abonado, y

la clave básica y un identificador de clave asociado, identificando el identificador de clave asociado respectivamente una clave básica, se transfieren desde el servidor de AAA, preferiblemente en un mensaje de petición de acceso, al componente de red de telecomunicaciones.

12. Componente de red de telecomunicaciones según cualquiera de las reivindicaciones 9 a 11,

caracterizado porque el componente de red de telecomunicaciones es un servidor de DHCP.

13. Componente de red de telecomunicaciones según la reivindicación 12, caracterizado porque

cuando el servidor de DHCP recibe un mensaje de DHCP para el que no está disponible todavía ninguna clave de cifrado, pero una subopción de autenticación incluida en el mensaje de DHCP indica que el servidor de DHCP ya conoce un identificador de clave, el servidor de DHCP genera una clave de cifrado nueva a partir de la clave básica conocida asociada con el identificador de clave recibido.

14. Componente de red de telecomunicaciones según cualquiera de las reivindicaciones 9 a 11, caracterizado porque

el mensaje de DHCP generado por el dispositivo de abonado se intercepta por el componente de red de telecomunicaciones

en el que la información cifrada con la clave de cifrado se añade por el componente de red de telecomunicaciones.

15. Componente de red de telecomunicaciones según cualquiera de las reivindicaciones 9 a 11 ó 14,

caracterizado porque el componente de red de telecomunicaciones es un retransmisor de DHCP.

16. Componente de red de telecomunicaciones según cualquiera de las reivindicaciones 9 a 11 ó 14, caracterizado porque

el componente de red de telecomunicaciones es una pasarela de red de acceso y la clave de cifrado se deriva de manera específica para la pasarela de red de acceso usando la clave básica en una red de servicio de acceso respectiva y que actúa como el retransmisor de DHCP para el mensaje de DHCP.

17. Componente de red de telecomunicaciones según cualquiera de las reivindicaciones 9 a 11 ó 14 a 16, caracterizado por

soportar la transferencia del identificador de clave y valores de detección de reproducción desde un componente de red de telecomunicaciones antiguo que incluye una funcionalidad de retransmisión de DHCP a un componente de red de telecomunicaciones nuevo que incluye una funcionalidad de

retransmisión de DHCP como parte del contexto a través de mensajes de señalización específicos.

18. Componente de red de telecomunicaciones según cualquiera de las reivindicaciones 9 a 17, caracterizado porque

la red de telecomunicaciones es una red según la norma WiMAX.

FIG 1

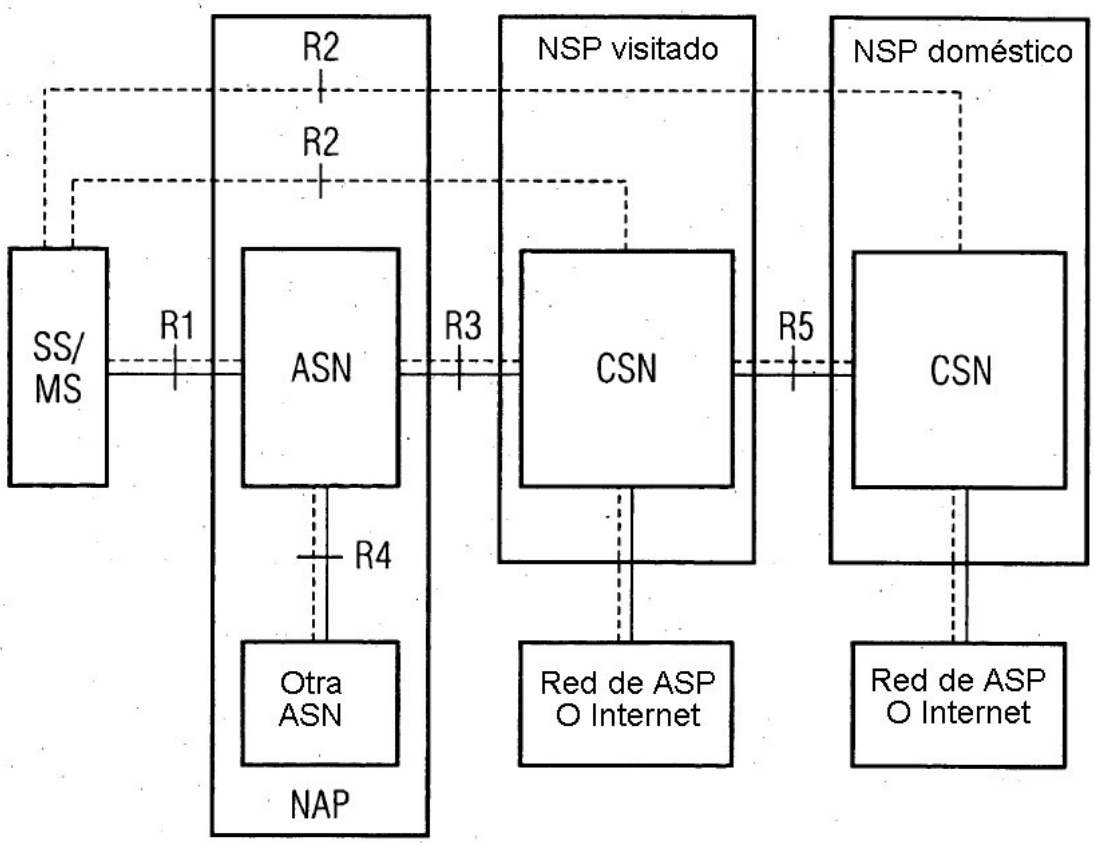

R2
R2
NSP visitado
NSP doméstico
SS/
MS
R1
ASN
R3
CSN
R5
CSN
R4
Otra
ASN
Red de ASP
O Internet
Red de ASP
O Internet
NAP

FIG 2

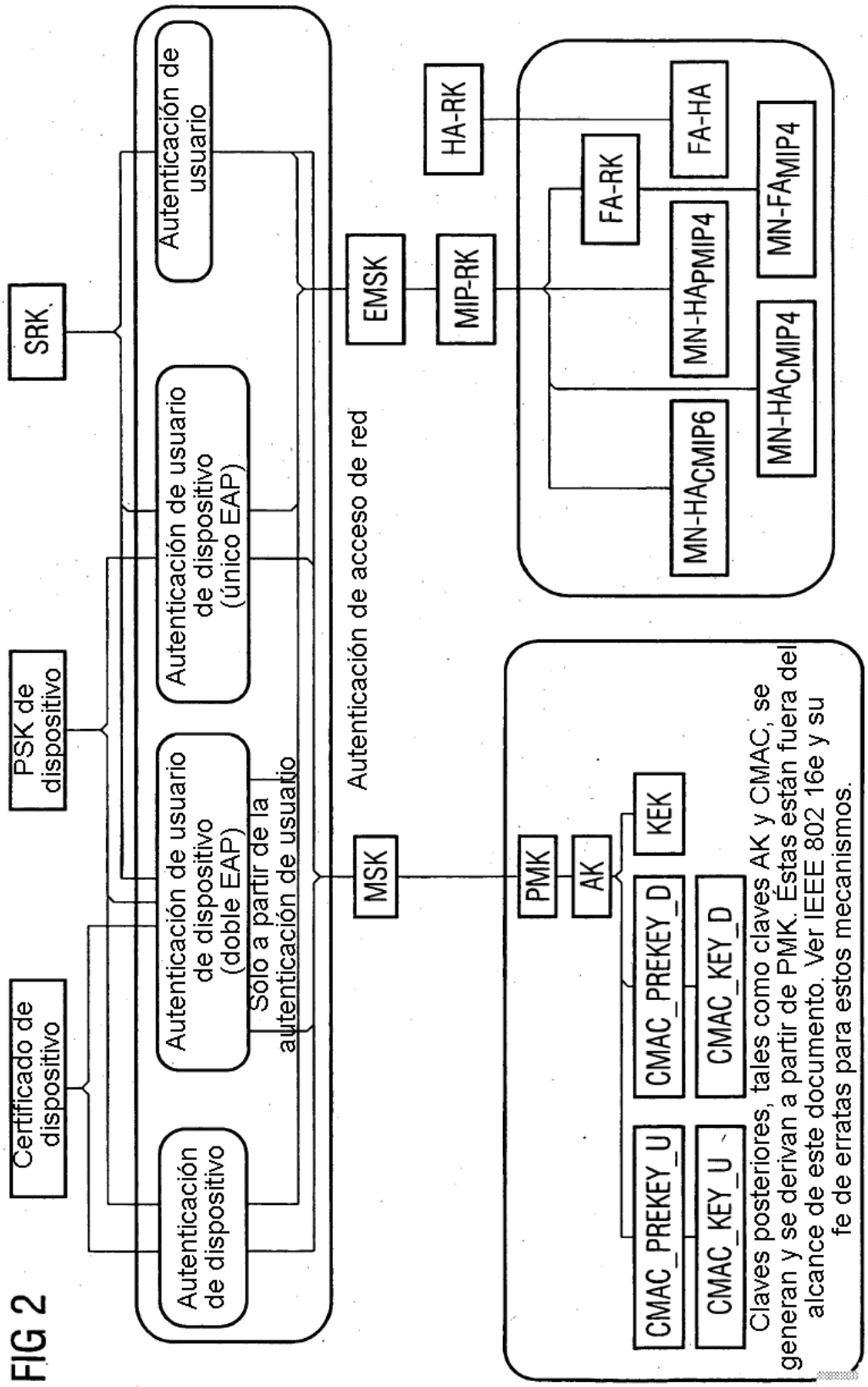

Certificado de dispositivo
PSK de dispositivo
SRK
Autenticación de dispositivo
Autenticación de usuario de dispositivo (doble EAP)
Autenticación de usuario de dispositivo (único EAP)
Autenticación de usuario
Sólo a partir de la autenticación de usuario
Autenticación de acceso de red
MSK
EMSK
MIP-RK
HA-RK
FA-RK
FA-HA
MN-HACMIP6
MN-HAPMIP4
MN-HACMIP4
MN-FAMIP4
PMK
AK
KEK
CMAC_PREKEY_U
CMAC_KEY_U
CMAC_PREKEY_D
CMAC_KEY_D
Claves posteriores, tales como claves AK y CMAC, se generan y se derivan a partir de PMK. Éstas están fuera del alcance de este documento. Ver IEEE 802 16e y su fe de erratas para estos mecanismos.

FIG 3

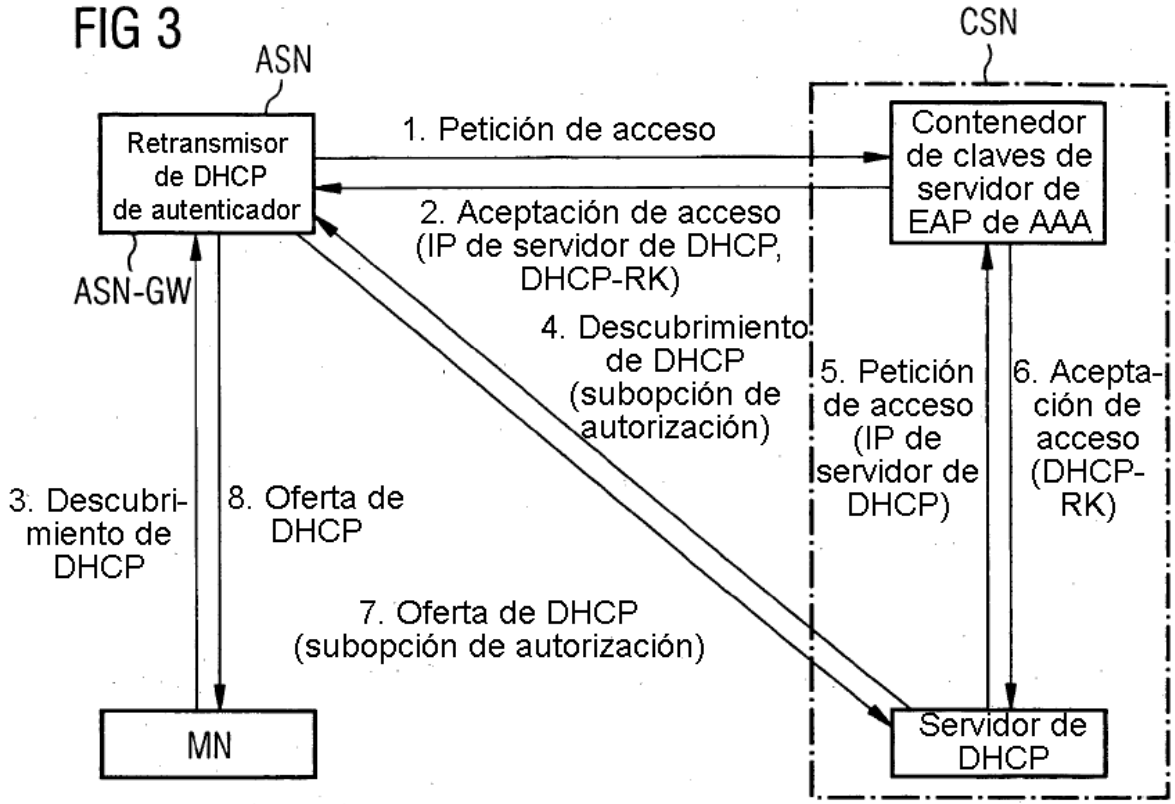
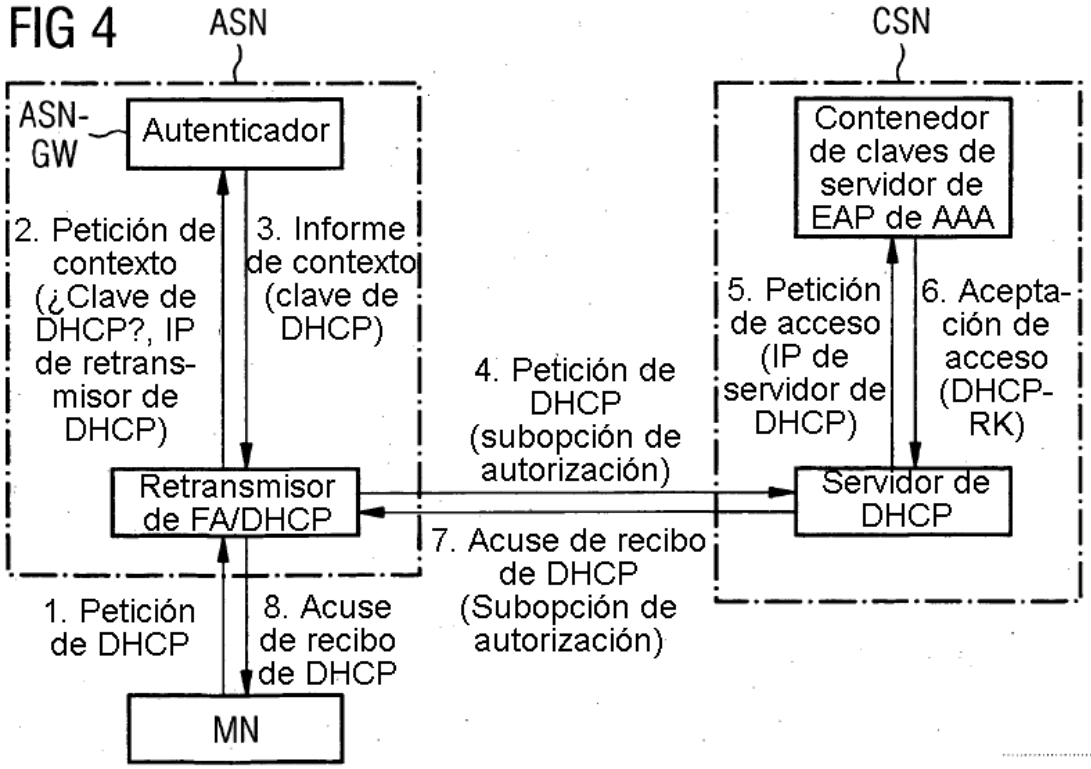

ASN
CSN
Retransmisor de DHCP de autenticador
1. Petición de acceso
Contenedor de claves de servidor de EAP de AAA
2. Aceptación de acceso (IP de servidor de DHCP, DHCP-RK)
ASN-GW
4. Descubrimiento de DHCP (subopción de autorización)
5. Petición de acceso (IP de servidor de DHCP)
6. Aceptación de acceso (DHCP-RK)
3. Descubrimiento de DHCP
8. Oferta de DHCP
7. Oferta de DHCP (subopción de autorización)
MN
Servidor de DHCP

FIG 4


ASN
CSN
ASN-GW
Autenticador
Contenedor de claves de servidor de EAP de AAA
2. Petición de contexto (¿Clave de DHCP?, IP de retransmisor de DHCP)
3. Informe de contexto (clave de DHCP)
5. Petición de acceso (IP de servidor de DHCP)
6. Aceptación de acceso (DHCP-RK)
4. Petición de DHCP (subopción de autorización)
Retransmisor de FA/DHCP
Servidor de DHCP
7. Acuse de recibo de DHCP (Subopción de autorización)
1. Petición de DHCP
8. Acuse de recibo de DHCP
MN