(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 455 716**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.09.2008 E 08800752 (1)**

(97) Fecha y número de publicación de la concesión europea: **22.01.2014 EP 2154858**

(54) Título: **Método y dispositivo para evitar que una dirección ARP sea falsificada y atacada**

(30) Prioridad:

06.09.2007 CN 200710121472

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.04.2014

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:

LI, ZHENHAI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo para evitar que una dirección ARP sea falsificada y atacada

Campo de la invención

La presente invención está relacionada con las comunicaciones de red y, en particular, con un método y un equipo para defenderse frente a ataques de suplantación ARP en una red.

Antecedentes de la invención

En el entorno de red actual, el Protocolo de Resolución de Direcciones (ARP) es un protocolo de bajo nivel en la pila del Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP). La finalidad del ARP es convertir direcciones IP en direcciones de Control de Acceso al Medio (MAC) que son direcciones físicas Ethernet. La comunicación entre dispositivos de red utiliza direcciones MAC pero las aplicaciones basadas en TCP/IP utilizan direcciones IP. Todos los paquetes de datos basados en direccionamiento IP tienen en último término que ser encapsulados en tramas Ethernet basadas en direccionamiento MAC para poderse transmitir. Por lo tanto, cuando un dispositivo de red se encuentra en comunicación, el dispositivo de red debe obtener la dirección MAC correspondiente a la dirección IP utilizando un protocolo. El protocolo que lleva a cabo la resolución es el ARP.

Para conseguir una conversión de direcciones más rápida, un dispositivo de red con el ARP habilitado siempre adopta la tecnología de almacenamiento temporal de ARP para almacenar temporalmente un cierto número de relaciones de asociación de direcciones en una estructura de tabla local que, en general, se denomina tabla de almacenamiento temporal ARP (tabla ARP para abreviar). Las entradas ARP del almacenamiento temporal tienen dos orígenes: uno es la generación dinámica de acuerdo con mensajes ARP, lo cual significa que el dispositivo puede aprender la asociación entre una dirección IP y una dirección MAC a partir de una petición ARP o una respuesta ARP para generar una entrada dinámica de almacenamiento temporal del ARP; el otro es una configuración estática manual. Para mantener la validez de las entradas de almacenamiento temporal ARP dinámicas, las entradas dinámicas caducan en un determinado tiempo. Las entradas configuradas de forma estática no caducan. Su incorporación o eliminación depende de operaciones manuales.

El procesamiento del protocolo ARP es complejo. Normalmente, el plano de reenvío recibe un mensaje ARP y reenvía el mensaje al plano de control para su procesamiento. El plano de control genera una entrada de almacenamiento temporal del ARP y envía la entrada a la tabla de almacenamiento temporal de ARP del plano de reenvío. El plano de reenvío utiliza la entrada de almacenamiento temporal del ARP para encapsular y enviar mensajes. En la técnica anterior, el procesamiento ARP proporciona únicamente una asociación simple entre las direcciones de los protocolos de capas más altas y las direcciones físicas de las capas más bajas sin ninguna autenticación de seguridad de dichas asociaciones. En un entorno de red complejo como el acceso a Internet, dicha simplicidad y apertura ofrece oportunidades para ataques de suplantación de direcciones. Al ataque de suplantación ARP está dirigido, generalmente, a hacerse con información privada del usuario. El atacante envía peticiones o respuestas ARP incluyendo asociaciones incorrectas de direcciones para corromper la tabla de almacenamiento temporal de ARP de un dispositivo de red. Como resultado, el dispositivo de red envía paquetes de datos a la dirección física errónea. El dispositivo de red puede ser una pasarela o un servidor, o cualquier otro dispositivo de red. Para defender la tabla de almacenamiento temporal de ARP del dispositivo de red frente a ataques de suplantación de direcciones, la técnica anterior proporciona las siguientes soluciones:

(1) ARP persistente

Después de haber habilitado las características de ARP persistente, una entrada de almacenamiento temporal del ARP aprendida a partir de una petición ARP o una respuesta ARP no se actualiza hasta que la entrada caduca. Después de haber caducado, la entrada de almacenamiento temporal del ARP se elimina y comienza un nuevo proceso de aprendizaje. La solución es simple pero da lugar a un problema. Esto es, una vez que el dispositivo de red genera una entrada de almacenamiento temporal del ARP de acuerdo con un mensaje de ataque de ARP que llega antes que un mensaje ARP legal, el servidor no es capaz de crear una entrada de almacenamiento temporal del ARP correcta en el dispositivo de red, de modo que la utilización del servidor se ve afectada y no se defiende de la suplantación ARP.

(2) Verificación activa

Después de que el dispositivo de red recibe una petición ARP o una respuesta ARP, el dispositivo de red siempre envía una petición ARP a la dirección IP incluida en el mensaje ARP recibido para verificar la asociación de direcciones. Si la dirección no existe, el dispositivo de red no recibe una respuesta ARP desde la dirección IP. Si se suplanta la dirección MAC en la entrada de almacenamiento temporal del ARP correspondiente a la dirección IP, el dispositivo de red recibe una respuesta ARP que incluye una dirección MAC diferente. En cualquier caso, el dispositivo de red se da cuenta de la suplantación y, de este modo, puede llevar a cabo el procesamiento correspondiente. La debilidad de esta solución consiste en que dicha verificación se lleva a cabo sobre mensajes

ARP desde cada dirección IP. Si no se producen ataques de suplantación, la solución provoca un desaprovechamiento de los anchos de banda de red e impacta en el rendimiento de la red.

Para finalizar, la técnica anterior presenta al siguiente problema: las soluciones existentes para defenderse frente a ataques de suplantación ARP carecen de una verificación fiable y efectiva y provocan un desaprovechamiento de anchos de banda de la red e impacta en el rendimiento si no se producen ataques de suplantación.

El documento de Kanamori M y otros: "A Self-confirming Engine For Preventing Man-In-The-Middle-Atack (Una herramienta de autocomprobación para evitar un Ataque Man In The Middle)" Actas del IEICE sobre la Comunicación, Sociedad de Comunicaciones, Tokio, JP, vol. E87B, núm. 3, 1 de marzo de 2004 (2004-03-01), páginas 530-538, XP001503188, ISSN: 0916-8516, divulga un tipo de método de acceso no autorizado. De acuerdo con el D1, en ARP, cuando se produce una alteración de un Almacenamiento Intermedio de ARP, el SCE envía una petición ARP como paquete de confirmación a la dirección de la capa de enlace antigua correspondiente al servidor B. En este caso, se puede comprobar la validez esperando una respuesta ARP. Existen dos situaciones: (1) no se recibe ninguna respuesta ARP: ningún servidor responde a la petición ARP debido a que no existe el servidor con la dirección de la capa de enlace antigua. Esto prueba que la dirección IP se ha asignado a un nuevo servidor. Por lo tanto, es normal la nueva tabla de asociación de direcciones modificada en el servidor A. (2) se recibe una respuesta ARP: el servidor B con la dirección de la capa de enlace antigua recibe nuestra petición ARP. La recepción de una respuesta ARP indica que el servidor B todavía sigue utilizando la misma dirección de la capa de enlace y la misma dirección IP. Esto prueba que el cambio de la tabla de asociación de direcciones en el servidor A es anormal (ver sección 3.2.1, Fig. 6 (I)).

El documento de Ilya Teterin "arp spoofing defence (defensa frente a suplantación arp)" del 15 de noviembre de 2002 (2002-11-15), páginas 1-1, XP002580036, divulga que: "el núcleo enviará una petición ARP para comprobar si existe un servidor en la dirección MAC "antigua". Si se recibe dicha respuesta nos permite conocer que una IP pretende tener varias direcciones MAC al mismo tiempo, probablemente provocado por un ataque de suplantación ARP".

Resumen de la invención

La presente invención proporciona un método y un equipo para defenderse frente a ataques de suplantación ARP con el fin de permitir una verificación ARP fiable y efectiva, reducir las interacciones de señalización y preservar recursos de red y está definida mediante la reivindicación 1 independiente del método y la reivindicación 4 independiente del equipo.

Breve descripción de los dibujos

La FIG. 1 es un diagrama esquemático de un método proporcionado de acuerdo con un modo de realización de la presente invención;

la FIG. 2 es un diagrama esquemático de una estructura de un equipo proporcionado de acuerdo con un modo de realización de la presente invención; y

la FIG. 3 es un diagrama esquemático que muestra el cambio de estado del indicador de actualización de acuerdo con un modo de realización de la presente invención.

Descripción detallada de la invención

Los modos de realización de la presente invención proporcionan un método y un equipo para defenderse frente a ataques de suplantación ARP. Cuando una entrada ARP es actualizable, si la dirección MAC en un mensaje ARP recibido tiene una misma dirección IP que la de la entrada ARP con la misma dirección MAC en la entrada ARP, se determina que el mensaje ARP recibido no es un mensaje ARP ambiguo. Esto quiere decir que no se produce ninguna suplantación de direcciones. En este caso no se inicia ningún proceso de verificación de modo que no se añade ninguna sobrecarga de señalización de verificación. Cuando más tarde se recibe un mensaje ARP ambiguo, se inicia un proceso de verificación ARP para enviar una petición de verificación ARP a la dirección IP incluida en el mensaje ARP ambiguo. De este modo, cuando se recibe un mensaje ARP no ambiguo, lo que significa que no se produce ninguna suplantación de direcciones, no se genera ningún mensaje de verificación adicional. De este modo se reducen las interacciones de señalización y se preservan recursos de red.

Además, cuando una entrada ARP no es actualizable, la entrada ARP se bloquea. En este caso, cuando se recibe otro mensaje ARP, no es necesario comprobar la dirección MAC del mensaje ARP y no se inicia ninguna verificación. Por lo tanto, no se provoca ninguna sobrecarga de señalización de verificación adicional.

Normalmente, después de haber enviado una petición de verificación ARP, se recibe una respuesta a la verificación ARP. A continuación, el dispositivo de red puede comparar la dirección MAC en la respuesta a la verificación ARP, la dirección MAC en la entrada ARP y la dirección MAC en el mensaje ARP ambiguo. Si el dispositivo de red es capaz

de realizar una comprobación óptima en función del resultado de la comparación para decidir la dirección MAC real, el dispositivo de red toma la entrada ARP con la dirección MAC real como la entrada ARP óptima y la bloquea como la entrada ARP óptima. Esto quiere decir que la entrada ARP no se podrá actualizar hasta que la entrada ARP caduque. De este modo, el dispositivo de red puede denegar posibles ataques de suplantación que sucedan en cualquier momento y evitar ataques de suplantación de direcciones utilizando un barrido aleatorio y proteger la utilización normal del servidor real.

Para explicar mejor la presente invención, los modos de realización de la presente invención se describen haciendo referencia a los dibujos adjuntos.

La FIG. 1 es un diagrama esquemático del método de acuerdo con un modo de realización de la presente invención. El método incluye los siguientes pasos:

Paso 11: determinar si se ha recibido un mensaje ARP ambiguo.

Cuando una entrada ARP es actualizable, por ejemplo, durante el aprendizaje inicial de la entrada ARP, este paso es el mismo que en el procesamiento normal. Esto es, la entrada ARP se genera mediante aprendizaje a partir de una petición ARP y una respuesta ARP, y la entrada ARP se utiliza como la entrada ARP aprendida inicialmente. Esto quiere decir que el dispositivo de red utiliza la entrada ARP para encapsular los mensajes que se van a reenviar. En este momento, la entrada ARP aprendida inicialmente es actualizable.

Si un mensaje ARP recibido más tarde que tiene la misma dirección IP que la entrada ARP es un mensaje ARP ambiguo, lo cual quiere decir que la dirección MAC en el mensaje ARP es diferente de la dirección MAC en la entrada ARP, es necesario ejecutar el paso 12 para validar la entrada ARP. Si un mensaje ARP recibido más tarde tiene la misma dirección MAC que la entrada ARP, se ejecuta el paso 13.

Paso 12: iniciar un proceso de verificación ARP y, a continuación, ejecutar el paso 14.

El proceso de verificación ARP consisten en enviar una petición de verificación ARP a la dirección IP y realizar una comprobación en función de la dirección MAC incluida en la respuesta de verificación ARP recibida. Por ejemplo, una petición ARP se difunde a todos los dispositivos de red en el segmento de red, solicitando la dirección MAC asociada con la dirección IP. Después de que el dispositivo de red que tiene la dirección IP haya recibido la petición ARP, el dispositivo de red envía una respuesta ARP únicamente al solicitante para notificar al solicitante su dirección MAC. Después de recibir la respuesta ARP, el dispositivo de red, esto es, el solicitante, puede utilizar la dirección MAC incluida en la respuesta ARP para realizar una comprobación de verificación.

Además, cuando se inicia la verificación ARP, es necesario configurar la entrada ARP de modo que la entrada únicamente acepte la actualización a partir de una respuesta ARP, lo cual quiere decir que la entrada no se actualiza hasta que se haya recibido la respuesta de verificación ARP. Esto puede evitar que no se pueda realizar una comprobación de verificación, lo cual se produce si se actualiza la entrada antes de haber recibido la respuesta a la verificación ARP.

Paso 13: utilizar la entrada ARP como una entrada ARP normal sin un proceso de verificación ARP.

Como no se ha iniciado ninguna verificación, no existe ninguna sobrecarga de señalización de verificación adicional. Por lo tanto, cuando no se produce ninguna suplantación de dirección, no se genera ningún mensaje de verificación adicional y, de este modo, se reducen las interacciones de señalización y se preservan recursos de red.

Paso 14: realizar una comparación y una comprobación óptima. Cuando se ejecuta el paso 12 para iniciar un proceso de verificación ARP, es necesario realizar una comprobación de verificación de acuerdo con la dirección MAC incluida en la respuesta de verificación ARP. Específicamente, la dirección MAC en la respuesta de verificación ARP se compara con la dirección MAC en la entrada ARP, y la dirección MAC en el mensaje ARP ambiguo.

Si la dirección MAC en la respuesta de verificación ARP recibida es la mima que una de las otras dos direcciones MAC, lo cual quiere decir que la dirección MAC en la respuesta de verificación ARP es la misma que la dirección MAC en la entrada ARP, o la misma que la dirección MAC en el mensaje ARP ambiguo, se puede realizar una comprobación óptima para utilizar la entrada ARP que tiene la misma dirección MAC que la entrada ARP óptima y, a continuación, se ejecuta el paso 15. Si la dirección MAC en la respuesta de verificación ARP recibida es distinta de las otras dos direcciones MAC, es imposible una comprobación óptima y se ejecuta el paso 16.

Paso 15: bloquear la entrada ARP óptima y ejecutar el paso 17.

Bloquear la entrada ARP óptima quiere decir que la entrada ARP no se actualiza antes de que caduque la entrada ARP óptima. De este modo, se deniega la suplantación de dirección que pueda ocurrir en cualquier instante y el proceso de verificación es más fiable y más efectivo.

Paso 16: mantener la entrada ARP. La entrada ARP antigua no se cambia y se sigue utilizando como una entrada

ARP normal. A continuación, el procedimiento vuelve al paso 11 para determinar si se recibe un mensaje ARP ambiguo.

Paso 17: actualizar la entrada ARP antes de su caducidad. Específicamente, antes de que caduque la entrada ARP óptima, se envía una petición ARP para iniciar un nuevo proceso de aprendizaje.

Además, se puede configurar un contador asociado a la entrada ARP. Cuando el número de verificaciones ARP alcance un valor del contador especificado dentro de un ciclo de vida, no se inicia ninguna verificación con respecto a la entrada ARP. De este modo, cuando se producen ataques masivos de suplantación de direcciones, el dispositivo de red no envía demasiados mensajes de verificación para consumir recursos de CPU excesivos de modo que se preservan los recursos del dispositivo.

Un modo de realización de la presente invención proporciona un equipo para defenderse frente a ataques de suplantación ARP. La FIG. 2 es un diagrama esquemático de la estructura del equipo, el cual incluye una unidad de comprobación de recepción y una unidad de verificación. Cuando una entrada ARP es actualizable, la unidad de comprobación de recepción se configura para comprobar si la dirección MAC en un mensaje ARP recibido que tiene la misma dirección IP que la entrada ARP es la misma que la dirección MAC en la entrada ARP.

Si las direcciones MAC son diferentes, la unidad de comprobación de recepción determina que el mensaje ARP recibido es un mensaje ARP ambiguo e informa del resultado de la comprobación. Si las direcciones MAC son iguales, la unidad de comprobación de recepción determina que no se ha recibido un mensaje ARP ambiguo y no realiza ninguna acción ni informa del resultado de la acción de comprobación no realizada.

La unidad de verificación está configurada para iniciar un proceso de verificación ARP en función del resultado de la comprobación de la unidad de comprobación de recepción. El proceso de verificación puede difundir una petición ARP a todos los dispositivos de red en el segmento de red, solicitando la dirección MAC asociada con la dirección IP. Después de que el dispositivo de red que tiene la dirección IP haya recibido la petición ARP, el dispositivo de red envía una respuesta ARP únicamente al solicitante para notificar al solicitante su dirección MAC. Después de recibir la respuesta ARP, el dispositivo de red, esto es, el solicitante, puede utilizar la dirección MAC incluida en la respuesta ARP para realizar la comprobación de verificación.

El equipo incluye, además, una unidad de comparación, la cual está configurada para comparar la dirección MAC en la respuesta de verificación ARP con la dirección MAC en la entrada ARP y la dirección MAC en el mensaje ARP ambiguo cuando la unidad de verificación inicia el proceso de verificación ARP. Si la dirección MAC en la petición de verificación ARP es la misma que una de las otras dos direcciones MAC, la unidad de comparación realiza una comprobación óptima para utilizar la entrada ARP que tenga la misma dirección MAC que la entrada ARP óptima; no se realiza una comprobación óptima si la dirección MAC de la respuesta de verificación ARP es diferente de las otras dos direcciones MAC.

Adicionalmente, el equipo incluye, además, una unidad de realización de la comprobación, la cual está configurada para llevar a cabo una operación apropiada en función del resultado de la comprobación de la unidad de comparación. Específicamente, si la unidad de comparación realiza una comprobación óptima, la unidad de realización de la comprobación bloquea la entrada ARP óptima de modo que la entrada no se vuelve a actualizar antes de su caducidad. De este modo, se deniegan los ataques de suplantación de direcciones que puedan ocurrir en cualquier momento y la verificación es más fiable y más efectiva. Si la unidad de comparación no consigue realizar una comprobación óptima, la unidad de realización de la comprobación mantiene la entrada ARP como la entrada ARP normal.

Adicionalmente, el equipo incluye, además, una unidad de control de contador, la cual está configurada para: configurar un contador para la entrada ARP y controlar que la unidad de verificación no inicie, dentro de un ciclo de vida de la entrada, un proceso de verificación con respecto a la entrada ARP cuando el número de verificaciones ARP alcance un valor de contador especificado. De este modo, cuando se producen ataques masivos de suplantación de direcciones, un dispositivo de red no envía demasiados mensajes de verificación que consumen excesivos recursos de CPU. De este modo se preservan los recursos del dispositivo.

Para explicar aún más los modos de realización de la presente invención, se ofrece un ejemplo específico para clarificar aún más la solución técnica de los modos de realización de la presente invención. Con el fin de evitar que la tabla ARP de un dispositivo de red sea suplantada, el procesamiento es del siguiente modo:

Al inicio, el aprendizaje inicial de las entradas ARP en el dispositivo de red es el mismo que el del procesamiento normal. El dispositivo de red genera una entrada ARP a partir del mensaje ARP recibido inicialmente para encapsular mensajes que vayan a ser reenviados independientemente de que el mensaje ARP sea una petición ARP o una respuesta ARP. En este momento, la entrada ARP aprendida inicialmente es actualizable.

La FIG. 3 es un diagrama esquemático que muestra el cambio de estado del indicador de actualización de acuerdo con un modo de realización de la presente invención. Como se muestra en la FIG. 3, en la entrada ARP se configura

un indicador de actualización. El valor inicial del indicador es 0, lo cual indica que la entrada ARP es actualizable y que la dirección MAC en la entrada ARP es actualizable. También se establece que cada entrada ARP en el dispositivo de red puede almacenar temporalmente dos direcciones MAC: una es la dirección MAC maestra y la otra es una dirección temporal. Aquí, la dirección MAC en la entrada ARP, o la dirección MAC aprendida inicialmente, se considera como la dirección MAC maestra y únicamente se le envía al plano de reenvío la dirección MAC maestra.

Si se determina que la dirección MAC en un mensaje ARP recibido es diferente de la dirección MAC maestra, o que se ha recibido un mensaje ARP ambiguo, la dirección MAC en el mensaje ARP ambiguo se considera como la dirección MAC temporal y se inicia un proceso de verificación. El método de verificación consiste en enviar una petición ARP a la dirección IP de la entrada ARP.

En este caso, también es necesario cambiar a 1 el indicador de actualización en la entrada ARP, tal como se muestra mediante “21” en la FIG. 3. Esto indica que la entrada ARP únicamente acepta la actualización procedente de una respuesta ARP. A continuación se envía una petición de verificación ARP. De este modo, no se actualiza el contenido de la entrada ARP que incluye la dirección MAC temporal antes de que se haya recibido la respuesta ARP. De este modo se evita lo siguiente: antes de haber recibido la respuesta ARP, cambia el contenido de la entrada, lo que provoca que sea imposible una comprobación de verificación correspondiente.

Supóngase que ya existen dos direcciones MAC en la entrada ARP actual, MAC1 y MAC2, donde MAC1 es la dirección MAC maestra actual y MAC2 es la dirección MAC temporal ambigua y supóngase que MAC3 es la dirección MAC del remitente de la respuesta de verificación ARP recibida. Después de que se haya recibido la respuesta a la verificación ARP, existen tres posibilidades:

(1) MAC1, MAC2 y MAC3 son todas diferentes.

Como se muestra mediante “22” en la FIG. 3, en este caso, no se lleva a cabo una comprobación óptima y se mantiene la dirección MAC1 en la entrada ARP, y se ignoran MAC2 y MAC3. El indicador de actualización de la entrada ARP se cambia a 0. La entrada ARP no se actualiza y se sigue utilizando como una entrada normal. El indicador también indica que la entrada ARP es actualizable.

(2) MAC1 y MAC3 son iguales.

Como se muestra mediante “23” en la FIG. 3, en este caso se puede llevar a cabo una comprobación óptima. Se mantiene la dirección MAC1 en la entrada ARP y se considera como la entrada ARP óptima y MAC2 se ignora (lo cual indica que MAC2 es una dirección de suplantación). El indicador de actualización se cambia a 2. Se bloquea la entrada ARP óptima de modo que no se actualice antes de su caducidad.

(3) MAC2 y MAC3 son iguales.

Como se muestra mediante “23” en la FIG. 3, en este caso se puede llevar a cabo una comprobación óptima. Se actualiza la dirección MAC maestra en la entrada ARP a MAC2 (lo cual indica que MAC1 es una dirección de suplantación) y se considera como la entrada ARP óptima y se actualiza la entrada ARP en el plano de reenvío. El indicador de actualización se cambia a 2. Se bloquea la entrada ARP óptima de modo que no se actualice antes de su caducidad.

Además, antes de que la entrada ARP óptima caduque, se envía una petición ARP, y el indicador de actualización se fija a 0, tal como se muestra mediante “24” en la FIG. 3. El indicador indica que se puede iniciar una nueva actualización.

Se puede configurar un contador para la entrada ARP con el fin de evitar el consumo excesivo de recursos de CPU provocados por el envío de demasiados mensajes de verificación por parte de una pasarela en el caso de ataques masivos de suplantación de direcciones. Cuando el número de procesos de verificación con respecto a la entrada alcanza un número dado dentro de un ciclo de vida de la entrada, no se inicia una nueva verificación con respecto a la entrada de modo que se preservan los recursos del dispositivo.

Aquellos experimentados en la técnica entienden que todos o una parte de los pasos en los modos de realización anteriores se pueden completar utilizando un hardware que siga las instrucciones de un programa. El programa puede ser almacenado en un medio de almacenamiento legible por un ordenador y cuando se ejecuta, se ejecutan los siguientes pasos:

Cuando la entrada ARP es actualizable, comprobar si la dirección MAC de un mensaje ARP recibido es la misma que la dirección MAC de una entrada ARP, donde el mensaje ARP tiene la misma dirección IP que la entrada ARP.

Si las direcciones MAC son diferentes, considerar el mensaje ARP recibido como un mensaje ARP ambiguo e iniciar un proceso de verificación ARP; o en caso contrario, no iniciar un proceso de verificación ARP.

El medio de almacenamiento puede ser una memoria de solo lectura, un disco magnético o un disco compacto.

Como conclusión, los modos de realización de la presente invención pueden reducir las interacciones de señalización y preservar recursos de red. Además, los ataques de suplantación que puedan ocurrir en cualquier momento se pueden denegar y se evita de forma efectiva una suplantación de direcciones mediante un barrido aleatorio con el fin de proteger la utilización normal del servidor real. Con los modos de realización de la presente invención, en el caso de ataques masivos de suplantación de direcciones no se consumen recursos de CPU excesivos cuando un dispositivo de red envía demasiados mensajes de verificación de modo que se preservan los recursos del dispositivo.

Aunque la invención se ha descrito mediante varios ejemplos de modos de realización, la invención no se encuentra limitada por dichos modos de realización.

REIVINDICACIONES

1. Un método para defenderse frente a ataques de suplantación del Protocolo de resolución de Direcciones, ARP, que comprende:

cuando una entrada ARP es actualizable, comprobar si una dirección del Control de Acceso al Medio (MAC) en un mensaje ARP recibido es la misma que una dirección MAC en la entrada ARP, donde el mensaje ARP tiene la misma dirección del Protocolo de Internet, IP, que la entrada ARP; y

si las direcciones MAC son diferentes, determinar (11) que el mensaje ARP recibido es un mensaje ARP ambiguo e iniciar (12) un proceso de verificación ARP;

en donde el inicio del proceso de verificación ARP comprende:

enviar una petición de verificación ARP a la dirección IP en la entrada ARP;

recibir una respuesta a la verificación ARP procedente de la dirección IP; caracterizado por

realizar una comprobación de la verificación en función de la dirección MAC en la respuesta a la verificación ARP;

en donde la realización de la comprobación de verificación de acuerdo con la dirección MAC en la respuesta a la verificación ARP comprende:

comparar la dirección MAC en la respuesta a la verificación ARP, la dirección MAC en la entrada ARP y la dirección MAC en el mensaje ARP ambiguo;

si la dirección MAC en la respuesta a la verificación ARP es la misma que una de las otras dos direcciones MAC, realizar una comprobación óptima, en donde la comprobación óptima consiste en tomar la entrada ARP que tiene dicha misma dirección MAC como una entrada ARP óptima y bloquear la entrada ARP óptima; y

si la dirección MAC en la respuesta a la verificación ARP es diferente de las otras dos direcciones MAC, mantener la entrada ARP sin realizar una comprobación óptima,

en donde el bloqueo de la entrada ARP óptima comprende:

configurar la entrada ARP óptima para que no se pueda actualizar de modo que la entrada ARP óptima no se actualice antes de que caduque.

2. El método de la reivindicación 1, en el que el inicio del proceso de verificación ARP comprende, además:

configurar la entrada ARP de modo que la entrada únicamente acepte la actualización procedente de una respuesta a la verificación ARP.

3. El método de una cualquiera de las reivindicaciones 1 ó 2, que comprende, además:

establecer un contador con respecto a la entrada ARP y no iniciar un proceso de verificación para la entrada ARP cuando el número de verificaciones ARP alcance un valor de contador especificado dentro de un ciclo de vida de la entrada.

4. Un equipo para defenderse frente a ataques de suplantación del Protocolo de resolución de Direcciones, ARP, que comprende:

una unidad de comprobación de recepción, configurada para: cuando una entrada ARP es actualizable, comprobar si una dirección del Control de Acceso al Medio, MAC, en un mensaje ARP recibido es la misma que una dirección MAC en la entrada ARP, donde el mensaje ARP tiene la misma dirección del Protocolo de Internet, IP, que la entrada ARP, y si las direcciones MAC son diferentes, considerar el mensaje ARP recibido como un mensaje ARP ambiguo y enviar un resultado de la comprobación a una unidad de verificación; y

la unidad de verificación, configurada para: iniciar un proceso de verificación ARP de acuerdo con el resultado de la comprobación procedente de la unidad de comprobación de recepción, enviar una petición de verificación ARP a la dirección IP en la entrada ARP; y

recibir una verificación ARP procedente de la dirección IP, caracterizado por

una unidad de comparación, configurada para comparar la dirección MAC en la respuesta a la verificación ARP, la dirección MAC en la entrada ARP y la dirección MAC en el mensaje ARP ambiguo después de que la unidad de verificación inicie el proceso de verificación ARP;

si la dirección MAC en la respuesta a la verificación ARP es la misma que una de las dos otras direcciones MAC, configurada para realizar una comprobación óptima, en donde la comprobación óptima consiste en tomar la entrada ARP que tiene dicha misma dirección MAC como una entrada ARP óptima; y

si la dirección MAC en la respuesta a la verificación ARP es diferente de las otras dos direcciones MAC, configurada para no realizar una comprobación óptima, y

una unidad de realización de la comprobación, configurada para establecer que la entrada ARP óptima no sea actualizable de tal modo que la entrada ARP óptima no se actualice antes de su caducidad si la unidad de comparación realiza una comprobación óptima; y si la unidad de comparación no realiza una comprobación óptima, configurada para mantener la entrada ARP.

5. El equipo de la reivindicación 4, que comprende, además:

una unidad de control de un contador, configurada para: establecer un contador con respecto a la entrada ARP y cuando el número de verificaciones ARP alcanza un valor de contador especificado dentro de un ciclo de vida de la entrada ARP, controlar que la unidad de verificación no inicie un proceso de verificación para la entrada ARP.

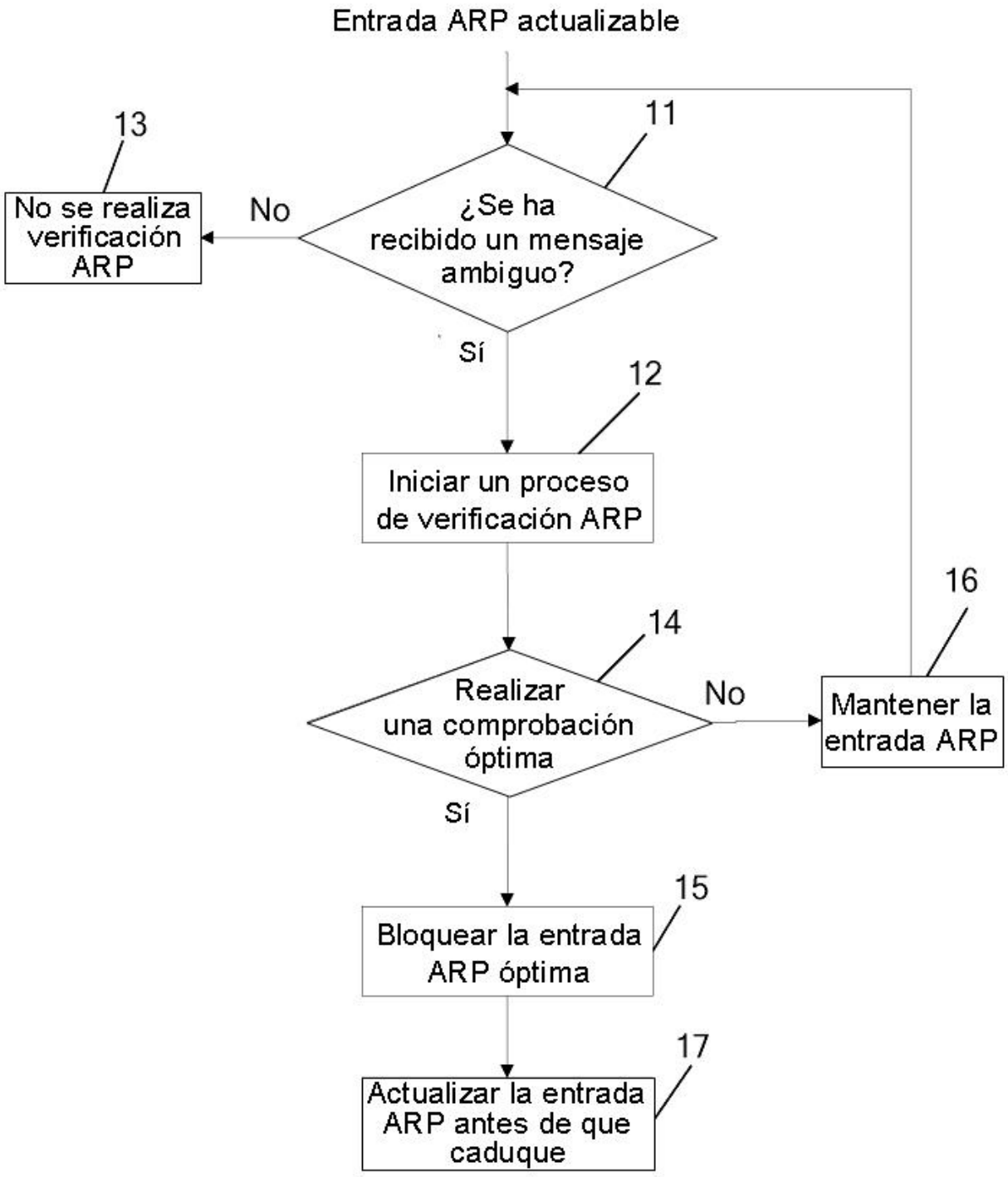
Entrada ARP actualizable
11
¿Se ha recibido un mensaje ambiguo?
No
13
No se realiza verificación ARP
Sí
12
Iniciar un proceso de verificación ARP
14
Realizar una comprobación óptima
No
16
Mantener la entrada ARP
Sí
15
Bloquear la entrada ARP óptima
17
Actualizar la entrada ARP antes de que caduque

FIG. 1

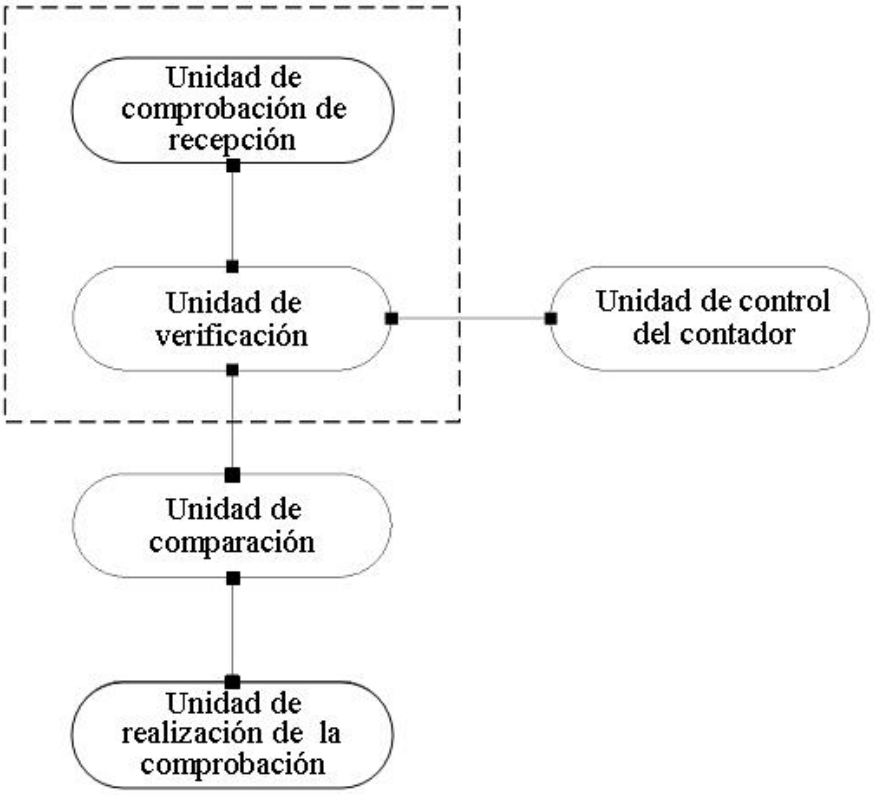
Unidad de comprobación de recepción
Unidad de verificación
Unidad de control del contador
Unidad de comparación
Unidad de realización de la comprobación

FIG. 2

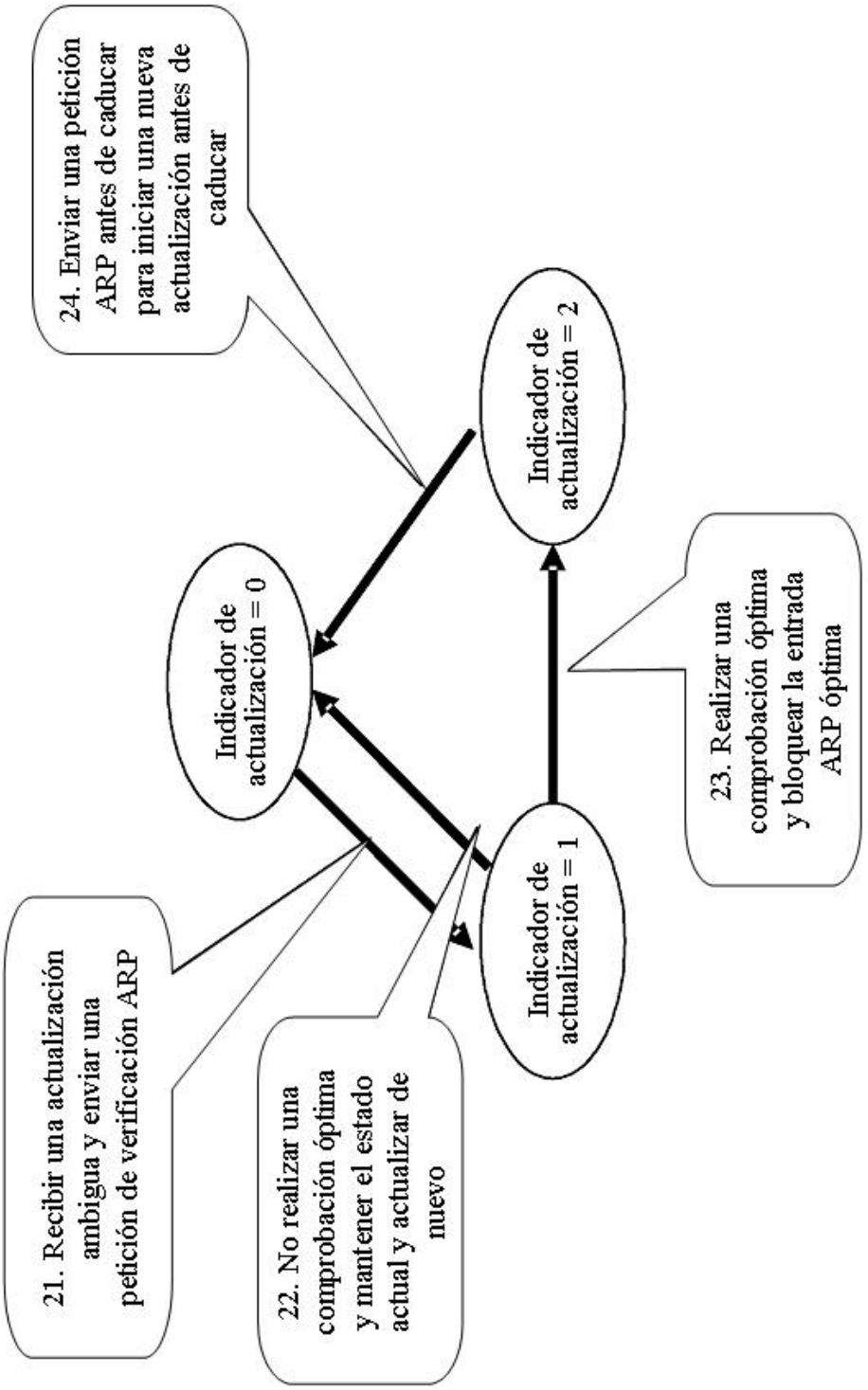
24. Enviar una petición ARP antes de caducar para iniciar una nueva actualización antes de caducar
Indicador de actualización = 2
Indicador de actualización = 0
23. Realizar una comprobación óptima y bloquear la entrada ARP óptima
21. Recibir una actualización ambigua y enviar una petición de verificación ARP
22. No realizar una comprobación óptima y mantener el estado actual y actualizar de nuevo
Indicador de actualización = 1

FIG. 3