(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 358 811**

(51) Int. Cl.:
H04L 29/12 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06740671 .0**
(96) Fecha de presentación : **04.04.2006**
(97) Número de publicación de la solicitud: **1867141**
(97) Fecha de publicación de la solicitud: **19.12.2007**

(54) Título: **Uso de una consulta de prueba para determinar si un dispositivo de red tiene un error de software o un fallo de diseño.**

(30) Prioridad: **04.04.2005 US 98135**

(45) Fecha de publicación de la mención BOPI:
13.05.2011

(45) Fecha de la publicación del folleto de la patente:
13.05.2011

(73) Titular/es: **APPLE Inc.**
1 Infinite Loop
Cupertino, California 95014, US

(72) Inventor/es: **Graessley, Joshua, V. y**
Cheshire, Stuart, D.

(74) Agente: **Fàbrega Sabaté, Xavier**

DESCRIPCIÓN

Uso de una consulta de prueba para determinar si un dispositivo de red tiene un error de software o un fallo de diseño

ANTECEDENTES

Técnica relacionada

Con el fin de participar en una red de protocolo de Internet (IP), un nodo de red, tal como un ordenador o una impresora, necesita configurarse con una dirección IP. Además, con el fin de comunicarse con otro dispositivo utilizando IP sobre Ethernet o un medio similar, el nodo de red necesita la capacidad de convertir una dirección IP para el dispositivo en la dirección de hardware correspondiente (por ejemplo, Ethernet) para el dispositivo. El protocolo de resolución de direcciones (ARP) soluciona este problema de conversión proporcionando un mecanismo de resolución de direcciones que determina la dirección de hardware para una dirección IP dada, permitiendo de ese modo que un nodo de red participe en una red IP.

Las direcciones IP pueden configurarse o bien manualmente por el usuario, o automáticamente con la ayuda de otro nodo de red, tal como un servidor DHCP. Desafortunadamente, es posible que un servidor DHCP no esté siempre disponible. Además, para el usuario resulta engorroso configurar una dirección IP. Por lo tanto, existe una gran necesidad de un mecanismo de configuración mediante el cual un nodo de red pueda configurar automáticamente una red IP por sí mismo.

El direccionamiento de enlace local IPv4 (norma RFC 3927) proporciona un mecanismo de configuración de este tipo. En el direccionamiento de enlace local IPv4, un mecanismo de configuración en un nodo de red elige de manera aleatoria una dirección IP "candidata" en un intervalo especificado de direcciones de enlace local y envía una solicitud ARP para comprobar si la dirección IP candidata de enlace local es única dentro del alcance del enlace. Si la dirección IP candidata de enlace local ya está utilizándose por otro nodo de red, entonces el mecanismo de configuración elige otra dirección IP de enlace local y comprueba si es única. Una vez que el mecanismo de configuración encuentre una dirección IP de enlace local única, el nodo de red la utiliza para comunicarse con otros nodos de la red.

Desafortunadamente, algunos enrutadores de red no están configurados correctamente para responder a todas las solicitudes ARP, incluyendo solicitudes ARP para cualquier dirección IP de enlace local. Si un enrutador de este tipo está acoplado a una red local, puede interferir en el mecanismo de configuración respondiendo a solicitudes ARP enviadas por el mecanismo de configuración, haciendo parecer que cada posible dirección única ya está utilizándose. Esto puede impedir que el mecanismo de configuración seleccione una dirección IP.

Por ejemplo, la FIG. 1 ilustra cómo un enrutador puede interferir en el proceso de asignación de una dirección IP. Durante el funcionamiento, el nodo A selecciona una dirección IP candidata (etapa 102). A continuación, el nodo A sondea la dirección IP candidata llevando a cabo una solicitud ARP (etapa 104). Después, el enrutador que interfiere responde a la solicitud ARP (etapa 106). Esto hace al nodo A determinar que otro nodo ya tiene la dirección IP y seleccionar una dirección IP candidata diferente (etapa 108). Después, el sistema vuelve a la etapa 104 y el proceso se repite indefinidamente. Por consiguiente, el nodo A no puede asignar una dirección IP.

Debe observarse que si un enrutador de este tipo está configurado para ignorar las "sondas" ARP enviadas por un dispositivo que está intentando asignar una dirección IP de enlace local, el enrutador puede interferir aún en las solicitudes ARP normales (que no son de tipo sonda) que se envían para determinar una dirección de Ethernet asociada con una dirección IP.

Por ejemplo, la FIG. 2 ilustra cómo un enrutador puede interferir en solicitudes ARP normales. En primer lugar, un nodo A envía una solicitud ARP con la dirección IP de un dispositivo con el que el nodo A desea comunicarse (etapa 202). A continuación, un enrutador responde incorrectamente a la solicitud ARP, interfiriendo en la respuesta procedente del dispositivo real con el que el nodo A desea comunicarse (etapa 204). Esto hace que el nodo A obtenga una dirección de Ethernet errónea. Los paquetes IP se envían posteriormente al enrutador en lugar de al dispositivo deseado, donde se pierden ya que el enrutador o bien los reenvía incorrectamente o simplemente los descarta sin reenviarlos.

Por lo tanto, lo que se necesita es un procedimiento y un aparato para tratar los problemas descritos anteriormente encontrados durante la ejecución de solicitudes ARP.

En un problema relacionado, los proveedores de servicios de Internet (ISP) proporcionan normalmente una única dirección de protocolo de Internet (IP) por cuenta de conexión a Internet, lo que puede implicar convencionalmente que solo un dispositivo habilitado para Internet por cuenta pueda acoplarse a la red del ISP en un momento dado. Esto no es deseable, ya que actualmente muchos hogares tienen varios ordenadores y otros dispositivos habilitados para Internet que el consumidor puede desear tener conectados a la red del ISP simultáneamente.

Una solución común a este problema de compartición de conexiones a Internet es utilizar un dispositivo de conversión de direcciones de red (NAT) (denominado comúnmente como “pasarela doméstica”) para compartir una única dirección IP con múltiples dispositivos habilitados para Internet que están acoplados a la pasarela doméstica a través de una red de área local (LAN). El dispositivo de pasarela doméstica tiene normalmente al menos dos interfaces físicas y dos direcciones de Internet: una pública que se utiliza para comunicaciones con la red del ISP, y otra interna privada que se utiliza para comunicaciones con los dispositivos de la LAN. Desde el punto de vista de un observador externo, todos los ordenadores locales y otros dispositivos habilitados para Internet del consumidor adoptan la apariencia de un único dispositivo con una única dirección IP pública.

Si la pasarela doméstica está configurada para ofrecer un servicio de protocolo de configuración dinámica de anfitrión (DHCP) a los dispositivos del consumidor, la pasarela doméstica asigna normalmente una dirección IP privada a cada dispositivo habilitado para Internet acoplado a la pasarela doméstica. La pasarela doméstica también proporciona su propia dirección IP LAN a estos dispositivos habilitados para Internet como la pasarela por defecto a la que deben enviar paquetes IP salientes y como el servidor DNS por defecto al que deben enviar consultas DNS. Puesto que normalmente la pasarela doméstica no tiene, por sí misma, autorización para ningún dominio DNS, todo lo que hace con las consultas DNS recibidas es reenviarlas a un servidor DNS más reconocible situado en alguna otra ubicación, normalmente uno controlado por el ISP del cliente.

Cuando se comunica con servicios de Internet, un dispositivo cliente envía paquetes IP a través de la pasarela doméstica. La pasarela doméstica reescribe la dirección IP origen en cada paquete para que sea la dirección IP pública compartida común y después lo reenvía a través de la red del ISP a Internet. Durante este proceso, la pasarela doméstica lleva a cabo normalmente un seguimiento de qué paquete se envió por cuál dispositivo local habilitado para Internet, de manera que cuando el (los) paquete(s) de respuesta vuelvan de Internet a través de la red del ISP a la pasarela doméstica, la pasarela doméstica pueda enrutar estos paquetes de respuesta al dispositivo apropiado habilitado para Internet que originó el paquete de solicitud saliente correspondiente.

Por ejemplo, la FIG. 3 ilustra una pasarela doméstica 304 que está acoplada tanto a una red 302 como a una red local 306. La red local 306 acopla la pasarela doméstica 304 a ordenadores 308, 310 y 312 y al dispositivo de Ethernet 314.

Una pasarela doméstica (o cualquier otro dispositivo de compartición de Internet) tal como la pasarela doméstica 304, incluye normalmente un mecanismo para reenviar consultas DNS a servidores DNS que puedan proporcionar respuestas a las consultas DNS. Este mecanismo permite a la pasarela doméstica 304 funcionar como el "servidor DNS configurado" por defecto para todos los dispositivos de la red local 306.

Debe observarse que un “servidor DNS configurado” puede incluir cualquier dispositivo habilitado para DNS que pueda devolver una respuesta a una consulta DNS, tal como (1) un servidor DNS con autoridad, (2) un servidor DNS recursivo, y (3) un servidor DNS de reenvío. Un servidor DNS con autoridad contesta consultas DNS dirigidas a un dominio o a un conjunto de dominios que han sido delegados al servidor DNS con autoridad. Al hacer esto, el servidor DNS con autoridad mantiene registros DNS para el dominio delegado o conjunto de dominios delegados, y es el único tipo de servidor DNS que puede responder con autoridad para el dominio delegado o conjunto de dominios delegados.

Un servidor DNS recursivo (una caché DNS) recibe consultas DNS y lleva a cabo consultas para buscar el dominio solicitado. Cuando se recibe una respuesta desde un servidor DNS con autoridad o desde otro servidor DNS recursivo, el servidor DNS recursivo almacena la respuesta en su caché DNS local. Si se lleva a cabo una consulta para un registro DNS que ya estaba almacenado previamente en

la caché DNS local, el servidor DNS recursivo utiliza la información almacenada para contestar a la consulta DNS en lugar de llevar a cabo otra consulta DNS.

Un servidor DNS de reenvío (un retransmisor DNS) reenvía consultas DNS a un servidor DNS recursivo o a un servidor DNS con autoridad. Tal y como se ha mencionado anteriormente, las pasarelas domésticas contienen normalmente retransmisores DNS simples que funcionan como el "servidor DNS configurado" para dispositivos locales que se comunican a través de la pasarela doméstica.

Aunque algunas pasarelas domésticas son capaces normalmente de permitir que múltiples dispositivos habilitados para Internet compartan una única conexión a Internet de manera satisfactoria, algunas de estas pasarelas domésticas tienen errores de software o fallos de diseño similares. Uno de estos fallos provoca que la pasarela doméstica maneje incorrectamente el reenvío de consultas DNS válidas a servidores DNS. Además, tales pasarelas domésticas defectuosas pueden bloquearse y dejar de funcionar completamente durante el procesamiento de determinadas consultas DNS válidas, afectando por tanto a la capacidad de llevar a cabo su función prevista, en concreto proporcionar acceso a Internet a ordenadores locales y a dispositivos similares habilitados para Internet.

El documento US 5.708.654 divulga un procedimiento que utiliza un instrumento de prueba LAN para detectar agentes ARP proxy y enrutadores mal configurados en una LAN TCP/IP. El procedimiento permite en primer lugar la detección de enrutadores implementando ARP proxy para el enrutador por defecto emitiendo un único comando ARP para un único anfitrión remoto. Puesto que la dirección IP destino elegida como un dispositivo único no existente, el enrutador responderá a la solicitud ARP con una respuesta ARP proxy para su ruta por defecto si esta función está habilitada. El procedimiento permite además distinguir entre respuestas procedentes de dispositivos reales que tienen direcciones IP duplicadas y respuestas procedentes de enrutadores mal configurados que responden en ARP proxy para ordenadores centrales locales. Las direcciones IP duplicadas falsas debidas a respuestas ARP proxy pueden identificarse como entradas fantasma en una base de datos, pudiendo entonces etiquetarse o eliminarse de manera apropiada para mostrar al usuario del instrumento de prueba LAN solamente las entradas que corresponden a dispositivos físicos reales.

Por lo tanto, lo que se necesita es un procedimiento y un aparato para que un cliente de la red local determine si su servidor DNS tiene este error de software conocido particular, de manera que el cliente pueda determinar cuándo debe evitar llevar a cabo aquéllas determinadas consultas DNS válidas que se sabe que tienen una alta probabilidad de bloquear ese dispositivo particular.

RESUMEN

Una forma de realización de la presente invención proporciona un sistema que detecta un enrutador no compatible que responde incorrectamente a todas las solicitudes de protocolo de resolución de direcciones (ARP), incluyendo solicitudes ARP para direcciones IP de enlace local. Se permite a un enrutador responder a solicitudes ARP para una dirección de enlace local IPv4 única que haya reivindicado correctamente para su propio uso legítimo (por ejemplo, bajo el protocolo especificado en la norma RFC 2937 del Grupo de Trabajo de Redes), pero no es correcto que responda indiscriminadamente a solicitudes ARP para cada dirección de enlace local IPv4.

Según un primer aspecto de la invención, se proporciona un procedimiento como el definido en la reivindicación 1.

En una variación de esta forma de realización, la sonda ARP se envía por un dispositivo solicitante que esté en el proceso de asignarse una dirección IP candidata de enlace local.

En una variación de esta forma de realización, si la solicitud ARP con la dirección IP reservada de enlace local no se ha respondido, el dispositivo solicitante asigna la dirección IP candidata de enlace local.

Según un segundo aspecto de la invención, se proporciona un medio de almacenamiento legible por ordenador como el definido en la reivindicación 4.

Según un tercer aspecto de la invención, se proporciona un aparato como el definido en la reivindicación 7.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La FIG. 1 presenta un diagrama de flujo que ilustra cómo un enrutador puede interferir en el proceso de asignación de una dirección IP.

La FIG. 2 presenta un diagrama de flujo que ilustra cómo un enrutador puede interferir en una solicitud ARP normal.

La FIG. 3 ilustra un sistema informático interconectado según una forma de realización de la presente invención.

La FIG. 4 presenta un diagrama de flujo que ilustra el proceso de asignar una dirección IP según una forma de realización de la presente invención.

La FIG. 5 presenta un diagrama de flujo que ilustra el proceso de realizar una solicitud ARP según una forma de realización de la presente invención.

La FIG. 6 presenta un diagrama de flujo que ilustra el proceso de determinar si un servidor DNS tiene un error de software conocido particular o un fallo de diseño similar según una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA

La siguiente descripción se presenta para permitir que cualquier experto en la técnica haga y utilice la invención, y se proporciona en el contexto de una aplicación particular y de sus requisitos.

Las estructuras de datos y el código descritos en esta descripción detallada están almacenados normalmente en un medio de almacenamiento legible por ordenador, que puede ser cualquier dispositivo o medio que puede almacenar código y/o datos para su utilización por parte de un sistema informático. Esto incluye, pero sin limitarse a, dispositivos de almacenamiento magnéticos y ópticos, tales como unidades de disco, cintas magnéticas, CD (discos compactos) y DVD (discos versátiles digitales o discos de vídeo digital), y señales de instrucciones informáticas contenidas en un medio de transmisión (con o sin una onda portadora según la cual se modulan las señales). Por ejemplo, el medio de transmisión puede incluir una red de comunicaciones, tal como una LAN, una WAN o Internet.

Sistema informático interconectado

La FIG. 3 ilustra un sistema informático interconectado 300 según una forma de realización de la presente invención. El sistema informático interconectado 300 incluye una red local 306 que acopla entre sí ordenadores 308, 310 y 312, un enrutador 304 y un dispositivo de Ethernet 314. La red local 306 puede incluir cualquier tipo de red informática, tal como una Ethernet. Los ordenadores 308, 310 y 312 pueden incluir cualquier tipo de dispositivo de red que pueda llevar a cabo una solicitud ARP. El dispositivo de Ethernet 314 puede incluir cualquier tipo de dispositivo (tal como una impresora) con el que un nodo (tal como el ordenador 308) desee comunicarse.

El enrutador 304 es un dispositivo que acopla la red local 306 a una red 302, tal como Internet. Sin embargo, en este sistema, el enrutador 304 es un enrutador “no compatible” que posiblemente puede interferir en las solicitudes ARP llevadas a cabo por un ordenador 308. Por ejemplo, el enrutador 304 puede interferir en las sondas ARP llevadas a cabo durante el proceso de asignación de una dirección IP de enlace local, o en solicitudes ARP llevadas a cabo para identificar una dirección de Ethernet asociada con una dirección IP, tal como una dirección IP para el dispositivo de Ethernet 314.

Esta interferencia puede tratarse tal y como se describe a continuación con referencia a las FIG. 4 y 5.

Proceso de asignación de una dirección IP

La FIG. 4 presenta un diagrama de flujo que ilustra el proceso de asignación de una dirección IP según una forma de realización de la presente invención. El proceso comienza cuando un nodo A selecciona una dirección IP candidata para ser asignada (etapa 402). A continuación, el nodo A genera una sonda ARP inicial para la dirección IP candidata (etapa 404) y espera una respuesta (etapa 406).

Si no hay respuesta a la sonda ARP inicial, la dirección IP candidata no está asignada a ningún dispositivo. En este caso, el sistema asigna la dirección IP candidata, normalmente a una de sus interfaces (etapa 416). En este momento finaliza el proceso de asignación de la dirección IP.

Si hay una respuesta, el nodo A genera una segunda sonda ARP para una dirección IP reservada de enlace local, la cual no debe estar asignada a ningún dispositivo, tal como la dirección de transmisión 169.254.255.255 y/o 169.254.0.0 (etapa 408). Si no hay respuesta a esta segunda sonda ARP, el sistema deduce que ningún enrutador está respondiendo a las solicitudes ARP para direcciones IP de enlace local. Por lo tanto, la respuesta a la sonda ARP inicial indica de manera válida que la dirección IP candidata ya está asignada a otro dispositivo. En este caso, el sistema selecciona una nueva dirección IP candidata (etapa 412) y vuelve a la etapa 404 para sondear la nueva dirección IP candidata.

Por otro lado, si hubo una respuesta a la segunda sonda ARP en la etapa 410, el sistema deduce que un enrutador está respondiendo incorrectamente a direcciones IP de enlace local. En este caso, el sistema pone la dirección origen de la respuesta en una lista negra para ignorar respuestas posteriores procedentes de la dirección origen (etapa 416). Después, el sistema vuelve a la etapa 404 para sondear de nuevo la dirección candidata.

Debe observarse que una sonda ARP (que se utiliza para probar una dirección IP candidata) puede diferenciarse de una solicitud ARP normal ya que la dirección origen de una sonda ARP es todo ceros. Por lo tanto, es posible que un enrutador pueda estar configurado correctamente para no responder a sondas ARP y, con todo, responder incorrectamente a solicitudes ARP normales. En este caso, el enrutador no interferirá en las sondas ARP durante el proceso de asignación de direcciones IP pero, en cambio, puede interferir en las solicitudes ARP normales, en las que un nodo busca determinar una dirección de Ethernet asociada con una dirección IP válida de enlace local. Este problema puede tratarse mediante el proceso descrito a continuación con referencia a la FIG. 5.

Proceso de ejecución de una solicitud ARP

La FIG. 5 presenta un diagrama de flujo que ilustra el proceso de llevar a cabo una solicitud ARP según una forma de realización de la presente invención. El proceso comienza cuando el código IP de un nodo A solicita una dirección de Ethernet para una dirección IP deseada (etapa 502). A continuación, el sistema determina si (a) ésta será la primera solicitud ARP de enlace local en esta interfaz para la red ya que la interfaz se habilitó, o (b) ha pasado más de un periodo de tiempo desde que el sistema comprobó por última vez un enrutador no compatible en este enlace (etapa 504). Si no, el sistema lleva a cabo solicitudes ARP para la dirección de la manera habitual para determinar la dirección de Ethernet para la dirección IP deseada (etapa 512).

Por otro lado, si en la etapa 504 el sistema determina que ésta será la primera solicitud ARP de enlace local en la interfaz, o que es momento de volver a comprobar esta interfaz, el sistema comprueba en primer lugar si hay un enrutador que esté respondiendo indiscriminadamente a solicitudes ARP en la red asociada a la interfaz. Esto implica enviar una solicitud ARP inicial en la red para una dirección que no debe estar asignada a ningún nodo (tal y como se ha descrito anteriormente) (etapa 506). Después, el sistema espera una respuesta (etapa 508). Si no hay ninguna respuesta, el sistema deduce que ningún enrutador está respondiendo indiscriminadamente a solicitudes ARP de enlace local en la red. En este caso, el sistema lleva a cabo solicitudes ARP para la dirección IP deseada de la manera habitual (etapa 512).

Por otro lado, si hay una respuesta a la solicitud ARP, el sistema deduce que un enrutador está respondiendo indiscriminadamente a direcciones IP de enlace local. En este caso, el sistema pone la dirección origen de la respuesta en una lista negra para ignorar respuestas posteriores procedentes de esa dirección origen (etapa 510) cuando pertenecen a direcciones IP de enlace local. Después, el sistema avanza hasta la etapa 512 y lleva a cabo solicitudes ARP para la dirección IP deseada de la manera habitual.

Servidor DNS defectuoso

Algunos servidores DNS que residen en pasarelas domésticas son defectuosos y pueden producir respuestas incorrectas o pueden provocar que la pasarela doméstica se bloquee. (Debe observarse que un servidor DNS puede incluir cualquier dispositivo habilitado para DNS, incluyendo un servidor DNS, un retransmisor DNS o una caché DNS). Tales servidores DNS defectuosos suponen que si un cliente lleva a cabo una consulta DNS de tipo PTR, la única solicitud posible que el cliente está haciendo es llevar a cabo una consulta DNS de “búsqueda inversa” IPv4, traduciendo desde una dirección IP a un nombre.

Un ejemplo de una consulta de nombre de dominio de “búsqueda inversa” IPv4 formada correctamente

es “2.1.168.192.in-addr.arpa”. Esta consulta y otras parecidas pueden llevarse a cabo mediante software o mediante el usuario con una utilidad DNS tal como “*nslookup*”. El comando *nslookup* y los argumentos para este ejemplo son:

> “nslookup -q=ptr 2.1.168.192.in-addr.arpa”. En este ejemplo, el tipo de consulta DNS es PTR y la consulta DNS es “2.1.168.192.in-addr.arpa”. Debe observarse que una consulta PTR es normalmente una consulta DNS de “búsqueda inversa” que lleva a cabo una correlación de una dirección IP con un nombre de dominio correspondiente. Sin embargo, otras consultas DNS formadas correctamente son posibles incluso aunque no tengan sentido. Por ejemplo, la consulta DNS de tipo PTR "2.1.168.192.nonsense" es una consulta DNS formada correctamente, pero no genera ningún registro de respuesta ya que el dominio de nivel superior "nonsense" no existe realmente. Debe observarse que el dominio “in-addr.arpa” es el sufijo de dominio adecuado a utilizar cuando se lleve a cabo una consulta DNS de “búsqueda inversa”.

Algunas pasarelas domésticas defectuosas examinan solamente las cuatro primeras etiquetas de la consulta DNS de tipo PTR ("etiquetas" en un nombre de dominio son los grupos de caracteres separados por puntos) e ignoran el resto del nombre. En "2.1.168.192.nonsense”, por ejemplo, las cuatro primeras etiquetas son "2.1.168.192.". Por lo tanto, para estas pasarelas domésticas defectuosas, la consulta DNS de tipo PTR “2.1.168.192.nonsense” no puede distinguirse de la consulta DNS de tipo PTR “2.1.168.192.in-addr.arpa”.

También debe observarse que estas mismas pasarelas domésticas defectuosas suponen que las cuatro primeras etiquetas son números decimales entre 0 y 255. Si las cuatro primeras etiquetas de la consulta DNS de tipo PTR no son números entre 0 y 255, estas pasarelas domésticas defectuosas se bloquean.

Detectar un enrutador de Internet defectuoso

Una forma de realización de la presente invención detecta tales pasarelas domésticas defectuosas llevando a cabo una consulta DNS especial que se genera para detectar la existencia de un fallo en el servidor DNS sin bloquearlo.

Por ejemplo, la consulta especial que detecta un fallo en el servidor DNS de la pasarela doméstica es la consulta DNS de tipo PTR "2.1.168.192.nonsense", que produce una respuesta NXDOMAIN (es decir, el dominio no existe) en una pasarela doméstica que funciona correctamente sin el fallo. Sin embargo, pasarelas domésticas con servidores DNS defectuosos intentarán proporcionar un nombre de anfitrión como respuesta a la consulta 2.1.168.192.nonsense, incluso aunque la consulta no fuera en realidad una consulta de búsqueda de nombre "in-addr-arpa".

Desafortunadamente, la consulta DNS de tipo PTR “2.1.168.192.nonsense”, cuando está dirigida a un servidor DNS sin el fallo mencionado anteriormente, provoca que se envíe una consulta DNS a uno de los servidores de nombre raíz DNS. Puesto que en general la única manera de que un servidor o un retransmisor DNS sepan si existe o no un dominio de nivel superior particular es interrogar a uno de los servidores de nombre raíz, cada consulta de prueba de este tipo da posiblemente como resultado el envío de una consulta de molestias a los servidores de nombre raíz.

En una forma de realización de la presente invención, la consulta especial se genera de manera que el servidor DNS no se comunique con un servidor de nombre raíz DNS tanto exista el fallo como si no.

Por ejemplo, la consulta especial puede ser "1.0.0.127.dnsbugtest.1.0.0.127.in-addr-arpa”. En esta consulta a modo de ejemplo, la dirección "127.0.0.1" es la "dirección de bucle". La dirección de bucle es una dirección IP especial disponible para utilizarse cuando dos fragmentos de software de red de la misma máquina desean comunicarse entre sí utilizando mecanismos de interconexión IP e interfaces de programación, independientemente de si una interconexión IP (entre máquinas) convencional está disponible.

También debe observarse que cada servidor DNS debe contener un registro DNS fijo que correlacione "1.0.0.127.in-addr.arpa" con el nombre "*localhost*". Por lo tanto, cualquier nombre que sea subdominio del nombre “1.0.0.127.in-addr.arpa” está formado correctamente y es válido, pero son nombres que se sabe que no tienen registros DNS asociados. Dicho de otro modo, "1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa" es un nombre legal, pero cualquier consulta para ese nombre no debe proporcionar ningún resultado. Por lo tanto, una pasarela doméstica con un servidor DNS que funciona correctamente devuelve una respuesta NXDOMAIN (es decir, el nombre del dominio no existe) sin tener que

comunicarse con un servidor de nombre raíz DNS para hacer tal determinación.

Debe observarse que puesto que las seis últimas etiquetas en esta consulta DNS de tipo PTR son “1.0.0.127.in-addr.arpa”, una pasarela doméstica con un servidor DNS que funciona correctamente no reenviará la consulta DNS al servidor de nombre raíz DNS ya que el servidor DNS de la pasarela doméstica sabe que la dirección IP es un subdominio de la dirección de bucle. Puesto que los subdominios de la dirección de bucle no se utilizan, el servidor DNS debe responder con una respuesta NXDOMAIN sin comunicarse con un servidor de nombre raíz DNS.

Asimismo, una pasarela doméstica con el fallo para cuya detección se genera la consulta especial, no se comunica con un servidor de nombre raíz DNS. Debe recordarse que una pasarela doméstica con un servidor DNS defectuoso solo utiliza las cuatro primeras etiquetas de la consulta DNS de tipo PTR y que interpreta esta consulta DNS de tipo PTR como la consulta DNS de tipo PTR "1.0.0.127.in-addr-arpa". Puesto que el servidor DNS de la pasarela doméstica defectuosa sabe que la respuesta correcta para una consulta DNS de tipo PTR para “1.0.0.127.in-addr.arpa” debe ser “*localhost*”, la pasarela doméstica devuelve la respuesta “*localhost*” sin comunicarse con ningún servidor de nombre raíz DNS.

La FIG. 6 presenta un diagrama de flujo que ilustra el proceso de determinar si un servidor DNS es defectuoso según una forma de realización de la presente invención. El proceso comienza cuando el sistema envía una consulta especial al servidor DNS (etapa 602). En una forma de realización de la presente invención, la consulta especial es la consulta DNS de tipo PTR "1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa".

A continuación, el sistema recibe una respuesta del servidor DNS (etapa 604). Si la respuesta es la correcta (etapa 606 - SÍ), el sistema determina que el servidor DNS no está defectuoso (etapa 612). En una forma de realización de la presente invención, la respuesta correcta es un código de error NXDOMAIN que indica que un nombre de dominio no existe.

Si la respuesta es incorrecta (etapa 606 - NO), el sistema determina que el servidor DNS está defectuoso (etapa 608) y lleva a cabo una acción correctiva (etapa 610).

En una forma de realización de la presente invención, la acción correctiva implica llevar a cabo etapas para evitar la ejecución de aquéllas determinadas consultas DNS válidas que se considera que tienen una alta probabilidad de bloquear ese dispositivo particular.

En una forma de realización de la presente invención, las consultas DNS válidas a evitar son aquéllas utilizadas por Wide-Area Bonjour, una tecnología de interconexión que permite a los clientes descubrir servicios de red en una red de área extensa.

Las anteriores descripciones de formas de realización de la presente invención se han presentado solamente para fines de ilustración y descripción. No pretenden ser exhaustivas o limitar la presente invención a las formas divulgadas. Por consiguiente, muchas modificaciones y variaciones resultarán evidentes a los expertos en la técnica. Además, la anterior descripción no pretende limitar la presente invención. El alcance de la presente invención está definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento para detectar un dispositivo (304) que responde incorrectamente a solicitudes del protocolo de resolución de direcciones, ARP, tal como un dispositivo (304) que responde incorrectamente a solicitudes ARP para direcciones IP de enlace local que no ha reivindicado correctamente para su propio uso legítimo, que comprende:

seleccionar (402) una dirección IP candidata de enlace local;

enviar (404) una primera sonda ARP para la dirección IP candidata de enlace local;

sólo si se ha recibido una respuesta a la primera sonda ARP, enviar (408) una segunda sonda ARP al dispositivo respondedor (304) solicitando una dirección de Ethernet asociada con una dirección IP reservada, en el que la dirección IP reservada es una dirección de transmisión de enlace local IPv4 169.254.255.255 o una dirección de enlace local IPv4 169.254.0.0, que no debe estar asignada a ningún dispositivo;

si se recibe una respuesta desde el dispositivo (304) a la segunda sonda ARP, poner (414) la dirección del dispositivo (304) en una lista negra asociada con un intervalo de direcciones IP de enlace local e ignorar respuestas ARP posteriores procedentes de las direcciones origen de la lista negra para el intervalo de direcciones de enlace local, de manera que se ignoren respuestas ARP posteriores del dispositivo (304) que pertenezcan a ese intervalo de direcciones.

2. El procedimiento según la reivindicación 1, en el que la primera sonda ARP se envía por un dispositivo solicitante (308) que está en el proceso de asignar una dirección IP candidata de enlace local.

3. El procedimiento según la reivindicación 2, en el que si no se recibe respuesta a la primera sonda ARP, el dispositivo solicitante (308) asigna (416) la dirección IP candidata de enlace local.

4. Un medio de almacenamiento legible por ordenador que almacena instrucciones que cuando se ejecutan por un ordenador hacen que el ordenador lleve a cabo un procedimiento para detectar un dispositivo (304) que responde incorrectamente a solicitudes del protocolo de resolución de direcciones, ARP, tal como un dispositivo (304) que responde incorrectamente a solicitudes ARP para direcciones IP de enlace local que no ha reivindicado correctamente para su propio uso legítimo, comprendiendo el procedimiento:

seleccionar (402) una dirección IP candidata de enlace local;

enviar (404) una primera sonda ARP para la dirección IP candidata de enlace local;

sólo si se ha recibido una respuesta a la primera sonda ARP, enviar (408) una segunda sonda ARP al dispositivo respondedor (304) solicitando una dirección de Ethernet asociada con una dirección IP reservada, en el que la dirección IP reservada es una dirección de transmisión de enlace local IPv4 169.254.255.255 o una dirección de enlace local IPv4 169.254.0.0, que no debe estar asignada a ningún dispositivo;

si se recibe una respuesta desde el dispositivo (304) a la segunda sonda ARP, poner (414) la dirección del dispositivo (304) en una lista negra asociada con un intervalo de direcciones IP de enlace local e ignorar respuestas ARP posteriores procedentes de las direcciones origen de la lista negra para el intervalo de direcciones de enlace local, de manera que se ignoren respuestas ARP posteriores del dispositivo (304) que pertenezcan a ese intervalo de direcciones.

5. El medio de almacenamiento legible por ordenador según la reivindicación 4, en el que la primera sonda ARP se envía por un dispositivo solicitante (308) que está en el proceso de asignar una dirección IP candidata de enlace local.

6. El medio de almacenamiento legible por ordenador según la reivindicación 5, en el que si no se recibe respuesta a la primera sonda ARP, el dispositivo solicitante (308) asigna (416) la dirección IP candidata de enlace local.

7. Un aparato que detecta un dispositivo (304) que responde incorrectamente a solicitudes del protocolo de resolución de direcciones, ARP, tal como un dispositivo (304) que responde incorrectamente a solicitudes ARP para direcciones IP de enlace local que no ha reivindicado correctamente para su propio uso legítimo, que comprende:

un mecanismo de envío configurado para seleccionar una dirección IP candidata de enlace local y para enviar una primera sonda ARP para la dirección IP candidata de enlace local;

en el que, cuando se recibe una respuesta a la primera sonda ARP, el mecanismo de envío está configurado para enviar una segunda sonda ARP solicitando una dirección de Ethernet asociada con una dirección IP reservada, en el que la dirección IP reservada es una dirección de transmisión de enlace local IPv4 169.254.255.255 o una dirección de enlace local IPv4 169.254.0.0, que no debe estar asignada a ningún dispositivo; y

un mecanismo de generación de lista negra, en el que si se recibe una respuesta del dispositivo (304) a la segunda sonda ARP, el mecanismo de generación de lista negra está configurado para:

poner la dirección del dispositivo (304) en una lista negra asociada con un intervalo de direcciones IP de enlace local, e

ignorar respuestas ARP posteriores procedentes de las direcciones origen de lista negra para el intervalo de direcciones de enlace local, de manera que se ignoren respuestas ARP posteriores del dispositivo (304) que pertenezcan a ese intervalo de direcciones.

8. El aparato según la reivindicación 7, en el que la primera sonda ARP se envía por un dispositivo solicitante (308) que está en el proceso de asignar una dirección IP candidata de enlace local.

9. El aparato según la reivindicación 8, que comprende además un mecanismo de asignación, en el que si no se recibe respuesta a la primera sonda ARP, el mecanismo de asignación está configurado para asignar la dirección IP candidata de enlace local.

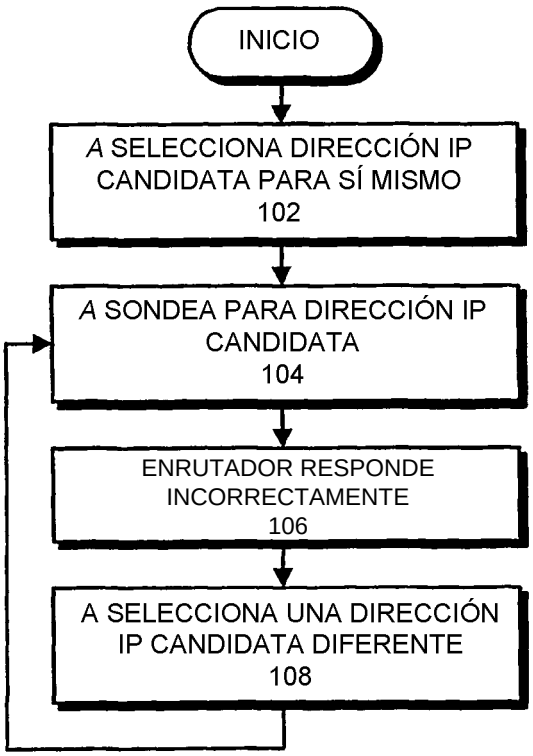

FIG. 1
(TÉCNICA ANTERIOR)

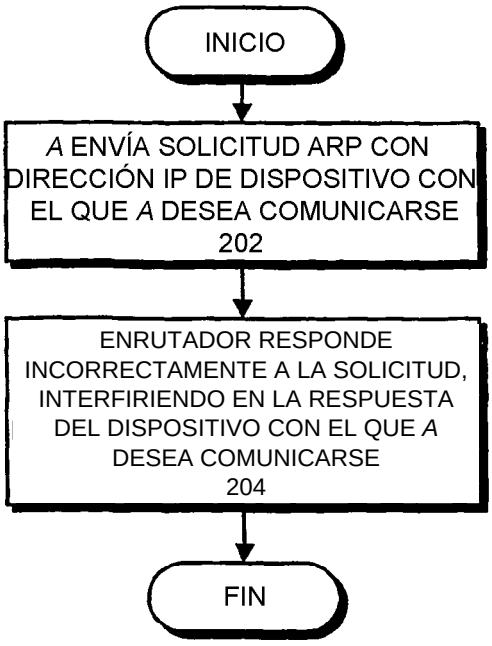

FIG. 2
(TÉCNICA ANTERIOR)

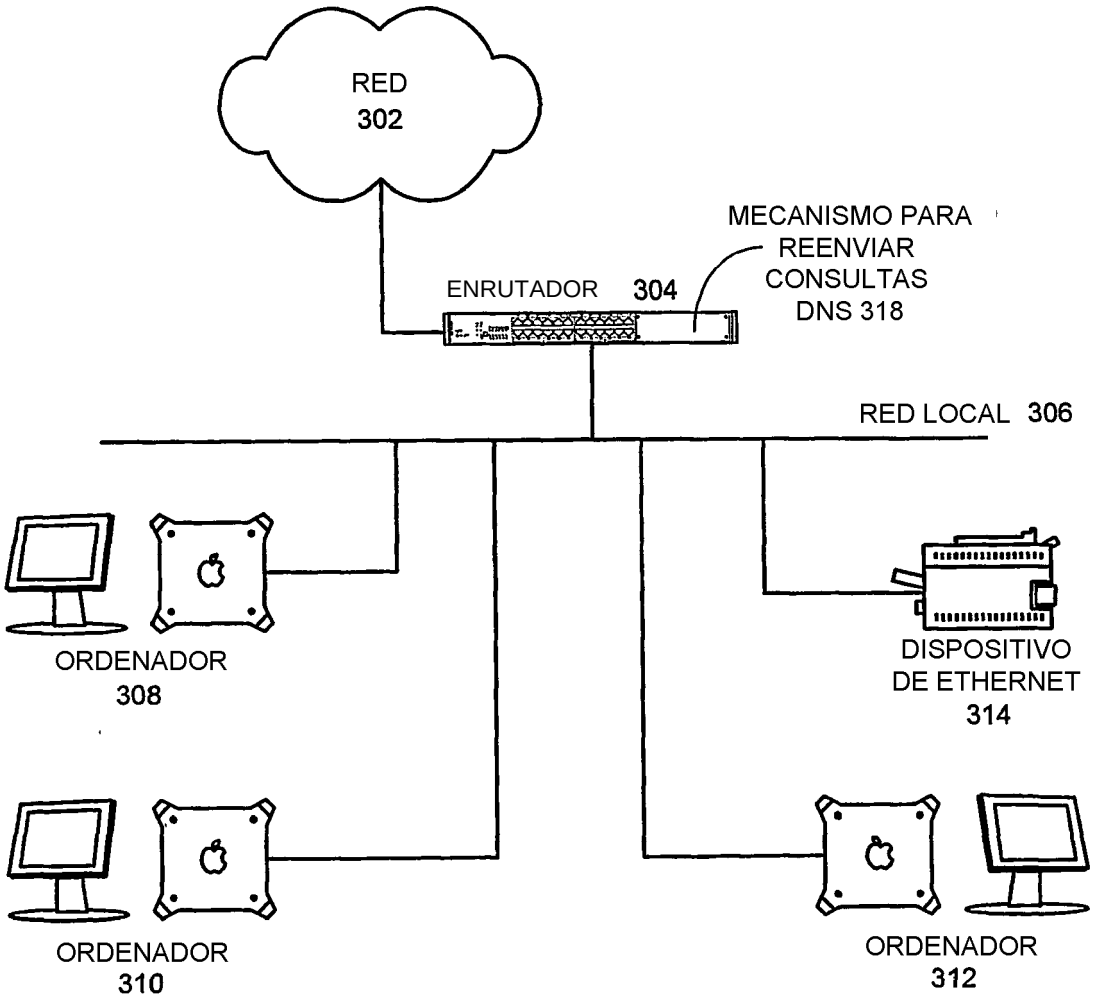
RED
302
MECANISMO PARA
REENVIAR
CONSULTAS
DNS 318
ENRUTADOR 304
RED LOCAL 306
ORDENADOR
308
DISPOSITIVO
DE ETHERNET
314
ORDENADOR
310
ORDENADOR
312

FIG. 3

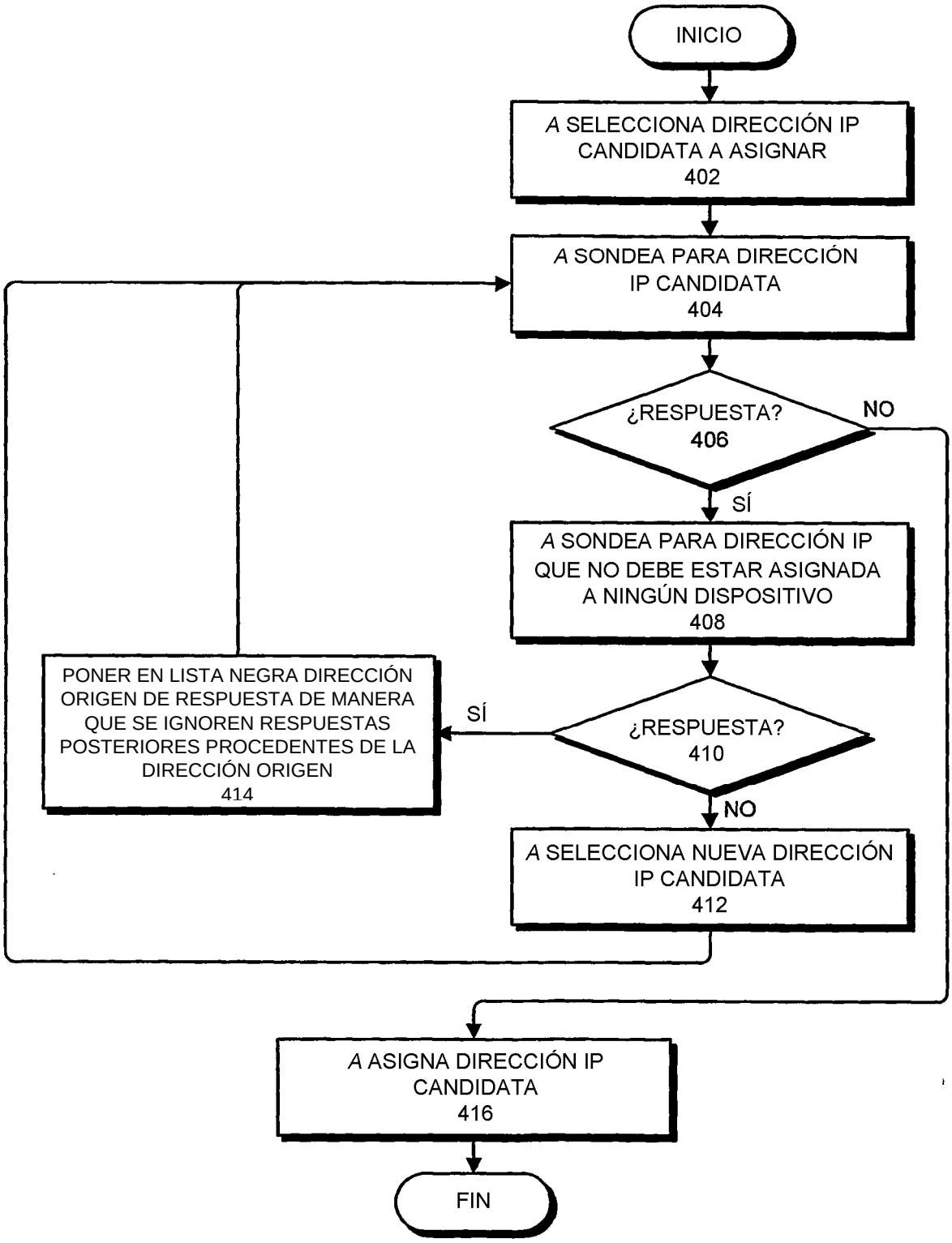
INICIO
A SELECCIONA DIRECCIÓN IP CANDIDATA A ASIGNAR 402
A SONDEA PARA DIRECCIÓN IP CANDIDATA 404
¿RESPUESTA? 406
NO
SÍ
A SONDEA PARA DIRECCIÓN IP QUE NO DEBE ESTAR ASIGNADA A NINGÚN DISPOSITIVO 408
¿RESPUESTA? 410
SÍ
NO
PONER EN LISTA NEGRA DIRECCIÓN ORIGEN DE RESPUESTA DE MANERA QUE SE IGNOREN RESPUESTAS POSTERIORES PROCEDENTES DE LA DIRECCIÓN ORIGEN 414
A SELECCIONA NUEVA DIRECCIÓN IP CANDIDATA 412
A ASIGNA DIRECCIÓN IP CANDIDATA 416
FIN

FIG. 4

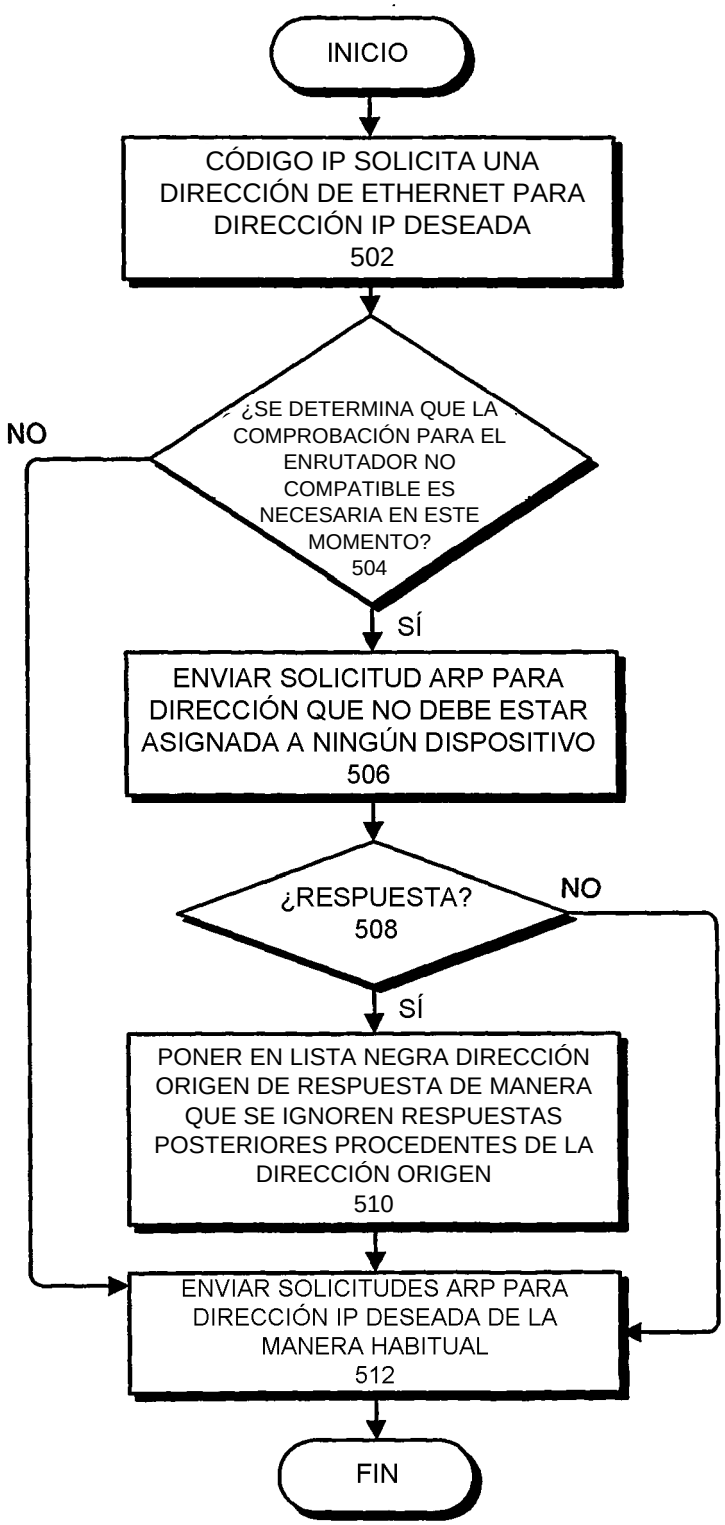
INICIO
CÓDIGO IP SOLICITA UNA DIRECCIÓN DE ETHERNET PARA DIRECCIÓN IP DESEADA
502
¿SE DETERMINA QUE LA COMPROBACIÓN PARA EL ENRUTADOR NO COMPATIBLE ES NECESARIA EN ESTE MOMENTO?
504
NO
SÍ
ENVIAR SOLICITUD ARP PARA DIRECCIÓN QUE NO DEBE ESTAR ASIGNADA A NINGÚN DISPOSITIVO
506
¿RESPUESTA?
508
NO
SÍ
PONER EN LISTA NEGRA DIRECCIÓN ORIGEN DE RESPUESTA DE MANERA QUE SE IGNOREN RESPUESTAS POSTERIORES PROCEDENTES DE LA DIRECCIÓN ORIGEN
510
ENVIAR SOLICITUDES ARP PARA DIRECCIÓN IP DESEADA DE LA MANERA HABITUAL
512
FIN

FIG. 5

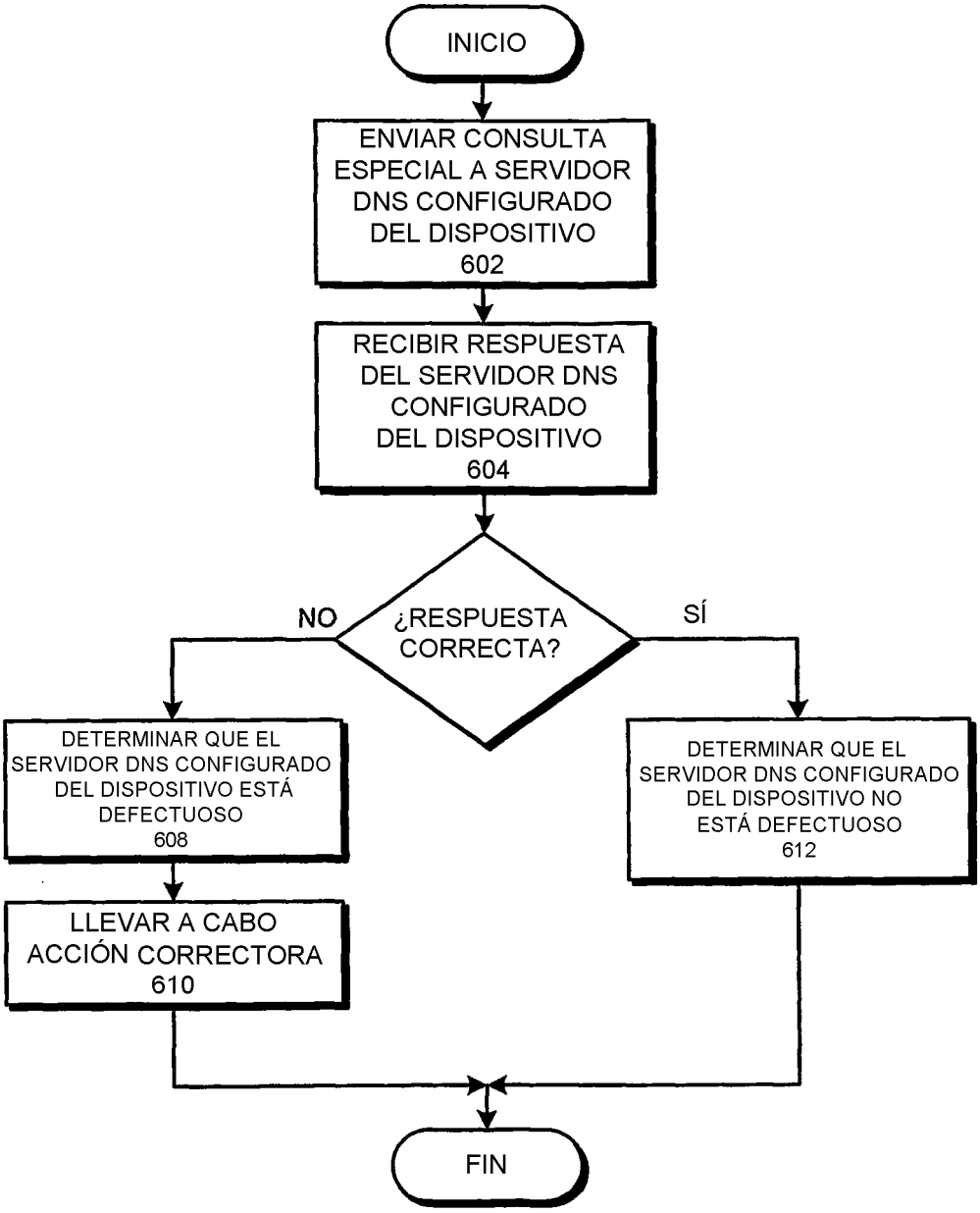
INICIO
ENVIAR CONSULTA ESPECIAL A SERVIDOR DNS CONFIGURADO DEL DISPOSITIVO
602
RECIBIR RESPUESTA DEL SERVIDOR DNS CONFIGURADO DEL DISPOSITIVO
604
¿RESPUESTA CORRECTA?
NO
SÍ
DETERMINAR QUE EL SERVIDOR DNS CONFIGURADO DEL DISPOSITIVO ESTÁ DEFECTUOSO
608
LLEVAR A CABO ACCIÓN CORRECTORA
610
DETERMINAR QUE EL SERVIDOR DNS CONFIGURADO DEL DISPOSITIVO NO ESTÁ DEFECTUOSO
612
FIN

FIG. 6