(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 433 272**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.11.2002 E 12162215 (3)**

(97) Fecha y número de publicación de la concesión europea: **18.09.2013 EP 2472824**

(54) Título: **Un método y un dispositivo en una red IP**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.12.2013

(73) Titular/es:

TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

NESZ, PETER;
JOHANSSON, THOMAS y
JUHL, MICHAEL

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Un método y un dispositivo en una red IP

Campo técnico de la invención

La presente invención se refiere a un método y un dispositivo en una red IP, los cuales contrarrestan el uso ilegítimo de direcciones IP.

Descripción de la técnica relacionada

Los abonados en una red IP pueden usar direcciones IP que no son adquiridas en una forma legítima. El abonado puede usar la dirección IP de alguien o una dirección IP actualmente no en uso. El abonado, que puede ser por ejemplo una empresa, está conectado a una isla de banda ancha, y usa la dirección IP para identificarse a sí mismo en la red. Si el abonado tiene intenciones de abusar hace un llamamiento para utilizar tal dirección IP ilegítima. El seguimiento de abusos está basado a saber en la dirección IP y el abusador se beneficiaría de la dirección ilegítima, dado que al abusador le sería más difícil de hacer el seguimiento en una investigación.

En la solicitud de patente internacional WO98/26550 se revela un sistema para asignación y uso de direcciones IP en una red con sistemas de abonado. Cada sistema de abonado está conectado a un servidor DHCP a través de un módem por cable. El servidor DHCP cede direcciones IP a los sistemas de abonados y trabaja en combinación con un agente de repetición DHCP seguro y un agente de repetición IP seguro. Cuando un sistema de abonado envía un mensaje de petición DHCP, el agente de repetición DHCP añade un identificador de confianza al mensaje y lo transmite al servidor DHCP. El identificador de confianza, el cual está asociado con el sistema de abonado de petición, se usa por el servidor DHCP para impedir al sistema de abonado acceder a cesiones de direcciones IP de otros sistemas de abonado. El servidor DHCP también cuenta el número de otros sistemas de abonados. servidor DHCP también cuenta el número de cesiones de direcciones IP por identificador de confianza y lo restringe a un número predeterminado. El sistema requiere un servidor DHCP no estándar y sistema de abonado.

La US 6.061.798 revela un cortafuegos para aislar los elementos de red de una red accesible públicamente. Todo acceso a elementos de red protegidos debe ir a través del cortafuegos, que funciona en un ordenador autónomo. Un agente intermediario, asignado específicamente a una petición entrante, verifica la autoridad de la petición de acceder a un elemento de red indicado en la petición. Una vez verificado, el agente intermediario completa la conexión a la red protegida en nombre de la fuente de la petición entrante.

Es conocido en la técnica impedir el mal uso de las direcciones IP mediante un filtro en un conmutador, el cual está conectado a un abonado. Unas tramas de datos de abonado se filtran por direcciones ilegítimas. El filtro se monta y se actualiza por un operador de red.

Un conmutador de filtrado de direcciones IP de fuente dinámica, que implementa un Agente de Repetición DHCP, se revela en la US 2002/0023160 A1.

El documento “A protection method against unauthorized access and address spoofing for open network access systems” de Hayato Ishibashi, et al. revela un método para proteger una red frente a un acceso no autorizado.

Resumen de la invención

La presente invención trata con el problema mencionado anteriormente de cómo restringir el uso de direcciones IP asignadas en una red IP a las legítimas.

Otro problema es cómo impedir a un abonado usar de por sí direcciones IP legítimas, las cuales ha obtenido el abonado en una forma ilegítima.

Aún un problema es cómo impedir al abonado hacer un gran número de intentos para usar ilegítimamente direcciones IP.

Aún otro problema es que un operador tiene que montar y actualizar un filtro para direcciones asignadas estáticamente.

El problema se resuelve mediante un método y un dispositivo según las reivindicaciones 1 y 6, respectivamente. En las reivindicaciones dependientes se recogen realizaciones particulares.

El problema se resuelve mediante un dispositivo de filtro IP con identificaciones de abonado y direcciones IP correspondientes. Las tramas de datos de los abonados tienen que tener la dirección IP fuente correcta para pasar el dispositivo de filtro. El filtro IP es actualizado sucesivamente según se usan nuevas direcciones IP de abonado. En caso de direcciones IP que se asignan por servidores DHCP (Protocolo de Configuración Central Dinámica), solamente se permiten servidores de confianza para asignar direcciones IP de abonado a los abonados.

El filtro IP es actualizado dinámicamente de la siguiente manera. Un abonado requiere una dirección IP. Una

respuesta de dirección con una dirección IP asignada desde un servidor DHCP es analizada tanto para ser unas tramas DHCP como para venir desde uno de los servidores DHCP de confianza, cuyos servidores se señalan en una lista. La dirección IP asignada y su tiempo de cesión se almacenan en el filtro IP junto con una identificación del abonado. Cuando el tiempo de cesión se acaba la identificación del abonado y la dirección IP son eliminadas del filtro. Nuevos abonados son almacenados sucesivamente. El tráfico desde uno de los abonados tiene que tener la dirección IP asignada a los abonados como dirección fuente para pasar el filtro. Los intentos de un abonado para usar direcciones IP ilegítimas son contados y a un número predeterminado de intentos se genera una advertencia.

Un propósito con la invención es restringir el uso de direcciones IP a las legítimas.

Otro propósito es impedir a un abonado usar de por sí direcciones IP legítimas las cuales, el abonado haya obtenido en una manera ilegítima.

Todavía un propósito es cómo impedir al abonado hacer un gran número de intentos para usar ilegítimamente direcciones IP.

Aún otro propósito es que las limitaciones de direcciones IP mencionadas funcionarán automáticamente en un entorno con direcciones IP asignadas dinámicamente.

La invención tiene la ventaja de que solamente los servidores DHCP de confianza pueden asignar direcciones IP.

Otra ventaja es que un abonado puede usar solamente direcciones IP legítimas obtenidas de una forma legítima.

Una ventaja adicional es que es posible impedir intentos repetidos para obtener direcciones IP.

Aún otra ventaja es que un abonado, que pretende emplear mal la red, no puede hacer el seguimiento más difícil usando una dirección IP obtenida ilegítimamente.

También, son ventajas que un operador no necesita montar y actualizar un filtro, un proceso automatizado no está afectado por errores humanos y la gestión del sistema es barata.

La invención se describirá ahora más estrechamente con la ayuda de las realizaciones en conexión con los dibujos adjuntos.

Breve descripción de los dibujos

La Figura 1 muestra una vista sobre una red IP;

La Figura 2 muestra un esquema de bloques sobre un conmutador;

La Figura 3 muestra una tabla en el conmutador;

La Figura 4 muestra un esquema de bloques sobre una trama IP;

La Figura 5 muestra un diagrama de flujo para procedimientos en el conmutador;

La Figura 6 muestra un esquema de bloques sobre una lista;

La Figura 7 muestra un esquema de bloques sobre un contador; y

La Figura 8 muestra un diagrama de flujo para procedimientos alternativos en el conmutador.

Descripción detallada

La Figura 1 muestra una vista sobre una red IP simple 1. La red 1 incluye una red central 2 la cual está conectada a un proveedor de servicios 3, servidores DHCP 4, 4a y 4b y a un conmutador 5 a través de un puerto PN de enlace ascendente. El conmutador a su vez incluye un motor conmutador 8, el cual está conectado a una base de datos 7 y un dispositivo de filtro IP 9. El dispositivo de filtro está conectado a los puertos físicos del conmutador P1, P2, P3 para abonados. Un dispositivo de abonado 6 está conectado a la red central 2 a través del filtro IP 9 en el conmutador 5. El dispositivo de abonado 6 tiene de manera convencional una dirección MAC MAC1 y está conectado al puerto físico P1 del conmutador y a una LAN virtual LAN1 en ese puerto. También, un abonado 6A con una dirección MAC MAC2 está conectado al puerto con la identificación P2 en una LAN VLAN2 virtual y el conmutador también tiene un puerto P3 adicional.

La asignación de direcciones dinámica convencional funciona en resumen de la siguiente manera. Un abonado en una red IP convencional con asignación de direcciones dinámica quiere tener una dirección IP, por la cual ha pagado. Él entonces transmite una petición DHCP (Protocolo de Configuración Dinámica de Servidor). Un servidor DHCP señala la petición y responde con una dirección IP y un intervalo de tiempo de cesión para la dirección. El abonado ahora puede comunicar con otros abonados o un proveedor de servicios a través de la red. Un abonado con intenciones de abusar puede adquirir una dirección IP de una manera ilegítima, lo cual hace más difícil rastrearle

en la red. El abonado puede por ejemplo obtener la dirección de un servidor DHCP fraudulento o puede él mismo escribir una dirección que pertenece a alguien más o que no está actualmente en uso. El abonado puede también comportarse de otras maneras inaceptables., por ejemplo requerir y obtener un gran número de direcciones IP y por ello hacer difícil para otros abonados obtener una dirección.

En resumen el conmutador 5 funciona de la siguiente manera. Para impedir el mal uso de direcciones IP asignadas el conmutador inventivo 5 está equipado con el filtro 5 para protección de suplantación de identidad de direcciones IP, que puede ser habilitado o deshabilitado por LAN virtual. El conmutador 5 también tiene una lista L1 sobre los de confianza de los servidores DHCP, en la realización los servidores 4, 4a y 4b. El conmutador está configurado de forma que, cuando la protección de suplantación de identidades habilitada, todas las direcciones IP son bloqueadas en el puerto del conmutador de los abonados. El único tráfico permitido es el tráfico DHCP a los servidores DHCP de confianza, las transmisiones DHCP y los envíos de ARP (Protocolo de Resolución de Direcciones). Cuando el abonado 6 necesita una dirección IP transmite una petición DHCP. Los servidores DHCP 4, 4a, 4b leen la petición y responden con una trama, que indica una dirección IP de abonado asignada IP1 y un intervalo de tiempo de cesión T1 para esta dirección. La trama también tiene una dirección IP fuente que define el servidor DHCP respectivo. El conmutador 5 comprueba a través de esta dirección IP fuente si la trama es enviada por los servidores DHCP de confianza 4, 4a, 4b en la lista. También comprueba que realmente es una trama DHCP la que es recibida. El conmutador 5 tiene almacenada en la base de datos 7 la dirección MAC MAC1 del abonado 6, una identificación de su puerto físico P1 y su LAN virtual VLAN1. El conmutador ahora configura dinámicamente el filtro 9, el cual incluye por abonado los siguientes valores: La dirección MAC de abonado MAC1, la identificación del puerto del abonado P1, la LAN virtual del abonado VLAN1, la dirección IP de abonado recibida IP1 y el intervalo de tiempo de cesión T1 para la dirección IP. Cuando el abonado 6 envía un mensaje el conmutador compara la dirección IP fuente de abonado en las tramas transmitidas con la dirección IP de abonado asignada IP1 en el filtro 9 en la identificación del puerto del abonado P1 y la LAN virtual VLAN1. Con dirección IP correcta las tramas pasan el filtro, de otro modo las tramas se descartan. Cuando el intervalo de tiempo de cesión T1 se agota la identificación de abonado y la dirección IP de abonado asignada IP1 es eliminada del filtro (9). Más detalles de los procesos brevemente descritos anteriormente serán dados en conexión con la figura 5.

De una manera correspondiente como anteriormente el filtro IP 9 se configurará dinámicamente con valores de abonado para el abonado 6A: La identificación de puerto P2, la LAN virtual VLAN2, una dirección IP de abonado asignada IP2, y un intervalo de tiempo de cesión correspondiente T2.

Las direcciones IP asignadas estáticamente pueden en una alternativa ser escritas directamente en el filtro IP 9. En otra alternativa los servidores DHCP tienen la dirección IP asignada estáticamente para un abonado. Esta última hace una petición DHCP convencional para su dirección IP estática. El servidor DHCP señala la dirección MAC del abonado en la petición y siempre asigna la dirección IP asignada estáticamente del abonado. Las direcciones IP asignadas estáticamente del primer tipo pueden ser usadas por ejemplo cuando aplicaciones en un ordenador no pueden utilizar peticiones DHCP para una dirección IP.

En la figura 2 el conmutador es mostrado en algo más de detalle. El filtro IP 9 está conectado a los puertos del conmutador P1, P2 y P3 y a la base de datos 7. Está también conectado al motor del conmutador 8 y a un clasificador 10. En la base de datos 7 está almacenada la dirección MAC de abonado MAC1, su identificación de puerto P1 y la identidad de LAN virtual VLAN1. El filtro IP 9 tiene una lista sobre los servidores DHCP de confianza y también una tabla de abonado, cuya lista y tabla serán descritas en conexión con la figura 3. El clasificador 10 comprueba si tramas de datos transmitidas vienen de o a un abonado y si el mensaje DHCP es un mensaje DHCPACK o algún otro mensaje DHCP. Qué operaciones, en más detalle, la parte del conmutador respectiva 7, 8, 9 y 10 se realizan cuando el abonado 6 hace peticiones DHCP o intercambia mensajes con la red 2 y los proveedores de servicio 3 serán descritas en conexión con la figura 5.

Anteriormente fue mencionado que el filtro 9 fue configurado con valores de abonado. Los valores se almacenan en una tabla de filtro TAB1, la cual se muestra en la figura 3. En un campo 31 los diferentes abonados 6, 6A son almacenados con sus direcciones MAC respectivas MAC1 y MAC2. Un campo 32 da el número de puerto de abonado P1 respectivo P2 y un campo 33 da las identidades VLAN1 respectiva VLAN2 para las LAN virtuales del abonado. En un campo 34 las direcciones IP de abonado IP1 respectiva IP2 son escritas y en un campo 35 los intervalos de tiempo de cesión de la dirección T1 respectivo T2 son escritos. En la figura 6 se muestra una lista L1 que tiene campos 61, 62, 63 para los servidores DHCP de confianza respectivos 4, 4a y 4b con sus direcciones IP IP4, IP4a e IP4b.

La comunicación en la red 1 se realiza de acuerdo con la Pila de Siete Capas TCP/IP. En la figura 4 se muestra una trama Ethernet FR1 de acuerdo con el estándar IEEE802.1q. La trama tiene un campo D1 para una dirección MAC de destino y un campo S1 siguiente para una dirección MAC fuente. También tiene un campo TY2 que indica que la VLAN está en uso. Un campo VL1 señala qué LAN virtual está afectada por una etiqueta de LAN virtual. En el ejemplo presente esta etiqueta es la identidad LAN virtual, ejemplificada por las identidades VLAN1 y VLAN2. La trama incluye un campo TY1 para definir un tipo de trama Ethernet. Un campo EPL1 contiene la carga útil Ethernet que incluye una cabecera IP IPH con direcciones IP fuente y destino, el intervalo de tiempo de cesión y el mensaje que va a ser transmitido.

La Figura 5 es un diagrama de flujo que describe una realización de diferentes tareas que el conmutador 5 realiza. En un bloque 501 el conmutador recibe una trama entrante y esta tarea se indica mediante (1) en el bloque. En un bloque 502 se realiza una tarea (2), incluyendo la comprobación de dónde viene la trama. El conmutador tiene tanto los puertos de abonado P1, P2 y P3 como el puerto de red PN, y se comprueba en qué tipo de puerto se recibe la trama.

En una alternativa 503 la trama entrante viene en uno de los puertos de abonado P1, P2 y P3. En un bloque 504 entonces se realiza una tarea (3), incluyendo una comprobación de si la trama es un mensaje DHCP. Esto se comprueba comprobando los números de puerto fuente y destino en el mensaje en el mensaje UDP, dado que el sistema está restringido de manera que sólo los mensajes DHCP pueden usar el puerto 67 y 68. Si la comprobación del mensaje DHCP falla implica que alguien está usando los puertos 67 y 68 y el mensaje se descarta. Si la trama se encuentra que es un mensaje DHCP, de acuerdo con una alternativa SÍ1, la trama es aceptada por un bloque 505. Este bloque realiza una tarea (6), la cual incluye que la trama se reenvíe y en este caso reenviada a la red central 2. Si la trama no es un mensaje DHCP, de acuerdo con una alternativa NO1, se realiza una tarea (4) en un bloque 506. La tarea (4) incluye una comprobación de si es válida la información fuente de la trama. Se comprueba que la dirección MAC fuente de la capa 2, la dirección IP de la capa 3, el intervalo de tiempo de cesión y en casos reales la identificación de la LAN virtual son todos válidos en el puerto real. En la presente realización en otras palabras se comprueba en la tabla TAB1 que la dirección MAC MAC1, la dirección IP IP1, el intervalo de tiempo de cesión T1 y la identificación LAN VLAN1 son válidas en el puerto P1. En una alternativa NO2 la tarea de comprobación (4) muestra que la información de la fuente no es válida y en un bloque 507 se realiza una tarea (5) la cual implica que se descarta la trama. En una alternativa SÍ2 para el bloque 506 la información de la fuente es válida y la trama es aceptada en el bloque 505 realizando la tarea (6).

El bloque 502 tiene la tarea (2) por la cual puede en una alternativa 508 detectar que la trama viene de la red central 2 en el puerto PN. En un bloque 509 se realiza una tarea (7), la cual incluye la comprobación de si la trama es un mensaje DHCP. En una alternativa NO3, cuando la trama no es un mensaje DHCP, la trama es aceptada en el bloque 505, el cual realiza la tarea (6). En una alternativa SÍ3, cuando la trama es un mensaje DHCP, se comprueba la trama en un bloque 510 realizando una tarea (8). Esta tarea incluye una pregunta de si el mensaje DHCP se origina desde un servidor DHCP válido, es decir es un servidor que está almacenado en la lista L1. En una alternativa NO4 el servidor no es válido y la trama es descartada en un bloque 511 realizando la tarea (5). En otra alternativa SÍ4 el servidor es válido y se realiza una comprobación en un bloque 512 realizando una tarea (9). La comprobación incluye una pregunta de si la trama es un mensaje de reconocimiento DHCP. En una alternativa NO5, cuando la trama no es un mensaje de reconocimiento, la trama es aceptada en el bloque 505. En una alternativa contraria SÍ5 la trama es un mensaje de reconocimiento. Entonces se maneja en un bloque 513 realizando una tarea (10). Esta tarea incluye que la dirección IP de la capa 3 y el intervalo de tiempo de cesión sean añadidos en la base de datos 7. Entonces la información sobre la dirección MAC fuente de la capa 2, la dirección IP de la capa 3, la identificación del puerto, el intervalo de tiempo de cesión y la identificación de LAN virtual para el abonado se insertan en la tabla TAB1. La trama entonces se acepta, tarea (6) en el bloque 505.

En la figura 2 se indican qué partes del conmutador 5 realizan las diferentes tareas. El filtro IP 9 realiza la tarea (1) de recibir una trama entrante, la tarea (4) que afecta a la información de la fuente de la trama, la tarea (5) que maneja el descarte de tramas, la tarea (6) que acepta una trama, la tarea (8) que maneja la pregunta del servidor DHCP válido y la tarea (10) de insertar valores en la tabla del filtro TAB1. El clasificador 10 realiza la tarea (2) de comprobar de dónde vienen las tramas, la tarea (3) de comprobar si una trama es un mensaje DHCP de un abonado, la tarea (7) de comprobar si una trama es un mensaje DHCP de la red central y la tarea (9) de si una trama es un mensaje de reconocimiento.

En conexión con la figura 1 fueron brevemente descritos los procesos cuando el abonado 6 obtiene la dirección IP IP1 y después envía un mensaje. Primero el proceso de obtener la dirección será más estrechamente descrito en conexión con la figura 5.

El abonado 6 envía un mensaje de descubrimiento DHCP M1 el cual es recibido por el conmutador 5 de acuerdo con el bloque 501, tarea (1). En el bloque 502, tarea (2), el origen del mensaje M1 es comprobado y de acuerdo con la alternativa 503 se decide el puerto P1. De acuerdo con el bloque 504, tarea (3) y la alternativa SÍ1, el mensaje M1 es un mensaje DHCP que es aceptado en el bloque 505, tarea (6) y es reenviado a la red central 2.

Uno o más de los servidores DHCP 4, 4a, 4b devuelve cada uno un mensaje de oferta DHCP M2 con una dirección IP ofrecida. De acuerdo con el bloque 501, tarea (1), el mensaje M2 es recibido y en el bloque 502, tarea (2), se comprueba su origen. El puerto PN se decide de acuerdo con la alternativa 508 y en el bloque 509, tarea (7), y la alternativa SÍ3 se señala que el mensaje M2 es un mensaje DHCP. De acuerdo con el bloque 510, tarea (8) y la alternativa SÍ4, el servidor DHCP 4 es válido. En el bloque 512, tarea (9) y la alternativa NO5, el mensaje M2 se señala que no sea un mensaje de reconocimiento DHCP y en el bloque 505, tarea (6), el mensaje de oferta DHCP M2 es reenviado al abonado 6.

El abonado 6 ahora selecciona una de las direcciones IP ofrecidas, en la realización la dirección IP1 del servidor 4. El abonado solicita la dirección IP1 mediante una petición DHCP M3 la cual es recibida por el conmutador 5 de acuerdo con el bloque 501, tarea (1). En el bloque 502, tarea (2), se comprueba el origen del mensaje M3 y de

acuerdo con la alternativa 503 se decide el puerto P1. De acuerdo con el bloque 504, tarea (3) y la alternativa SÍ1, el mensaje M3 es un mensaje DHCP que es aceptado en el bloque 505, tarea (6) y es reenviado a la red central 2.

El seleccionado de los servidores DHCP, servidor 4, devuelve un mensaje de reconocimiento DHCP M4, confirmando la dirección IP ofrecida IP1. De acuerdo con el bloque 501, tarea (1), se recibe el mensaje M4 y en el bloque 502, tarea (2) se comprueba su origen. El puerto PN se decide de acuerdo con la alternativa 508 y en el bloque 509, tarea (7), y la alternativa SÍ3 se señala que el mensaje M4 es un mensaje DHCP. De acuerdo con el bloque 510, tarea (8) y la alternativa SÍ4, el servidor DHCP 4 que ha enviado el mensaje M4 es válido. En el bloque 512, tarea (9) y la alternativa SÍ5, el mensaje M4 se señala que es un mensaje de reconocimiento DHCP (DHCPACK). Entonces se maneja en el bloque 513, tarea (10) por el cual la información sobre la dirección MAC fuente de la capa 2 de abonado MAC1, la dirección IP de la capa 3 IP1 recibida, la identificación de puerto P1, la identificación de LAN virtual VLAN1 y el intervalo de tiempo de cesión T1 son insertados en la tabla TAB1. El mensaje M4 es por ello aceptado y en el bloque 505, tarea (6), el mensaje de reconocimiento DHCP M4 es reenviado al abonado 6. El abonado ahora tiene una dirección IP válida.

Se debería señalar que un abonado, por ejemplo el abonado 6, puede usar legítimamente más de una dirección IP. El abonado hace un acuerdo con un operador y obtiene de esta manera legítima suscripciones adicionales para direcciones IP. El número de direcciones IP legítimas se señala en la base de datos 7. Las direcciones IP en sí mismas son obtenidas de los servidores de confianza de la misma manera que la dirección IP1 y son señaladas en la tabla del filtro TAB1.

El abonado 6 ahora quiere utilizar un servicio del proveedor de servicios 3 y envía un mensaje M5 en la figura 1. De acuerdo con el bloque 501, tarea (1), el conmutador 5 recibe el mensaje M5. En el bloque 502, tarea (2), se comprueba de dónde viene el mensaje M5. En la alternativa 503 viene en el puerto de abonado P1. En el bloque 504, tarea (3), se comprueba si el mensaje M5 es un mensaje DHCP. Como no es así, de acuerdo con la alternativa NO1, se comprueba en la tabla TAB1, de acuerdo con el bloque 506, tarea (4), que la dirección MAC fuente de la capa 2 MAC1, la dirección IP de la capa 3 IP1, el intervalo de tiempo de cesión T1 y la identificación de LAN virtual VLAN1 son todas válidas en el puerto real P1. En la alternativa SÍ2 la información es válida y el mensaje M5 es aceptado en el bloque 505, tarea (6). El mensaje es ahora reenviado al proveedor de servicios 3.

Si el abonado intenta enviar una trama como la trama FR1 en la figura 4 como un mensaje y usa una dirección IP inválida IPX en la cabecera IP IPH, esto se revela en la comprobación en la tabla TAB1. De acuerdo con la alternativa NO2, la trama FR1 entonces es descartada en el bloque 507, tarea (5). Se mencionó anteriormente que un problema es cómo impedir a los abonados, 6 y 6A, hacer un gran número de tales intentos, para usar ilegítimamente direcciones IP. Este problema se resuelve incluyendo un contador en la tarea (5) en el filtro IP 9. En la figura 7 se muestra un esquema de bloques sobre tal contador C1. El contador tiene los campos 71, 72, 73 en los cuales están escritos los puertos de abonado respectivos P1, P2 y P3 y el número correspondiente n de intentos falsos, es decir intentos con direcciones IP inválidas. También tiene un elemento de comparación 79 en el cual está escrito un número N de intentos falsos permitidos. En el ejemplo el abonado 6 en el puerto P1 ha hecho un falso intento. Cuando la trama con la dirección inválida es descartada, se envía un mensaje F1 al contador C1, campo 71 para el puerto P1. En este campo se fija n=1, el cual se compara con N=10, no provocando ninguna acción. El abonado 6A en el puerto P2 ha hecho n=11 falsos intentos. Como este número excede el número permitido N=10 se genera un mensaje de advertencia W1.

En la figura 8 se muestra un diagrama de flujo para una realización alternativa de los procedimientos en el conmutador 5. En un bloque 801 el conmutador recibe una trama entrante y esta tarea es, como anteriormente, indicada por (1) en el bloque. En un bloque 802 se realiza una tarea (7b), incluyendo la comprobación de si la trama es una trama DHCP. Si no lo es de acuerdo con una alternativa NO6, la tarea (4) se realiza en un bloque 803. Esta tarea incluye la comprobación de si la información de la fuente de la trama es válida y se realiza con la ayuda de la tabla TAB1 en el filtro 9. Si la información de la fuente de la trama es inválida, de acuerdo con una alternativa NO7, la trama es descartada en un bloque 804 realizando la tarea (5). Si en su lugar la información de la fuente de la trama es válida, de acuerdo con una alternativa SÍ7, la trama es aceptada por la tarea (6) realizada en un bloque 805. Si se encuentra en el bloque 802 que la trama entrante es una trama DHCP, la alternativa SÍ6, la tarea (7b) incluye la comprobación de qué tipo de puerto proviene la trama. En una alternativa 806 la trama DHCP viene en uno de los puertos de abonado P1, P2, P3 y es entonces aceptada en el bloque 805. En una alternativa 807 la trama DHCP en su lugar viene sobre el puerto PN de enlace ascendente. Entonces se comprueba en un bloque 808 por la tarea (8), la lista L1, si la trama DHCP se origina desde un servidor DHCP válido. En una alternativa NO8 el servidor no es válido y la trama es descartada en un bloque 809, que realiza la tarea (5). En una alternativa SÍ8 el servidor se encuentra que es válido y se realiza una comprobación por la tarea (9) en un bloque 810. La comprobación incluye la pregunta de si la trama es un mensaje de reconocimiento DHCP. Si no lo es de acuerdo con una alternativa NO9, la trama es aceptada en un bloque 811, que realiza la tarea (6). En una alternativa contraria SÍ9 la trama es una trama de reconocimiento DHCP y entonces se maneja en un bloque 812, que realiza la tarea (10). Esta tarea incluye que la dirección IP de la capa 3 y el intervalo de tiempo de cesión sean añadidos en la base de datos 7. Entonces la información sobre la dirección MAC fuente de la capa 2, la dirección IP de la capa 3, la identificación del puerto, el intervalo de tiempo de cesión y la identificación LAN virtual para el abonado se inserten en la tabla TAB1. La trama entonces es aceptada, tarea (6) en el bloque 811.

El proceso cuando el abonado 6 obtiene una dirección IP será descrito muy brevemente en conexión con la figura 8. En la fase de descubrimiento el mensaje de descubrimiento M1 es recibido en el bloque 801 y se encuentra que es un mensaje DHCP en el bloque 802. De acuerdo con la alternativa 806 se encuentra que viene del abonado y el mensaje M1 es aceptado en el bloque 805. El mensaje de oferta DHCP M2 de los servidores DHCP se recibe en el bloque 801, encuentra que es un mensaje DHCP en el bloque 802 y encuentra que es un mensaje de respuesta de acuerdo con la alternativa 807. El servidor DHCP es uno válido de acuerdo con el bloque 808, el mensaje M2 no es mensaje de reconocimiento, bloque 810 y es aceptado en el bloque 811 y reenviado al abonado 6. Este último selecciona la dirección IP1 y la solicita mediante el mensaje M3, el cual es recibido en el bloque 801. En el bloque 802 es señalado como un mensaje DHCP el cual viene del abonado, alternativa 806, y es aceptado en el bloque 805. El servidor obtiene el mensaje M3 y devuelve el mensaje de reconocimiento M4. En el bloque 801 se recibe el mensaje M4, se encuentra que es un mensaje DHCP en el bloque 802 y que es un mensaje de respuesta, alternativa 807. La fuente del mensaje es válida, bloque 808, y el mensaje M4 se encuentra que es un mensaje de reconocimiento, bloque 810 alternativa SÍ9. En el bloque 812 la dirección IP1 y su intervalo de tiempo de cesión T1 son añadidos en la base de datos 7 y se rellena la tabla TAB1 en el filtro IP 9. El mensaje M4 es aceptado, bloque 811, y el abonado 6 obtiene la dirección y su intervalo de tiempo de cesión T1. El abonado 6 tiene una dirección IP válida.

Cuando el abonado 6 envía el mensaje M5 al proveedor de servicios 3, se recibe el mensaje en el bloque 801 y se encuentra que no es un mensaje DHCP, bloque 802 alternativa NO6. La información de la fuente de la trama entonces se comprueba en el bloque 803 con la ayuda de la tabla TAB1 en el filtro 9. Si es válida, alternativa SÍ7, el mensaje M5 es aceptado y se envía al destinatario.

Realizaciones:

La realización A comprende un método en una red IP, incluyendo la red un nodo conmutador 5, al menos un servidor DHCP 4, 4a, 4b y al menos un abonado 6 que está asociado con el nodo El método incluye los siguientes pasos:

- crear una lista L1 de los de confianza de los servidores DHCP;

- transmitir por el abonado 6 un mensaje de petición DHCP M3 para una dirección IP;

- recibir un mensaje de respuesta M4, el cual transporta una dirección IP de abonado asignada IP1;

- analizar el mensaje de respuesta para ser un mensaje DHCP y que tiene una dirección fuente IP4 de uno de los servidores DHCP de confianza;

- actualizar un filtro 9, TAB1 dinámicamente en el nodo, almacenando el filtro una identificación MAC1, P1, VLAN1 del abonado 6 y la dirección IP de abonado asignada IP1;

La realización B incluye todas las características de la realización A e incluye además almacenar en el filtro una dirección MAC de abonado MAC1, un número de puerto físico de abonado P1, una LAN virtual VLAN1 y un intervalo de tiempo de cesión T1 para la dirección IP de abonado asignada IP1.

La realización C incluye todas las características de la realización A e incluye además la dirección IP de abonado que se asigna estáticamente y maneja por los servidores DHCP.

La realización D incluye todas las características de la realización B e incluye además eliminar la identificación de abonado MAC1, P1, VLAN1 y la dirección IP de abonado asignada correspondiente IP1 del filtro cuando el intervalo de tiempo de cesión T1 se agota.

La realización E incluye todas las características de la realización A, B o C e incluye además transmitir una trama FR1 desde el abonado usando una dirección IP fuente IPX, comparar en el filtro dicha dirección IP fuente con la dirección IP de abonado asignada IP1; y descartar dicha trama cuando dicha dirección IP fuente IPX difiere de la dirección IP de abonado almacenada IP1.

La realización F incluye todas las características de la realización E e incluye además contar un número de intentos n del abonado 6A para usar una dirección IP ilegítima; comparar 9, C1 el número n de los intentos con un número umbral N; y enviar una señal de advertencia W1 cuando el número de intentos excede unos criterios umbral.

La realización G comprende un dispositivo en una red IP. El dispositivo 5 incluye al menos un puerto P1, P2, P3 para un abonado ; un puerto PN de enlace ascendente para servidores DHCP en la red; y un dispositivo de filtro 9 que tiene una lista L1 sobre los de confianza de los servidores DHCP 4, 4a, 4b, estando asociado el dispositivo de filtro con los puertos P1, P2, P3; PN. El dispositivo está dispuesto para recibir un mensaje de petición de dirección IP de abonado M3 en el puerto de abonado P1, analizar que sea un mensaje DHCP y transmitirlo en el puerto PN de enlace ascendente. El dispositivo también está dispuesto para recibir un mensaje de respuesta M4 en el puerto PN de enlace ascendente, analizar que sea un mensaje DHCP y tener una dirección IP fuente IP4 de uno de los servidores DHCP de confianza en la lista L1. El dispositivo está dispuesto además para actualizar dinámicamente el filtro 9, TAB1 con una identificación del abonado y una dirección IP de abonado asignada correspondiente IP1 en el

mensaje de respuesta M4;

Según la realización H, el dispositivo según la realización G está dispuesto adicionalmente para almacenar en el filtro 9, TAB1 una dirección MAC de abonado MAC1, un número de puerto físico de abonado P1, una identidad LAN virtual de abonado VLAN1 y un intervalo de tiempo de cesión T1 para la dirección IP de abonado asignada IP1.

Según la realización I, el dispositivo según la realización G, incluye además que la dirección IP de abonado es una dirección asignada estáticamente la cual se maneja por los servidores DHCP 4, 4a, 4b.

Según la realización J, el dispositivo según la realización H está dispuesto adicionalmente para eliminar la identificación de abonado MAC1, P1, VLAN1 y la dirección IP de abonado asignada correspondiente IP1 del filtro 9, TAB1 cuando el intervalo de tiempo de cesión T1 se agota.

Según la realización K, el dispositivo según la realización G, H o I está dispuesto adicionalmente para recibir una trama FR1 con una dirección IP fuente IPX en el puerto de abonado P2 para comparar en el filtro 9, TAB1 dicha dirección IP fuente IPX con la dirección IP de abonado almacenada IP1 y descartar dicha trama, FR1, cuando dicha dirección IP fuente IPX difiere de la dirección IP de abonado almacenada IP1.

Según la realización L, el dispositivo según la realización J incluye además, el filtro 9 que tiene un contador C1 que se dispone a contar un número n de tramas descartadas FR1 en el puerto de abonado P2, comparar 9, C1 el número n de las tramas descartadas con un número umbral N y enviar una señal de advertencia W1 cuando el número de tramas descartadas excede un criterio umbral.

REIVINDICACIONES

1.Un método para usar en un nodo conmutador (5), para gestionar tramas entrantes de un abonado (6) en una red IP, incluyendo el método los siguientes pasos para ser realizados por el nodo conmutador:

-recibir del abonado (6) un mensaje de petición DHCP (M3) para una dirección IP;

-reenviar el mensaje de petición DHCP (M3);

-recibir un mensaje de respuesta (M4), el cual transporta una dirección IP de abonado asignada (IP1);

-analizar (510, 808, (8)) el mensaje de respuesta (M4) para ser un mensaje DHCP que viene de un servidor DHCP de confianza;

-actualizar (513, 812, (10)) un filtro (9, TAB1) dinámicamente en el dispositivo (5), almacenando el filtro una identificación (MAC1, P1, VLAN1) del abonado (6) y la dirección IP de abonado asignada (IP1);

-recibir (501, 801) del abonado (6) una trama en el puerto de abonado (P1);

-comprobar (506, 803) cuando la trama no es un mensaje de petición DHCP (M3), si una información fuente de la trama es válida en el puerto de abonado (P1); y

-descartar (507, 804) o aceptar (505, 805) dicha trama dependiendo de la información fuente de la trama.

2. Método según la reivindicación 1, en el que dicho paso de comprobación incluye comprobar que una dirección IP de la trama es válida en el puerto de abonado (P1).

3. Método según la reivindicación 1 ó 2, en el que dicho paso de comprobación incluye comprobar que una dirección MAC de la trama es válida en el puerto de abonado (P1).

4. Método según cualquiera de las reivindicaciones anteriores, en el que dicho paso de comprobación incluye comprobar que un intervalo de tiempo de cesión es válido en el puerto de abonado (P1).

5. Método según cualquiera de las reivindicaciones anteriores, en el que dicho paso de comprobación incluye comprobar que una identificación LAN es válida en el puerto de abonado (P1).

6. Un dispositivo (5), para gestionar tramas entrantes de un abonado (6) en una red IP, incluyendo el dispositivo (5) al menos un puerto (P1, P2, P3) para un abonado (6, 6A); donde el dispositivo está dispuesto para:

-recibir del abonado (6) un mensaje de petición DHCP (M3) para una dirección IP;

-reenviar el mensaje de petición DHCP (M3);

-recibir un mensaje de respuesta (M4), el cual transporta una dirección IP de abonado asignada (IP1);

-analizar (510, 808, (8)) el mensaje de respuesta (M4) para ser un mensaje DHCP que viene de un servidor DHCP de confianza;

-actualizar (513, 812, (10)) un filtro (9, TAB1) dinámicamente en el dispositivo (5), almacenando el filtro una identificación (MAC1, P1, VLAN1) del abonado (6) y la dirección IP de abonado asignada (IP1);

-recibir (501, 801) del abonado (6) una trama en el puerto de abonado (P1);

-comprobar (506, 803) cuando la trama no es un mensaje de petición DHCP (M3), si una información fuente de la trama es válida en el puerto de abonado (P1); y

-descartar (507, 804) o aceptar (505, 805) dicha trama dependiendo de la información fuente de la trama.

7. Dispositivo según la reivindicación 6, en el que el dispositivo está dispuesto para comprobar que una dirección IP de la trama es válida en el puerto de abonado (P1).

8. Dispositivo según la reivindicación 6 ó 7, en el que el dispositivo está dispuesto para comprobar que una dirección MAC de la trama es válida en el puerto de abonado (P1).

9. Dispositivo según cualquiera de las reivindicaciones 6-8, en el que el dispositivo está dispuesto para comprobar que un intervalo de tiempo de cesión de la trama es válido en el puerto de abonado (P1).

10. Dispositivo según cualquiera de las reivindicaciones 6-9, en el que el dispositivo está dispuesto para comprobar que una identificación LAN es válida en el puerto de abonado (P1).

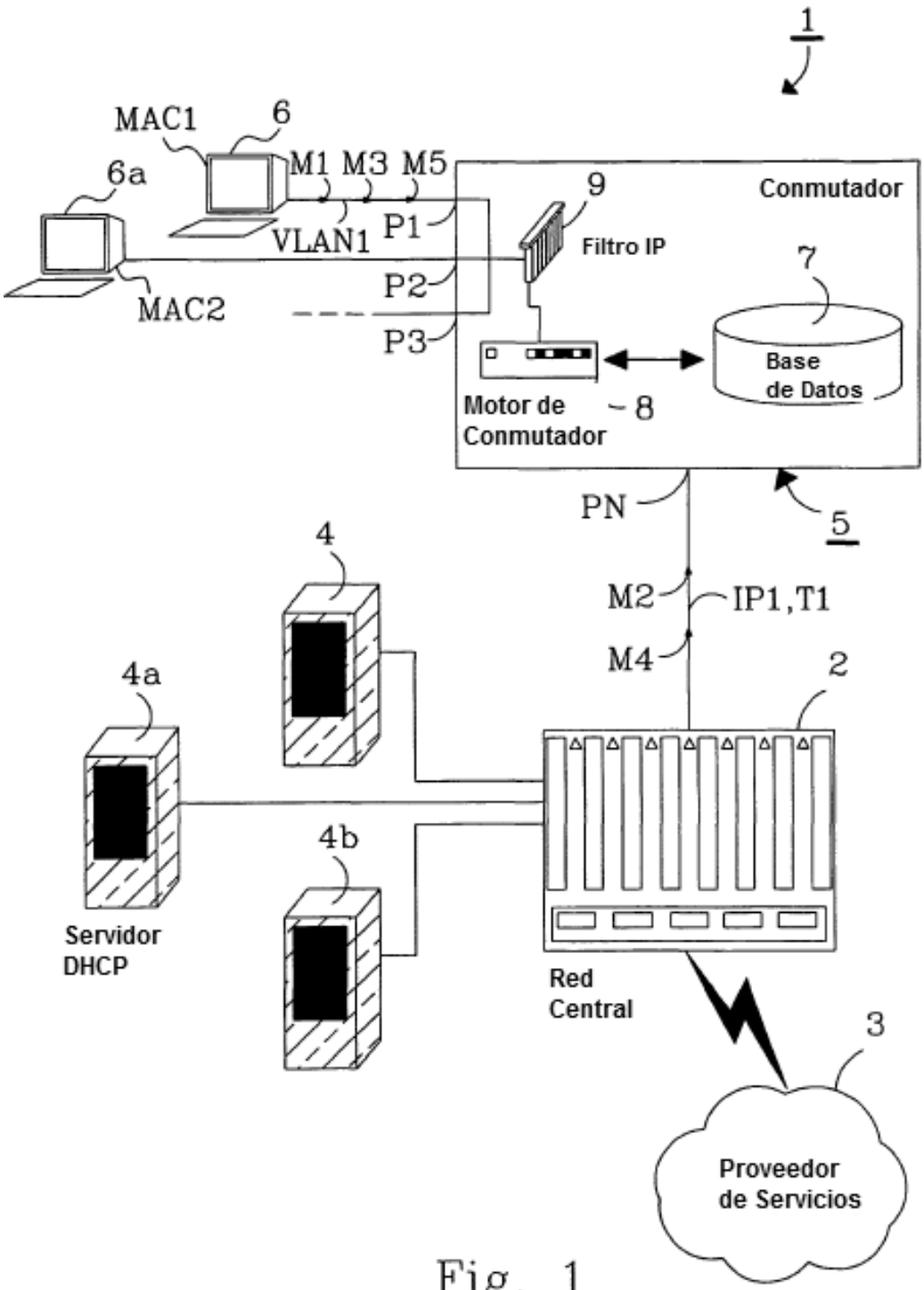
1
MAC1
6
6a
M1 M3 M5
VLAN1
P1
P2
P3
MAC2
9
Filtro IP
Conmutador
7
Base
de Datos
Motor de
Conmutador
8
PN
5
4
M2
IP1,T1
M4
2
4a
4b
Servidor
DHCP
Red
Central
3
Proveedor
de Servicios

Fig. 1

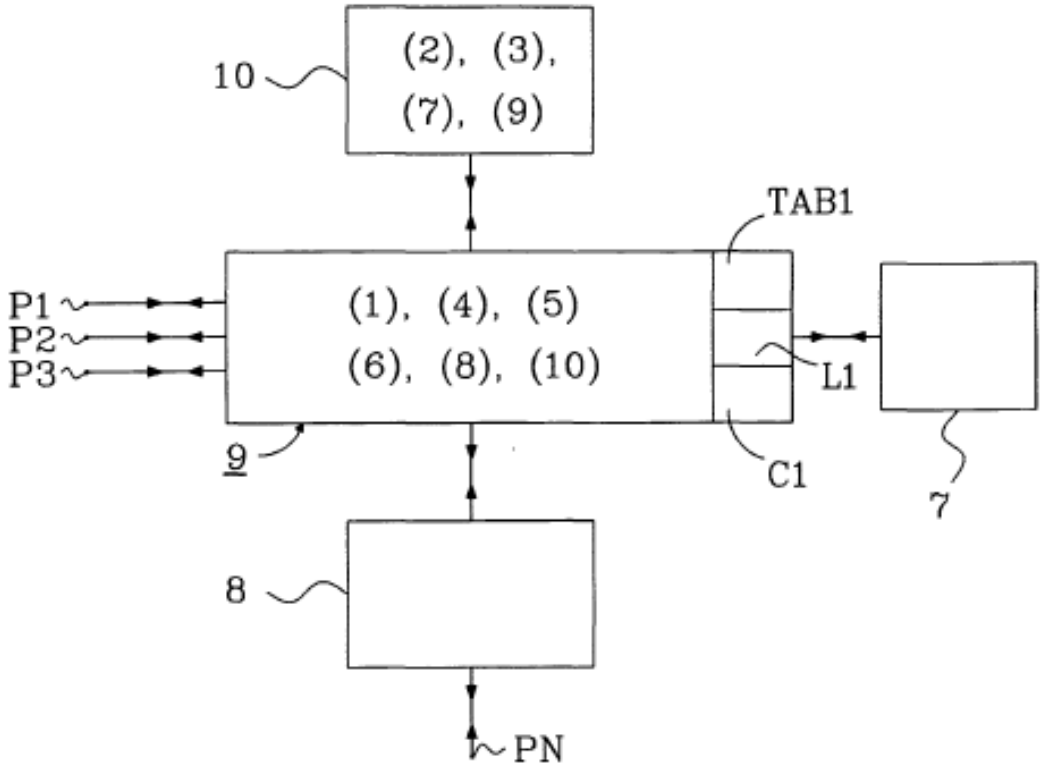

Fig. 2

31	Abonado	MAC1	MAC2
32	Puerto nº.	P1	P2
33	Identidad de VLAN	VLAN1	VLAN2
34	Dirección IP	IP1	IP2
35	Tiempo de cesión	T1	T2

TAB1

Fig. 3

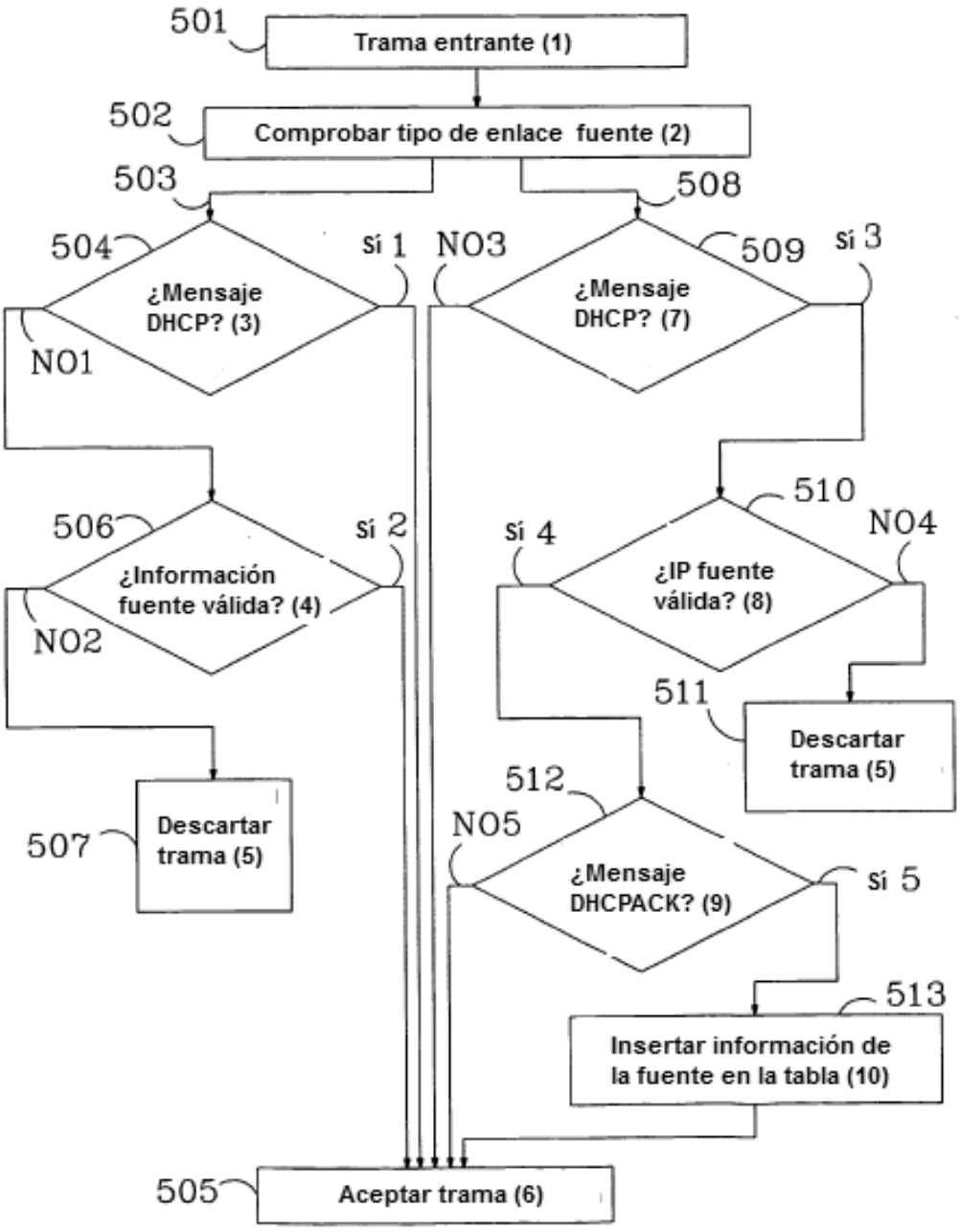
501
Trama entrante (1)
502
Comprobar tipo de enlace fuente (2)
503
508
504
¿Mensaje DHCP? (3)
Sí 1
NO3
509
¿Mensaje DHCP? (7)
Sí 3
NO1
506
¿Información fuente válida? (4)
Sí 2
NO2
510
Sí 4
¿IP fuente válida? (8)
NO4
511
Descartar trama (5)
512
NO5
¿Mensaje DHCPACK? (9)
Sí 5
507
Descartar trama (5)
513
Insertar información de la fuente en la tabla (10)
505
Aceptar trama (6)

Fig. 5

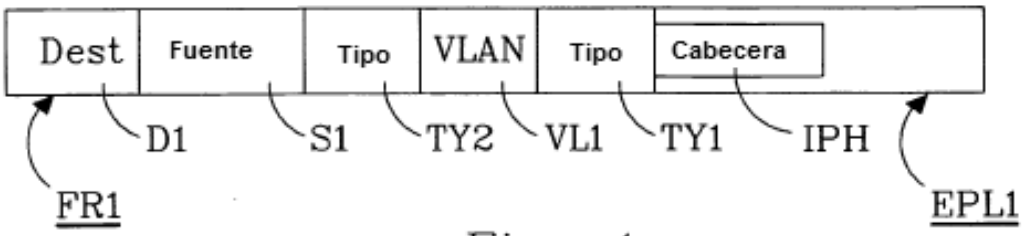

Fig. 4

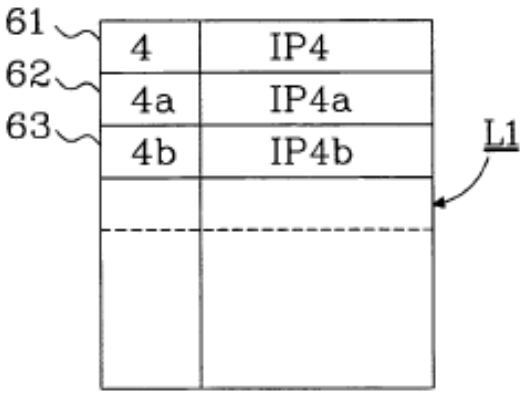

Fig. 6

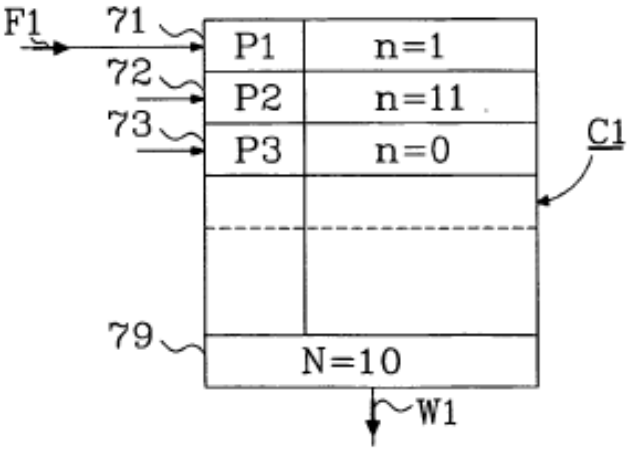

Fig. 7

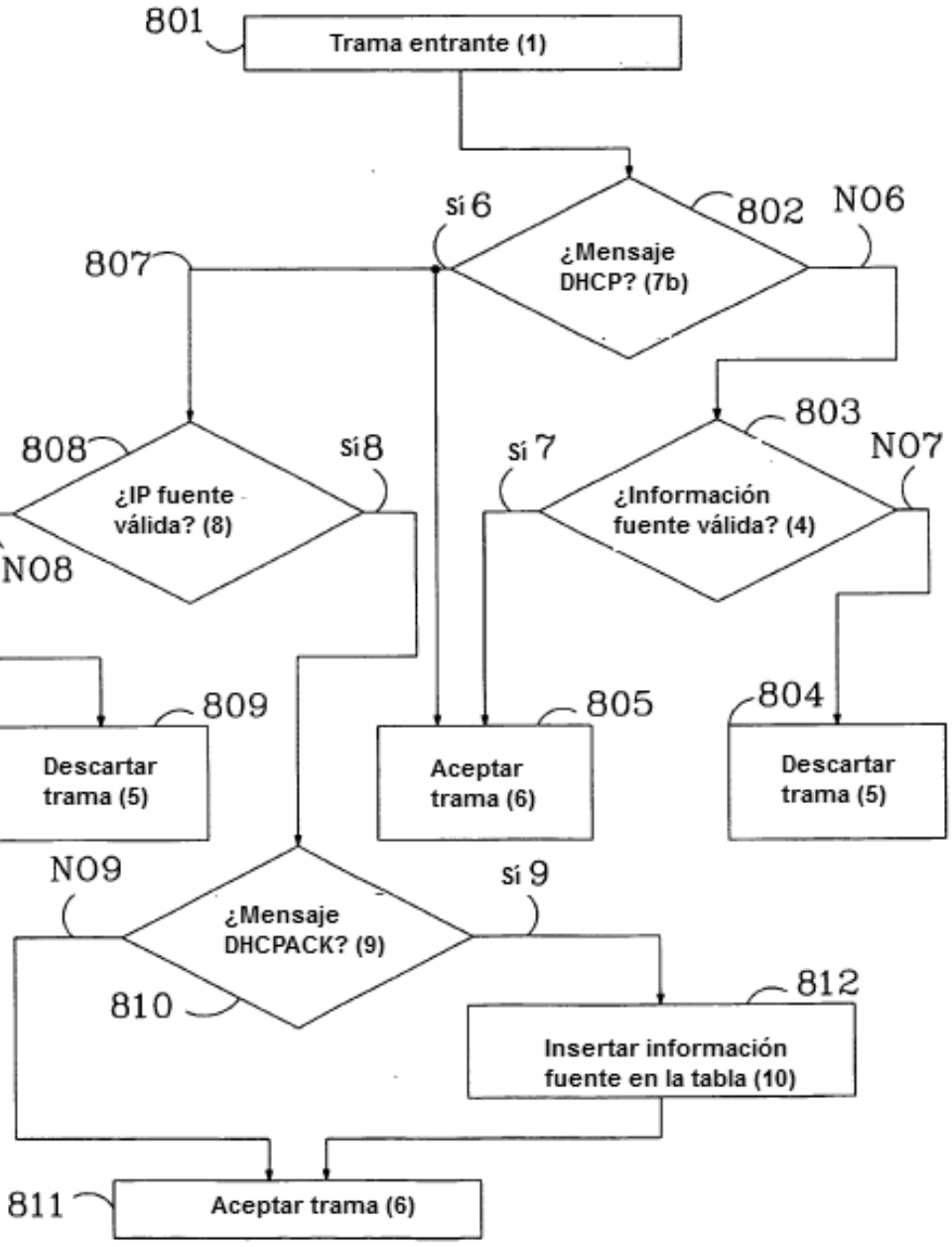
801
Trama entrante (1)
Sí 6
802
N06
¿Mensaje DHCP? (7b)
807
808
Sí 8
¿IP fuente válida? (8)
N08
803
Sí 7
N07
¿Información fuente válida? (4)
809
Descartar trama (5)
805
Aceptar trama (6)
804
Descartar trama (5)
N09
Sí 9
¿Mensaje DHCPACK? (9)
810
812
Insertar información fuente en la tabla (10)
811
Aceptar trama (6)

Fig. 8