



①9



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

①1 Número de publicación: **2 334 634**

⑤1 Int. Cl.:
H04L 29/06 (2006.01)
H04L 12/14 (2006.01)

①2

TRADUCCIÓN DE PATENTE EUROPEA

T3

⑨6 Número de solicitud europea: **00982804 .7**
⑨6 Fecha de presentación : **22.12.2000**
⑨7 Número de publicación de la solicitud: **1240764**
⑨7 Fecha de publicación de la solicitud: **18.09.2002**

⑤4 Título: **Servidor y método para proveer acceso a una red.**

③0 Prioridad: **23.12.1999 CA 2293765**

④5 Fecha de publicación de la mención BOPI:
15.03.2010

④5 Fecha de la publicación del folleto de la patente:
15.03.2010

⑦3 Titular/es: **Solutioninc. Ltd.**
5692 Bloomfield St.
Halifax, NS B3K 1T2, CA

⑦2 Inventor/es: **Wilson, Tim**

⑦4 Agente: **Isern Jara, Jorge**

ES 2 334 634 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Servidor y método para proveer acceso a una red.

5 **Campo del invento**

Este invento se relaciona en general con redes LAN, WAN y el acceso a las mismas y otras redes por parte de usuarios móviles cuyos ordenadores no estén necesariamente configurados para la red con la cual se están conectando.

10 **Antecedentes del invento**

Al describir el invento a veces se emplean términos diferentes para referirse al equipo del usuario móvil que se conecta a una red diferente de la red para la cual el ordenador del usuario ha sido configurado. El equipo es típicamente un ordenador laptop, pero puede ser cualquier tipo de unidad o sistema de procesamiento similar. Durante toda esta especificación se le puede hacer referencia como un ordenador, ordenador laptop, notebook, ordenador notebook, asistente digital personal, sistema, ordenador del cliente, y móvil. En la actualidad, un usuario no puede llevar un ordenador que ha sido configurado para operar con su ISP personal o la red LAN/VVLAN de las oficinas de su empleador, conectarlo a otra red y esperar que funcione. En un ambiente TCP/IP (Transport Control Protocol/Internet Protocol) tradicional, un usuario típicamente debería reconfigurar manualmente un dispositivo tal como un ordenador notebook para obtener acceso a otras redes TCP/IP. Los protocolos de comunicaciones actuales TCP/IP de todos los sistemas operativos, por ej., Unix, Linux, Windows, Mac, etc., han sido diseñados para operar en un ambiente preprogramado y no para ser móviles. Los usuarios móviles pueden en la actualidad conectarse telefónicamente a un ISP con un módem para tener acceso a Internet. Sin embargo, las redes de conexión telefónica son más lentas que la Ethernet y redes del tipo, y pueden ser costosas si el usuario debe conectarse a larga distancia para tener acceso a su ISP. Además, las redes de conexión telefónica pueden ocupar líneas telefónicas y recursos PBX, lo cual puede resultar inconveniente en un ambiente tal como un hotel. Al presente, no existe una forma sencilla y eficaz de autorizar y controlar el acceso a una red por parte de los usuarios móviles que no sea hacerlo manualmente. Tampoco hay en estos momentos posibilidad de recopilar y mantener información para la facturación de los servicios utilizados por el usuario móvil.

EP 0899 925 revela un sistema para conectar los ordenadores de los clientes a una red comunicaciones con un sistema para clientes y un sistema de servidor. El sistema de clientes usa pautas de red especiales para la red conectada al servidor.

WO 99 38303 revela un sistema que cuenta con un servidor proxy y un concentrador. El proxy está ubicado entre dos redes diferentes, y ejecuta la traducción de una dirección de red.

Es conveniente suministrar un nuevo servidor con una red y método que permita al ordenador del cliente, que está configurado para una segunda red, el fácil acceso a una red sin modificar su software o hardware existente, y que ofrezca servicios de facturación al cliente.

Un objeto del presente invento es dar solución a uno o más de los problemas que se acaba de citar. El presente invento apunta a un método y aparato que permita a los usuarios remotos el acceso a servicios TCP/IP independientemente de las configuraciones TCP/IP de su ordenador remoto. Los usuarios pueden sencillamente enchufar su Tarjeta de Interfaz de Red (Network Interface Card o NIC) a una toma de datos de red para tener acceso instantáneo a servicios TCP/IP de alta velocidad sin la necesidad de tener una cuenta en ningún ISP en particular.

Según una corporización del invento, un servidor permite acceso remoto a la World Wide Web sin modificaciones al ordenador del usuario móvil remoto. No es necesario añadir software ni hardware al ordenador remoto, ni tampoco se precisa modificaciones de configuración o de hardware. Las ventajas del presente invento incluyen: facilidad de uso, ningún cambio necesario en el ordenador remoto, y para un hotel o miembro de la industria de servicios que desee proveer a sus clientes conexión instantánea para el acceso a Internet, pueden obtenerse ganancias, u ofrecer un servicio a sus clientes al tiempo de reducir las demanda a su sistema telefónico interno (PBX).

Según otro aspecto del presente invento, se provee un método para permitir a un usuario acceso a una red para un ordenador configurado para una primera red. El método se implementa mediante un servidor que permite al ordenador acceso a la red a través de una segunda red sin necesidad de software existente iniciado por el cliente ni de cambios en la configuración del hardware existente. El método incorpora los pasos de determinación y asignación automática de una dirección de Internet Protocol (IP) para el ordenador conectado a la segunda red; el registro del ordenador en relación con la información de direccionamiento, incluyendo la dirección IP asignada, y una dirección de Media Access Control (MAC) del ordenador; el almacenaje y mantenimiento de la información de direccionamiento de los ordenadores registrados; paquetes de filtro para sólo permitir el acceso a la red de los usuarios de ordenador registrados; la traducción de una dirección IP en un paquete en base a la dirección, y el direccionamiento transparente del tráfico a y desde el ordenador, a y desde la red, sobre la base de la información de direccionamiento. El paso de registro incluye el paso de recopilación y mantenimiento de información del estado de facturación y registro, en el cual el paso de recopilación y mantenimiento incluye el paso de identificación del ordenador para fines de facturación mediante el uso de Simple Network Management Protocol (SNMP) y una arquitectura de conmutación de red para identificar un puerto de conmutación al cual esté conectado el ordenador.

Otro aspecto del invento es un medio que pueda leerse por ordenador y contenga instrucciones para el ordenador que, al ejecutarse en el ordenador, desarrollan el método antedicho.

Según un aspecto más del presente invento, se provee un servidor para permitir el acceso de un usuario a la red para un ordenador configurado para una primera red. El ordenador está provisto para permitir el acceso del ordenador a la red mediante una segunda red sin necesidad de reconfigurar el ordenador a través del hardware o software existentes. El servidor incorpora un módulo de registro para registrar el ordenador que accede a la red, un driver de registro para la asignación transparente de la dirección IP al ordenador, para el mantenimiento y acceso de la información de dirección incluyendo la dirección IP asignada y una dirección MAC del ordenador, y para la recopilación y mantenimiento de información de estado de facturación y registro; una interfaz interna para la conexión del servidor al ordenador; una interfaz externa para conectar el servidor a la red, un módulo de driver de paquete para ejecutar NAT en la interfaz interna en base a la dirección MAC; un filtro de paquete para filtrar los paquetes y permitir la transmisión de los paquetes a y desde la interfaz externa desde y a la interfaz interna en base al estado de registro; un módulo DHCP para tramitar la solicitud DHCP en base a la dirección IP asignada; y un módulo ARP para detectar una solicitud ARP y para hacer que el driver de registro asocie la dirección MAC y las dirección IP asignada, y un demonio SNMP para identificar el ordenador para fines de facturación mediante el uso de un Simple Network Management Protocol (SNMP) y una arquitectura de conmutación de red para identificar un puerto de conmutación al cual el ordenador esté conectado. En respuesta al tráfico del ordenador a la red, el servidor redirige transparentemente el tráfico y permite acceso a la red en base a la información de direccionamiento.

Otro aspecto del invento provee funcionalidad de facturación. El servidor bloquea todo intento de acceso a Internet o el correo electrónico de un usuario si éste aún no se ha registrado para el servicio. El servidor también guarda registro del tiempo que cada usuario pasa en línea durante cada sesión, y envía esta información al hotel o centro de conferencias para fines de facturación.

Breve descripción de los planos

La Fig. 1 es una representación ilustrada de una conexión de servidor típica dentro de un ámbito hotelero.

La Fig. 2 muestra un diagrama de bloques funcional de una corporización del presente invento.

La Fig. 3 muestra un ejemplo de los componentes principales y las interacciones del servidor según el presente invento.

La Fig. 4 muestra un ejemplo del procesamiento de una solicitud DHCP.

La Fig. 5 muestra un ejemplo del procesamiento de una solicitud ARP.

La Fig. 6 muestra un ejemplo del procesamiento de una solicitud HTTP no registrada.

La Fig. 7 muestra un ejemplo del procesamiento de una solicitud HTTP registrada.

La Fig. 8 muestra los componentes de facturación y sus interacciones.

Descripción de las corporizaciones preferidas

A continuación se presenta la descripción detallada del invento, incluyendo la descripción del mejor modo de implementación de los inventos. La descripción se hace con referencia a los planos.

Una corporización del presente invento implica su uso en la industria de la hotelería. El objetivo primario es ofrecer a los huéspedes la posibilidad de acceder a Internet desde su cuarto del hotel sin tener que modificar las pautas de red de su ordenador móvil. Los huéspedes podrán con total transparencia y facilidad recibir su correo electrónico, navegar la web, y desarrollar sus actividades normales en la Internet.

Introducción

La corporización comercial del servidor y método del invento está identificada por marca SolutionIP™. Periódicamente se hace referencia al invento a través de su marca, y significa el servidor y/u otros aspectos del invento según lo dicte el contexto. Este invento es de utilidad en edificios de unidades múltiples, ya sea que se utilicen como oficinas, apartamentos y/o para hoteles o edificios de alojamiento similares. La inmediata conectividad permite a los arrendatarios (o huéspedes) del edificio cambiar de ubicación y volver a conectarse a Internet desde cualquier lugar del edificio, permitiendo que el acceso a Internet sea transparente y sin inconvenientes. También es ventajoso usar el invento en salones de seminario, salas de reuniones, salones de formación, y afines, en los que los usuarios deseen acceder a la red LAN desde el salón utilizando su propio ordenador.

Una implementación preferida de SolutionIP™ es para la industria de la hotelería. El objetivo primario es permitir a los huéspedes la posibilidad de acceder a Internet desde su cuarto en el hotel sin tener que modificar las pautas de red de su ordenador personal. Los huéspedes podrán, con total transparencia y facilidad, recibir correo electrónico, navegar la web, etc., tal como si estuvieran en sus propias oficinas.

Escenario de uso

Un escenario de uso típico para el invento SolutionIP™ se ilustra en la Fig. 1 y consiste en un viajante de negocios que precisa tener acceso al servidor de correo electrónico de su empresa desde su cuarto del hotel. Tras conectar su laptop 101 al toma de red del cuarto del hotel 102 y registrarse para el acceso al servicio SolutionIP™, el huésped del hotel puede tener acceso a Internet, al igual que a los servicios en línea del hotel 104 (por ej., Conserje Virtual) a través de la conexión de Internet de alta velocidad del hotel. Entonces puede conectarse al servidor de correo electrónico de su empresa a través de la Internet a velocidades mucho más altas que las permitidas por la conexión telefónica a la red. El invento de servidor 103 permite conectividad transparente y sin inconvenientes.

SolutionIP™ es una solución a base de servidor diseñada para permitir a los usuarios conectar un ordenador a la Internet mediante una Tarjeta de Interfaz de Red (Network Interface Card o NIC) Ethernet corriente y una configuración red basada en IP. Los huéspedes físicamente se conectan al sistema SolutionIP™ a través de una conexión de interfaz de red. La mayoría de los usuarios lograrán conectividad sin inconvenientes. Sin embargo, hay limitaciones, que se describen a continuación.

Se exige a los usuarios registrarse en el sistema a través de una aplicación de navegador, antes de establecer la conectividad con Internet. El servidor detecta todo intento de lograr acceso a Internet y sigue redirigiendo a los usuarios al sitio web de SolutionIP™ hasta que completen el registro. Una vez registrados, los usuarios podrán usar la conexión a Internet de alta velocidad del hotel para tener acceso a los recursos informáticos y el correo electrónico de su corporación, recorrer la World Wide Web (WWW), etc.

Los huéspedes que intenten leer o bajar su correo electrónico sin registrarse reciben un mensaje de correo electrónico. Este mensaje simplemente les solicita registrarse usando su navegador para poder bajar su correo electrónico.

Generalidades de funcionalidad

SolutionIP™ traduce el tráfico de red del ordenador del cliente (huésped del hotel) de modo tal que pueda ser apropiadamente dirigido a y desde el cliente a través de la conexión de Internet del hotel. Esto es posible independientemente de las pautas de red corrientes (dirección IP, servidores DNS, portal, etc.) en la máquina del cliente, siempre que la configuración existente sea funcional (esto significa que la máquina del cliente debe contar con una configuración de red operante, si bien las direcciones reales utilizadas no tienen que estar configuradas para la red del hotel): SolutionIP™ traduce con transparencia las pautas de la máquina del cliente a direcciones apropiadas para el ámbito de la red del hotel, a la vez que dirige los datos a la Internet. Además, el servidor efectúa la “traducción inversa” del tráfico de red de regreso para que use direcciones compatibles con la configuración del ordenador del cliente.

Más específicamente, en la actualidad sólo se apoyan protocolos a base IP. Otros tipos de tráfico de red se ignoran, y no son dirigidos por SolutionIP™. SolutionIP™ provee funcionalidad de servidor DHCP (Dynamic Host Configuration Protocol), que se utiliza para suministrar configuración de datos a los clientes configurados para obtener dinámicamente sus pautas de red. Las solicitudes de DNS (Domain Name Service) son interceptadas por SolutionIP™ (en base al número de puerto de destino) y son procesadas localmente por el servidor DNS en funcionamiento en el hotel. El tráfico de red de salida es interceptado por el servidor SolutionIP™, que actúa como portal a la Internet y transmite los datos según resulte apropiado. SolutionIP™ simula ser el portal del cliente, aún cuando el cliente haya especificado un portal diferente, tal como el que el cliente normalmente utiliza en la oficina.

SolutionIP™ bloquea el uso no autorizado de la red (o sea, el tráfico de red de los clientes que no se han registrado para el servicio de red) hasta que el cliente se registre. SolutionIP™ mantiene una lista de los ordenadores de los clientes que se han registrado y que están autorizados a usar la red. El tráfico de los clientes autorizados se transmite, mientras que todo otro tráfico se descarta o redirige.

La Fig. 2 provee un diagrama de bloques funcional del invento en una aplicación de hotel típica.

El huésped 201 se conecta a la red del hotel y el servidor SolutionIP™ 202 ejecuta las funciones apropiadas para manejar el tráfico del navegador 205 (HTTP), correo electrónico 206 (POP3), tráfico de servicios del hotel (207) (IP (TCP, UDP)) y tráfico de Internet 208 (IP(TCP,UDP)). El servidor 202 también ofrece una función para manejar el tráfico de mantenimiento 209 de los servicios del hotel. Los datos de facturación 210 se recopilan y mantienen en el servidor y se suministran a los servicios del hotel según sea necesario.

Un huésped puede comunicarse con el servidor SolutionIP™ a través de solicitudes de Hypertext Transfer Protocol (HTTP) 205 (el protocolo empleado para el acceso a la WWW), o solicitudes de correo electrónico 206 (POP3). Una vez registrado, el tráfico con base IP que se origine en el ordenador del huésped pasa por el servidor SolutionIP™ a la Intranet de los Servicios del Hotel 203 o a la Internet Pública 204.

ES 2 334 634 T3

En general, la solución SolutionIP™ no está directamente relacionada con intentos de asegurar la red del hotel contra amenazas externas. La creación y el cumplimiento de una política de seguridad para la conexión de Internet del hotel debe ser tratada por otros componentes de la solución total. SolutionIP™ no realiza filtros del tráfico de entrada en la red destinado a los clientes registrados.

El servidor SolutionIP™ tiene desactivados los servicios innecesarios, y los permisos de archivo se verifican para tratar de evitar modificaciones maliciosas. El único acceso de ingreso al servidor SolutionIP™ es a través de una cubierta segura (SSH), conexión en serie o desde la consola.

Componente de registro y de uso

El componente de registro es una aplicación basada en la web que permite a los huéspedes del hotel registrarse para el servicio de red, al igual que salir del sistema. Es accesible para todos los huéspedes que estén conectados a la red (o sea que SolutionIP™ no bloquea el acceso al sitio de registro). El servidor web para el componente de registro puede operar desde una máquina independiente de la de utilizada para SolutionIP™, minimizando así la carga para SolutionIP™.

Previamente al registro para los servicios de red, SolutionIP™ detecta e intercepta todo intento de acceso a servidores de WWW y POP3 (un tipo de correo electrónico). Esto se basa en el número de puerto TCP. SolutionIP™ responde a estas solicitudes o las envía al servidor web que suministra información sobre cómo registrarse para el servicio de red del hotel. Si bien esta corporización es específicamente para POP3, también podría incluirse otros protocolos de correo electrónico.

SolutionIP™ también puede rastrear la información de registro, que puede emplearse para fines de facturación. En la actualidad, esta información se encuentra disponible a través de un sitio web de administración que exhibe quién está conectado a la red, quién está registrado, la hora y fecha de registro, etc. El servidor podría incluir una función para rastrear los volúmenes de datos.

Requisitos de los clientes

Si bien el sistema es una solución transparente y de servidor único para los clientes registrados, existen ciertos requisitos mínimos para los ordenadores de los clientes. SolutionIP™ está diseñado para operar sin modificaciones en la configuración del ordenador del cliente en la mayoría de los casos, pero ciertos componentes deben estar presentes y operativos. Una utilidad podría permitir el acceso de ciertos sistemas a la red cuando el cliente no cumpla con los requisitos mínimos.

Los requisitos mínimos de los clientes son:

- Tarjeta de Interfaz de Red Ethernet instalada y configurada, con interfaz compatible con los tomas de la red del hotel;

- Pila TCP/IP instalada, configurada para DHCP o para la dirección IP estática, portal, y servidor(es) DNS; y

- navegador de red configurado para el acceso directo a la red (o sea, no una configuración de navegador sólo para la conexión telefónica y sin proxies habilitados). (Sólo necesario para el procedimiento de registro/finalización de sesión y

Los requisitos descriptos en este documento bastan para permitir que la mayoría de los clientes se conecten con facilidad a la Internet a través de las instalaciones del red del hotel. Sin embargo, algunos clientes contarán con configuraciones de sistema que no permitirán la conectividad a través del servidor SolutionIP™.

Diseño de alto nivel

SolutionIP™ permite un acceso transparente a la red a través de dos mecanismos:

- Traducción de Dirección de Red (Network Address Translation o NAT): Cada sistema interno recibe una dirección IP exclusiva para comunicarse con la Internet. Esto permite a los clientes conexiones externas y también facilita los protocolos con base UDP, pero necesitará la disponibilidad de una cantidad suficiente de números IP enrutables para su asignación a cada instalación.

- Máscara: Cada sistema interno aparece al mundo exterior bajo la dirección IP del servidor. Esto precisa gestores de detección de protocolo especiales (proxies) para protocolos tales como FTP modo activo que tratan de crear conexiones de retorno independientes para el cliente, y también se hacen modificaciones para apoyar las "conexiones" UDP (inspección dinámica de paquete).

ES 2 334 634 T3

SolutionIP™ utiliza NAT como mecanismo primario para permitir un acceso transparente a la red. A pesar de los problemas asociados con la asignación de un número IP, esta opción ofrece el mejor mecanismo posible para manejar eficientemente los diversos protocolos de red que no estén apoyados por el sistema. La corporización preferida del invento se basa en una versión adaptada del sistema operativo Linux.

Existen dos escenarios principales:

- Se configura al cliente para usar una configuración IP fija en particular. El servidor captura las solicitudes de Protocolo de Resolución de Dirección (Address Resolution Protocol o ARP) por parte del cliente, y el servidor responde con su propia dirección de Control de Acceso de Medio (Media Access Control o MAC). Al cliente se le asigna una dirección IP, que se conecta a la dirección IP configurada del cliente y su dirección MAC. Si el cliente no está “registrado” para el servicio, todo intento de comunicarse con un servidor web o un servidor pop hará que sea redirigido a la pantalla de registro (web) o que reciba un mensaje de correo con instrucciones para exhibir la pantalla de registro. Una vez registrado, el cliente abandona el sistema de registro, y su tráfico informático puede proseguir sin impedimentos. Cuando el tráfico pasa por el servidor, la dirección IP del cliente se traduce en una y otra dirección entre la dirección IP configurada (fija) y dirección IP asignada por el servidor.

- El cliente usa DHCP. En este caso, el componente de servidor DHCP de SolutionIP™ asigna una dirección IP, y luego SolutionIP™ simplemente actúa como un router, con la diferencia de que se bloquea o redirecciona el tráfico IP normal hasta que el cliente haya completado el proceso de registro.

Componentes principales del servidor y sus interacciones

La Fig. 3 muestra un desglose de los componentes principales del invento y sus interacciones. Estos componentes se describen en mayor detalle a continuación.

ARP

El módulo ARP 307 del servidor usa ARP, un protocolo de red estándar cuyo comportamiento se describe a continuación.

- ARP (Address Resolution Protocol) (Consulte RFC-826 (RFC significa Request For Comment (Solicitud de Comentario) y es un método estándar para solicitar comentarios sobre las normas y otros aspectos de la operación de la Internet a través de la Internet. Una dirección que resulta útil para acceder a los diversos RFC es www.faqs.com) para la especificación del protocolo) está dirigido a proporcionar un método para que una máquina obtenga la Dirección MAC (Media Access Control) de un sistema para el cual se conoce la dirección IP. Típicamente, una máquina determinará que la máquina con la que desea comunicarse pertenece a la misma red local mediante la comparación de la dirección IP de la máquina objetivo con su propia dirección IP. Si la máquina con la que quiere comunicarse pertenece a la misma red, en la actualidad no hay asociación entre la dirección IP del sistema objetivo y una dirección MAC, entonces la máquina efectuará una solicitud ARP en relación con la dirección IP de la máquina. Si la máquina objetivo está activa, deberá estar atenta a las solicitudes ARP, y si la dirección IP especificada en la solicitud ARP concuerda con la dirección IP de la máquina objetivo, entonces responderá a la solicitud ARP.

El protocolo de resolución de dirección es un protocolo utilizado por el protocolo de la capa de red de Internet Protocol (IP) para relacionar las direcciones de la red IP con las direcciones de hardware empleadas por el protocolo de enlace de datos. Este protocolo se usa por debajo de la capa de red como parte de la capa de enlace OSI, y se usa cuando IP se utiliza por Ethernet. El término resolución de dirección se refiere al proceso de hallar una dirección de un ordenador en la red. La dirección se “resuelve” utilizando un protocolo en el cual cierta información es enviada por el proceso de un cliente ejecutado en un ordenador local a un proceso de servidor ejecutado en un ordenador remoto. La información recibida por el servidor permite al servidor identificar de forma exclusiva el sistema de red para el cual se solicitó la dirección, y en consecuencia proporcionar la dirección solicitada. El procedimiento de resolución de dirección se completa cuando el cliente recibe una respuesta del servidor con la dirección solicitada.

- Proxy-ARP (Ver una descripción en RFC-1009) es una variación del protocolo ARP en la cual un router (un sistema con más de una interfaz que dirige paquetes entre redes en o a través de redes en cada interfaz) responderá a las solicitudes ARP de sistemas en una interfaz efectuados por sistemas en otra interfaz con su propia dirección MAC. Esto es para dar apoyo a situaciones en las que es necesario o conveniente dividir una red sin crear subredes, o cuando las máquinas que no pueden comprender subredes deben residir en redes con subredes.

SolutionIP modifica los comportamientos estándar que se acaban de describir sobre una base de “interfaz por interfaz” mediante la respuesta promiscua a las solicitudes ARP. Se trata de una extensión de Proxy-ARP. En general, el Servidor SolutionIP responde a toda solicitud ARP con una dirección MAC del Servidor SolutionIP independientemente de la dirección IP que se solicite, con las siguientes excepciones:

1. Microsoft Windows y otros sistemas operativos, al arrancar, envían una solicitud ARP para la dirección IP para la cual están configurados, y si reciben una respuesta, cierran esa interfaz y no intentan ninguna actividad de red. Esta

ES 2 334 634 T3

es una prueba para asegurar que la dirección IP a utilizar por el sistema es exclusiva, y para evitar conflictos. Estos paquetes de prueba tienen características exclusivas que permiten al servidor SolutionIP reconocerlos y no responder a estos paquetes.

2. Si la solicitud ARP es para un sistema para el cual el Servidor SolutionIP cuenta con una entrada en el driver de registro, entonces se deja que el sistema responda, en lugar de responder el Servidor SolutionIP.

3. En el caso en que el Servidor SolutionIP precise una dirección MAC para una dirección IP, primero se determina si existe una entrada en el driver de registro, y de ser así, usa esa dirección MAC en lugar de enviar una solicitud ARP.

Esto permite al servidor SolutionIP simular ser un portal (router implícito), Servidor DNS, etc. para clientes que utilicen configuraciones IP fijas. Además, el servidor evita demoras para la comunicación con sistemas en las redes de su cliente mediante el uso del driver de registro en lugar de efectuar solicitudes ARP.

Driver de dispositivo de registro (a veces denominado Dispositivo Soln)

El driver de dispositivo de registro 304 es un pseudo-driver desde el punto de vista que no está en realidad asociado con ningún dispositivo físico, sino que el dispositivo son los datos de registro almacenados y gestionados por este driver. La información de registro mantenida por el driver incluye:

- IP original: es la dirección IP original que el cliente usó para comunicarse con el servidor. Bajo ciertas circunstancias, puede ser igual a la dirección IP asignada. Un cliente con IP fijo configurado tiene la dirección IP para la cual el cliente está configurado. Para un cliente configurado con DHCP generalmente será cero o la dirección IP asignada al cliente en la red previa, o será igual a la dirección IP asignada.

- IP asignado: es la dirección IP asignada al cliente por el servidor de registro, y es un número elegido entre las direcciones IP disponibles en las gamas de direcciones que el driver está configurado para apoyar. Siempre se asigna una dirección IP a cada dirección MAC nueva que se encuentra. Si la dirección IP original es igual a una dirección IP no asignada que el driver está configurado para apoyar, entonces se asigna esa misma dirección IP; de lo contrario, se le ofrecerá la siguiente dirección IP disponible.

- Dirección MAC: es la dirección MAC del sistema del cliente.

- Hora de creación: es la hora en que se asignó la dirección IP a esta MAC, y ocurre cuando se recibe el primer paquete del cliente.

- Hora de registro: es la hora en que se registró el cliente (para el acceso a Internet) al completar el proceso de registro para esa localidad.

- Caducidad de registro: es la hora en que el registro caduca (se pierde el acceso a Internet).

- Caducidad de entrada: es la hora en que la dirección IP asignada regresará al grupo de direcciones IP libres.

- Último uso: la última vez que hubo tráfico desde/a el sistema del cliente.

- Banderas: usadas para contener campos de bits empleados para indicar el estado y la naturaleza de un cliente en particular (o sea, registrado, DHCP, válido, permanente, no caducado, etc.)

El acceso y manipulación de esta información se hace a través de otros drivers núcleo y procesos mediante llamadas de función definidos en el Driver de Dispositivo de Registro 304. El usuario determina el acceso a las aplicaciones y manipula la información de registro con la interfaz estándar del dispositivo Linux y las llamadas ioctl asociadas. Las entradas pueden buscarse utilizando la dirección IP original, la dirección MAC o la dirección IP asignada. Todos los rasgos de una entrada pueden manipularse, si bien no todos directamente; puede marcarse una entrada como registrada y el driver asignará una hora de caducidad de registro. Ciertos intentos de buscar una entrada provocarán la asignación de una entrada si no se puede hallar una entrada existente; específicamente, la llamada soln_get_aip_mac hará que se asigne una dirección IP a la dirección MAC específica si no puede hallarse una entrada existente. Puede obtenerse un volcado total del estado actual del driver a través de la apertura y lectura del dispositivo. Asimismo, esta información puede usarse para inicializar el driver mediante la apertura del dispositivo y la escritura de la misma (o similar) información en el dispositivo. Esto permite la posibilidad de backup y reposición del estado actual del driver, minimizando así los efectos de rearranques en clientes registrados. Además de la información ya descrita, la información de estado del driver incluye:

- La frecuencia con que se actualiza el tiempo corriente del driver (granularidad temporal).

- La frecuencia de operación de un algoritmo de purga que busca entradas no registradas y de la purga las entradas no registradas

ES 2 334 634 T3

-Cuál es el modo de caducidad implícito para el sistema, que puede incluir cualquiera de lo siguiente:

0. NO_EXPIRY (sin caducidad): ninguna entrada caduca automáticamente.

1. RELATIVE_OFFSET_EXPIRY (período de tiempo fijo): cuando las entradas caducan a un tiempo fijo en relación con su hora de registro.

2. TIMEOFDAY_EXPIRY (hora del día): cuando las entradas caducan a una hora determinada del día sin importar la hora de registro.

- El período es el tiempo establecido para el modo Relative Offset o el tiempo del modo Timeofday, dependiendo del método de caducidad elegido.

- El período de gracia de Timeofday se usa para determinar si la segunda hora de caducidad de Timeofday ha de usarse en lugar de la siguiente. En otras palabras, si la hora de caducidad es las 11.00 de la mañana, y el período de gracia es media hora, entonces si alguien se registra entre las 10.30 y las 11.00, en realidad se registran hasta el día próximo en lugar de registrarse por sólo media hora o menos.

- El tiempo de inactividad que se utiliza para decidir si caducar una entrada no registrada, en esencia si se ha detectado actividad para una entrada dentro del período de desconexión por inactividad, la entrada no se purga.

- La cantidad de gamas disponibles para asignar a los clientes.

- La gama de datos, cada gama se especifica mediante una dirección IP inicial y una dirección IP final. Las direcciones IP deben aparecer en la forma A.B.C.x y A.B.C.y, donde $0 \leq x \leq y \leq 255$. De este modo, cada gama puede constar de hasta 256 entradas, lo cual permite gamas múltiples para especificar una red más grande que una subred de clase C.

Además de los eventos de activación externa, el driver de registro cuenta con ciertas actividades automáticas que ejecuta sobre una base regular (configurable):

- Si el tiempo corriente es superior al tiempo de caducidad de registro de una entrada, entonces el driver anula el registro de una entrada, a menos que la entrada esté marcada como sin caducidad.

- Si el tiempo corriente es superior al tiempo de caducidad de entrada de una entrada, entonces el driver purga la entrada (regresa el IP asignado al grupo de direcciones IP asignadas disponibles) a menos que la entrada esté marcada como permanente.

- El driver de registro actualiza su concepto en cuanto a la hora actual.

Interfaz de toma TCP/IP

La interfaz de Toma TCP/IP (311) es un toma estándar de interfaz de red provisto por Linux, Unix, y muchos otros sistemas operativos que aportan servicios de red.

Interfaz de línea de comando/Demonio Soln

La Interfaz de Línea de Comando (317) permite una herramienta administrativa y de diagnóstico para los administradores del sistema. Sirve como una interfaz de espacio de usuario en el driver de registro. Cuenta con opciones para la mayoría de las ioctl del Driver de Registro. Puede emplearse para verificar el estado corriente del driver de registro 304 o para modificarlo.

El Demonio Soln 315 comparte la misma base de código que la Interfaz de Línea de Comando 317, y por lo tanto, comparte gran parte de su funcionalidad. Se arranca a partir de la Interfaz de Línea de Comando utilizando un parámetro de línea de comando que lo obliga a operar como un demonio. En su calidad de demonio, cuenta con diversas funciones. Es responsable de la ejecución de backups periódicos y regulares del driver de registro. También detecta el tráfico UDP en un puerto especificado. Esto facilita la mayor parte de las necesidades de registro y de administración de una interfaz con base en la web. También puede comunicarse con Solsnmpd (un módulo que se ocupa de la gestión de la red) y recupera información según sea necesaria durante la solicitud de registro.

ES 2 334 634 T3

IPFW/ipfwadm/Reglas del Filtro de Paquete

El módulo de filtro de paquete 305, 306 permite a las reglas de filtro de paquete comprobar el estado de registro de las banderas de entrada de registro para las direcciones de fuente y/o de destino de los paquetes, incluyendo:

- pruebas para comprobar si la dirección es una entrada válida o no (o sea, si se encuentra dentro de una gama válida y si ha sido asignada a una dirección MAC);

- pruebas para comprobar si la dirección es una entrada DHCP o no

y

- pruebas para comprobar si la dirección está registrada o no.

Ipfwadm, la utilidad Linux estándar para definir las reglas de filtro de paquete en el núcleo durante el tiempo de operación ha sido modificada para establecer e interpretar nuevas pruebas como las arriba especificadas.

Las reglas de filtro de paquete se definen para proporcionar la siguiente funcionalidad:

- Las solicitudes POP de los clientes no registrados se redirigen al servidor POP adaptado de SolutionIP;

- Las solicitudes http de los clientes no registrados se redirigen al servidor web de redirección 314 que está configurado para redirigir solicitudes al servidor web de registro 310.

- Todas las solicitudes DNS de los clientes se redirigen al servidor DNS local 312.

- Todas las otras solicitudes de clientes no registrados se bloquean.

- Todas las solicitudes SMTP de los clientes registrados se redirigen al servidor SMTP local, no ilustrado).

- Cuando se utilicen para clientes direcciones que no pueden enrutarse, los filtros pueden configurarse para ejecutar enmascaramiento o Traducción de Puerto de Dirección de Red (Network Address Port Translation o NAPT).

- Otros filtros pueden configurarse para aportar seguridad al servidor SolutionIP o para bloquear el acceso de los clientes a protocolos arbitrarios específicos.

Drivers de paquete

Los drivers de paquete 303 cuentan con mayor funcionalidad que los gestores de protocolo estándar de Linux en el punto en que los gestores de paquetes genéricos hacen interfaz con los drivers Ethernet específicos del hardware. Esta funcionalidad adicional puede seleccionarse sobre una base pre-interfaz.

En una interfaz habilitada, se examinan todos los paquetes recibidos, y se busca su MAC en el driver de registro. Si el paquete es un paquete IP o ARP, el MAC se busca en el driver de registro; si se trata de la primera vez que se encuentra este MAC, entonces se asigna la dirección IP, y si la dirección IP de origen del paquete es una dirección IP válida no asignada, esa dirección IP se asigna a la dirección MAC. Una vez determinada la dirección IP asignada, se aplican pruebas de sanidad para asegurar que la dirección IP original asociada con la MAC no ha cambiado de forma inaceptable: si ha cambiado de forma inaceptable, la entrada se elimina, forzando así al cliente a volverse a registrar, si ya se encontraba registrado. Si la dirección IP asignada es diferente de la dirección IP original en el paquete del cliente, dicha dirección IP es reemplazada por la dirección IP asignada en el encabezado IP o ARP y se recalcula el checksum del paquete según los métodos descritos en RFC-1624. Si el paquete contiene un paquete TCP o UDP, entonces se vuelve a recalcular el checksum según se describe arriba para justificar el cambio de dirección IP en el pseudo-encabezado asociado con los paquetes descritos en la sección 3.3 de RFC1631.

La dirección de destino original de todos los paquetes enviados por una interfaz habilitada se buscan en el driver de registro (como una dirección IP asociada). Si se encuentra una entrada correspondiente, entonces se substituye la dirección IP original, siempre que no sea cero y que no sea igual a la dirección de destino corriente. Entonces los check-sums del paquete se recalculan del modo arriba descrito para los paquetes que se reciben.

Servidor DHCP

Un servidor DHCP modificado 316 ha sido incluido en SolutionIP para aportar direcciones IP a los clientes que soliciten información IP basada en la dirección IP asignada provista por el driver de dispositivo de registro 304 para la dirección MAC de dicho cliente. Adicionalmente, el servidor DHCP 316 ha sido modificado para otorgar extensiones sobre la base del período de inactividad obtenido del driver.

ES 2 334 634 T3

Servidor POP

Se incorpora un servidor POP modificado 313 para:

- 5 - Aceptar cualquier combinación de nombre de usuario y contraseña,
- Ignorar todos los comandos de modificación de casilla de correos, y
- Presentar una casilla de correos especial con un mensaje nuevo, único, y de sitio específico como el único correo disponible. La intención de este mensaje es hacer que el usuario use su navegador de web para acceder a la web con el fin de registrarse para el servicio.

Normalmente, las solicitudes POP (una solicitud de leer o bajar correo del servidor de correo electrónico del cliente) de los clientes sólo serían dirigidas a este servidor si el cliente intenta acceder a su correo electrónico sin haberse registrado.

Servidor SMTP

20 Se ha configurado un Agente de Transferencia de Correo (Mail Transfer Agent o MTA) para:

- Actuar como portal de correo de los clientes. Muchos sitios configuran sus servidores de correo para evitar que extraños envíen correo a otro sitio a través de ellos. Es una precaución de seguridad para que los que envían correo basura no usen el sitio como posta de retransmisión. Redirigimos el tráfico SMTP de todos los clientes a nuestro

25 servidor local para que los clientes puedan enviar correo según necesiten.

- El servidor SMTP (no ilustrado en la Fig. 3) está configurado para bloquear los intentos de retransmisión a través del servidor SolutionIP.

30 *Servidor WEB de registro (solhttpd)*

Las reglas de firewall redirigen todo el tráfico no registrado del puerto 80 (http) a un puerto especial en el servidor SolutionIP. El demonio solhttpd es un servidor web 314 configurado para detectar el tráfico http en un puerto especial. Cuando recibe una solicitud http, está configurado para reescribir el URL de modo tal de enviar el cliente al Servidor WEB de Registro 310. Esto significa que todo cliente no registrado que arranque su navegador de web estándar es redirigido al Servidor WEB de Registro en lugar de a su destino previsto.

40 *Servidor WEB de registro*

El Servidor WEB de Registro (310) es un servidor web que aporta contenido local al servidor SolutionIP, incluyendo las páginas de WEB de Registro, las páginas WEB Administrativas, y las páginas WEB de Configuración.

45 *Páginas WEB de registro/administración/configuración*

Las páginas WEB de Registro sirven como portal del cliente para los servicios de SolutionIP. Esto incluye el registro para el acceso a Internet. El cliente puede optar entre dos métodos de autenticación diferentes: basado en puerto o basado en un código de acceso. En el modelo de autenticación por puerto, el cuarto del cliente y la información de tarifa se determinan sobre la base de su dirección IP asignada (facilitada por Solsnmpd). En la autenticación por código de acceso, los clientes pueden introducir códigos de acceso que los relacionan con un número de cuarto y una tarifa en particular.

55 Además del aspecto de registro, también hay una serie de páginas administrativas. Estas páginas permiten a los administradores del servidor y el personal ejecutar diversas tareas, que incluyen:

- la verificación del estado corriente del driver de registro;
- 60 - cambios de registro manuales;
- modificación de las pautas del driver de registro,
- modificación de las pautas del Demonio Soln;
- 65 - exhibición de las variables de salud del sistema;
- exhibición de la información de facturación; y,

ES 2 334 634 T3

- exhibición y generación de códigos de acceso.

Las páginas WEB de registro usan el Demonio Soln (315) para comunicarse con el Driver de Registro y Solsnmpd a fin de facilitar el proceso de administración y registro.

También se incorporan diversas herramientas de primera generación con base en web. Primariamente están diseñadas como middleware para aislar a los usuarios de la base de datos.

Base de datos de facturación (ipbilling)

Un DBMS (sistema de gestión de base de datos) estándar de código abierto implementa un plan designado para apoyar el proceso de facturación. El plan permite la configuración flexible del sistema e incluye lo siguiente:

- información de configuración de sitio;
- información sobre tarifa;
- infraestructura de red y mapeos asociados, incluyendo mapeo de cuarto a puerto, y otra información relacionada con la conmutación;
- facturación e información de uso, y
- Códigos de acceso.

Servidor DNS

Un servidor DNS estándar de código abierto 312 se provee a todos los clientes para manejar sus solicitudes DNS. Este servidor no tiene nada de especial, pero lo que sí es especial es que todas las solicitudes DNS de los clientes se dirigen a este servidor. Esto asegura que no caducará el tiempo permitido para las solicitudes DNS de ningún cliente (estático o DHCP) porque el servidor DNS se encuentra inaccesible (detrás de un firewall) o demasiado lejos (demasiadas redes que atravesar) para responder a tiempo.

Solsnmpd

Este servidor emplea un protocolo patentado para aceptar solicitudes y responder con los resultados. Los formatos de los paquetes de solicitudes y respuestas se definen según resulte necesario para cada consulta. El fin de este demonio es manejar las comunicaciones con conmutadores y otros dispositivos de red de la red del cliente a través de un Simple Network Management Protocol (SNMP) para lograr los diversos objetivos. La funcionalidad inicial de este demonio es aceptar solicitudes para determinar el “puerto físico” al que el cliente está conectado. Se envía al demonio una solicitud con la dirección MAC del cliente. El demonio entonces usa la jerarquía de conmutación definida en la base de datos de facturación para pasar por los conmutadores utilizando el Bridge MIB (RFC-1493) para determinar el puerto a través del cual está conectado el cliente. Una vez determinados el conmutador y el puerto, entonces puede determinarse el “puerto físico”, nuevamente utilizando la base de datos de facturación. Esta información se remite al proceso de solicitud.

Solsyncd

Este servidor (no ilustrado en la Fig. 3) extrae información de configuración de la base de datos de facturación y la coloca en archivos de configuración plana (texto) para permitir el acceso a la información de configuración sin tener acceso a la base de datos. Si los archivos de configuración resultantes han cambiado, se envía una señal HUP a los procesos específicos para que vuelvan a leer sus archivos de configuración y actualicen los datos.

Monitor de proceso (keepalive)

Este script se opera a cada minuto y está configurado para verificar el estado de diversos demonios en el servidor, quejarse si no están operando, y si siguen sin funcionar pasado un tiempo configurable, se los vuelve a arrancar.

Herramienta de configuración de servidor (reconfig-all.pl)

Esta herramienta toma un archivo de configuración de un sitio y lo aplica a una jerarquía de archivos de configuración de plantillas para configurar al servidor para un sitio en particular.

ES 2 334 634 T3

A partir de esta descripción es obvio que no todos los componentes han sido ilustrados en la Fig. 3 pero una persona experta en este campo entendería la forma en que la funcionalidad descrita para los componentes no ilustrados se integraría al sistema. De la descripción que antecede puede apreciarse que el término servidor se utiliza tanto para referirse a un ordenador que opera los programas para lograr la funcionalidad deseada, como a los módulos de software que desarrollan la funcionalidad deseada. Se entiende que existe una estructura continua y que diversos aspectos del invento pueden ser ejecutados por hardware, firmware o software, o una combinación de los mismos, según se desee.

10 *Procesamiento del servidor*

Las siguientes secciones describen diversos procesamientos ejecutados por el servidor en términos generales.

15 *Procesamiento de solicitud DHCP*

A continuación se describe el procesamiento ejecutado por SolutionIP™ para las solicitudes DHCP con referencia a la Fig. 4.

20 Cuando un huésped con un ordenador configurado para DHCP enciende el ordenador, el ordenador 401 inicia una solicitud DHCP a los demás ordenadores en la LAN. El servidor DHCP modificado 405 recibe y procesa la solicitud. El servidor DHCP 405 captura la dirección MAC del ordenador huésped 401 e inicia una solicitud de una dirección IP al Driver de Dispositivo de Registro 404. El Driver de Dispositivo de Registro suministra una dirección IP apropiada para el huésped. La dirección IP se remite al servidor DHCP, que luego pasa la dirección y todo parámetro adicional (portal a usar, servidor DNS a usar, etc.) nuevamente al ordenador del huésped.

Procesamiento de solicitud ARP

30 El procesamiento ejecutado para una solicitud ARP se describe con referencia a la Fig. 5, más adelante.

Para identificar exactamente qué máquina en un LAN cuenta con una dirección IP en particular, un ordenador de un huésped 501 inicia una solicitud ARP, solicitando la dirección MAC de la máquina que tiene la dirección IP especificada. El Driver de Dispositivo de Registro 504 detecta la solicitud ARP y responde con su propia dirección MAC a través del servidor ARP 505, independientemente de la dirección IP en realidad solicitada. Durante el procesamiento de la solicitud ARP, el servidor ARP 505 notifica al Driver de Dispositivo de Registro 504 de la dirección MAC y la dirección IP del ordenador del huésped. El Driver de Dispositivo de Registro 504 puede entonces determinar si existe un par de dirección MAC y dirección IP, y también si el ordenador del huésped precisará NAT. El Driver de Dispositivo de Registro 504 entonces actualiza sus estructuras de datos con la información nueva, si es necesario.

Procesamiento de solicitud de HTTP no registradas

45 El procesamiento de solicitudes HTTP implica la redirección de huéspedes no registrados al servidor web de registro, permitiendo a la vez que las solicitudes de los huéspedes registrados sean dirigidas normalmente. El procesamiento de solicitudes HTTP no registradas se describe en la forma indicada en la Fig. 6.

El procesamiento de una solicitud Hypertext Transfer Protocol (HTTP) comienza cuando los drivers de paquete de SolutionIP™ reciben la solicitud 603. Estos drivers interrogan al Driver de Dispositivo de Registro 604 para identificar si se requiere la traducción NAT de los encabezados del paquete. De ser así, los drivers de paquete 603 ejecutan esta traducción. El componente IPFW 606 toma control de la solicitud e interroga al Driver de Dispositivo de Registro 604 para determinar si el huésped está registrado. Si el huésped está registrado, permite el enrutamiento normal de la solicitud. Si el huésped no está registrado, la solicitud pasa al Servidor Web de Redirección 608, que la traduce a una solicitud del área de registro del Servidor Web de Registro. La solicitud traducida luego se envía al Servidor Web de Registro y se presenta al huésped la pantalla de registro del hotel. Si el huésped opta por registrarse para el servicio de acceso a la red, esta información se envía al Programa/Demonio de Control, que actualiza al Driver de Dispositivo de Registro apropiadamente. Las solicitudes subsiguientes del ordenador del huésped, tras la actualización del Driver de Dispositivo de Registro se procesarán como provenientes de un huésped registrado.

60 *Procesamiento de solicitud HTTP registrada*

La siguiente descripción se hace con referencia a la Fig. 7. El procesamiento general ejecutado por el servidor SolutionIP™ para el tráfico con base IP que no sea tráfico de web o de correo electrónico es igual al indicado en las Figs. 6 y 7 con la excepción de que no está sujeto a redirección. El tráfico con base IP se inicia a partir del ordenador del huésped 701 y se envía al servidor SolutionIP™. Los drivers de paquete 703 del servidor SolutionIP™ a continuación determinan si el tráfico requiere NAT y ejecuta la traducción de los encabezados, de ser necesaria. El filtro de paquete IPFW 705,706 luego determina si el huésped se ha registrado para el servicio de acceso a la red. Si el huésped se ha

ES 2 334 634 T3

registrado, se permite que proceda el tráfico de datos, y se lo dirige por la ruta normal. Si el huésped no se ha registrado, los datos se bloquean mediante el descarte de los paquetes de red que se reciban.

5 *Aspecto de facturación del invento*

La siguiente sección describe los componentes y funcionalidad del aspecto de facturación del servidor y el invento de método.

10 El aspecto de facturación del invento cuenta con dos métodos de registro: códigos de acceso o identificación de puerto. Los códigos de acceso se generan a diario para cada cuarto. Los clientes deben introducir el código de acceso de su cuarto como parte del proceso de registro. La identificación de puerto automáticamente determina el número de cuarto del cliente interrogando a la infraestructura de conmutación de la red para determinar el puerto de conmutación específico al cual el cliente está conectado. Los puertos de conmutación se relacionan con cuartos específicos. Los
15 códigos de acceso pueden utilizarse en el caso de que el cliente no se esté conectando desde un cuarto del hotel, tal como ocurre cuando trabaja en un área pública del hotel, o si el puerto de conmutación no puede determinarse.

Los códigos de autorización se utilizan como un mecanismo de anulación dirigido a aplicar reglas de procesamiento especiales (descuentos, uso gratuito, etc.) con ciertos clientes. El sistema almacena y exhibe el código de autorización
20 como parte del informe de facturación. La interpretación y aplicación de los códigos de autorización es responsabilidad del personal del personal del hotel.

El Sistema de Gestión de Propiedad (Property Management System o PMS) del hotel se encarga de la facturación efectiva de los clientes. El sistema de facturación suministra informes con base web que el personal del hotel puede
25 imprimir e introducir manualmente al PMS.

Requisitos

30 SolutionIP precisa dos sistemas operativos de clase Pentium de 200 MHz o más. Uno actúa como el servidor SolutionIP, mientras que el otro es anfitrión del sitio web y la base de datos. Estas máquinas requieren el siguiente hardware:

- 35 - 64MB RAM;
- Disco duro 4.5GB;
- Tarjeta de Interfaz de Red (NIC) (Linux compatible)

40 Nota: El servidor SolutionIP requiere dos NIC y el servidor de web requiere una;

- Monitor y teclado son optativos; y
- Dos puertos en serie.

45

El componente del cliente tiene los siguientes requisitos:

- 50 - Tarjeta de Interfaz de Red y conector;
- Navegador de Web;
- Pila TCP/IP; y
- 55 - Una conexión de impresora para los informes de facturación.

SolutionIP apoya una diversidad de sistemas operativos de clientes, incluso Win95, Win98, WinNT, Macintosh OS
60 8 y Linux.

Los conmutadores para la identificación de puerto deben apoyar:

- Bridge MIP (RFC 1493);
- 65 - Acceso de lectura SNMP; y
- mapeo 1-1 (cuarto a puerto).

ES 2 334 634 T3

Los requerimientos de software se basan en la funcionalidad de cada máquina:

- Servidor SolutionIP:

Sistema operativo - RedHat Linux 5.1.

- Servidor Web/Base de Datos de SolutionIP:

Sistema operativo - RedHat Linux 5.1;

Servidor Web - Apache;

Base de datos - PostgreSQL 6.4 o superior; y Perl 5.004.

Se entiende que los componentes arriba mencionados son para la corporización preferida. Un experto en este campo reconocería que podría utilizarse otros componentes sin apartarse de este invento.

Áreas de funcionalidad

Existen tres áreas de funcionalidad principales para el sistema de facturación, a saber: identificación de puerto, generación e identificación de código de acceso, y administración de sistema de facturación. Esta sección presenta las generalidades de los requisitos del sistema, y también los requisitos específicos para cada área de funcionalidad.

Generalidades de facturación

La facturación comienza con la identificación del cuarto asociado con cada cliente. Los cuartos se identifican manualmente mediante la asociación de un código de acceso con un cuarto en particular, o bien automáticamente mediante la obtención del puerto de conmutación al cual el cliente está conectado, derivando así el cuarto de hotel asociado con el mismo. El sistema incorpora funciones que permiten generar automáticamente un nuevo código de acceso para cada cuarto, ya sea para el día corriente o el día siguiente. Los códigos se exhiben a través de una página web y pueden imprimirse. Se mantiene una historia configurable de los códigos de acceso para evitar la generación de códigos duplicados dentro del mismo período histórico. No se incluye un mecanismo para evitar que los códigos de acceso sean empleados más de una vez o por más de un cliente. Cada nueva MAC que se registre se factura al cuarto asociado. Los registros son válidos hasta el la próxima hora de salida del cuarto. El código de acceso se usa para determinar qué cuarto facturar, y por lo tanto, es responsabilidad del cliente asegurarse de guardar con seguridad el código. La facturación se basa en el cuarto a partir del cual el cliente se registra, cuando se usa la identificación de puerto.

Una vez identificado el cuarto, se determina una tarifa asociada con dicho cuarto. Una tarifa diaria fija está asociada con cada cuarto (se cobran tarifas diferentes por cuartos diferentes). La interfaz de registro permite a los clientes introducir códigos de autorización especiales. Estos códigos se almacenan en la información de facturación del cliente. Los códigos de autorización utilizados se incluyen en el informe de facturación generado por el personal del hotel, pero no afecta la tarifa generada por el sistema de facturación. La interpretación y aplicación de los códigos de autorización es responsabilidad del personal del hotel.

El personal del hotel provee e imprime un informe de facturación con base web, que muestra quién ha estado en línea desde la última hora de salida. También son posibles consultas adicionales sobre fechas arbitrarias, que muestran quién estaba en línea desde una hora de salida en el día específico hasta la hora de salida del día siguiente. La información incluida en el informe abarca el cuarto del cliente, la hora de registro, el código de acceso, el puerto, el código de autorización, y la tarifa. El acceso a los informes web administrativos está protegido por contraseña.

La base de datos puede guardar un mes de datos. Puede suministrarse procedimientos de backup, restauración, y recuperación de catástrofes.

Identificación de puerto

Un método para asociar un cliente (Dirección MAC) con un Cuarto para fines de facturación es la Identificación de Puerto. Si, al registro, la conexión de puerto físico puede identificarse como asociada con un cuarto, entonces el registro del cliente se factura a dicho cuarto. Para determinar el puerto físico al que el cliente está conectado se utiliza el protocolo Simple Network Management Protocol (SNMP) para descubrir el puerto de conmutación con el que se están comunicando, a continuación se utilizan tablas de datos estáticas para determinar el número de cuarto.

ES 2 334 634 T3

El número de conmutador/puerto que una MAC utiliza se determina usando SNMP para investigar los conmutadores de la instalación.

El mapeo del número de conmutador/puerto en el que la MAC aparece identifica los puertos físicos. Este mapeo se mantiene en la base de datos.

Los puertos físicos están asociados con números de cuarto y tarifas de facturación. Estos mapeos se mantienen en la base de datos.

La determinación del mapeo de la MAC al puerto físico se hace según sea requerido.

Si la identificación de puerto se encuentra disponible, ésta tiene prioridad sobre la identificación de código de acceso, y no se solicita al usuario un código de acceso durante el proceso de registro. La excepción es que ciertos puertos físicos están programados para necesitar un código de acceso válido para el éxito del registro.

Identificación de código de acceso

Una alternativa para la Identificación de Puerto es la Identificación de Código de Acceso. Cada código de acceso está asociado con un cuarto en particular, y es válido durante un período de tiempo limitado (generalmente un día desde la hora de salida a la hora de salida siguiente). Si fracasa la identificación de puerto, o si no se encuentra disponible en un puerto dado, entonces se solicitará al cliente la introducción de un código de acceso que el sistema entonces valida. Esto asegura la generación de un registro de facturación para dicho cuarto.

Funciones administrativas

Esta sección de la especificación describe las funciones administrativas relacionadas con la facturación. Las funciones administrativas sirven como interfaz ente el sistema de facturación y el personal del hotel. Los dos componentes principales son los informes de facturación y de código de acceso.

Informe de facturación

El informe de facturación provee al personal del hotel información relacionada con los números de cuarto, códigos de acceso, códigos de autorización, puertos físicos, hora de registro y tarifas. El informe tiene base web y puede verse con un navegador de web estándar. El personal del hotel puede generar y ver el informe según sea necesario.

Generación de informe de código de acceso

El informe de código de acceso suministra al personal del hotel información relacionada con los números de cuarto y códigos de acceso. El informe tiene base web y puede verse con un navegador de web estándar. El personal del hotel puede generar y ver el informe según sea necesario. Tras evaluar un informe, el sistema automáticamente genera los códigos de acceso para el día de la fecha o el día siguiente si tales no existen en la base de datos.

Componentes funcionales

La siguiente sección describe los componentes funcionales del sistema de facturación y se refiere a la Fig. 8. Debe entenderse que la corporización preferida aquí descrita usa dos ordenadores que actúan como servidores, pero un experto en el campo comprendería que puede usarse un servidor o más de dos servidores sin apartarse del invento.

Generalidades

El sistema de facturación consta de dos componentes que operan tanto en el Servidor SolutionIP 802 como en el Servidor Web 801. El Servidor Web es anfitrión de la base de datos de facturación y configuración 803; la Interfaz Administrativa 804, que formará parte del sitio web de Administración; y la Interfaz de Registro 805, que será las páginas Web de Registro con modificaciones para incluir los métodos del nuevo sistema de facturación. En el Servidor SolutionIP, el Driver de Registro 806 y el Demonio de Línea de Comando 807 dan cabida a los métodos del nuevo sistema de facturación. El Demonio de Sincronización 808 y el Demonio SNMP 809 se implementan para apoyar al sistema de facturación.

ES 2 334 634 T3

Base de datos

El Sistema de Facturación en la corporización preferida se implementa mediante el uso de una base de datos PostgreSQL 6.4. La base de datos almacena información de configuración, códigos de acceso, y registros de facturación. En todo momento se mantiene un mes de datos. Los datos de más de un mes se purgan con regularidad de la base de datos. Pueden proveerse procedimientos de backup y recuperación de la base de datos según resulte necesario.

Los datos de configuración manejados por la base de datos incluyen información sobre configuración de conmutadores, tipos, mapeo de puertos de conmutación a cuartos, etc.). La hora de salida del hotel, la cantidad de datos históricos a mantener, y otros parámetros relacionados también se almacenan en la base de datos.

La base de datos almacena el código de acceso y sus fechas de vigencia para cada cuarto. Como pauta implícita, cada código sólo tiene validez por un día. Se mantiene la historia de los códigos de acceso para cada cuarto. Los códigos nuevos se constatan con esta historia para evitar duplicación.

Los registros de facturación identifican el cuarto a facturar por cada conexión. Este registro incluye los siguientes campos:

- Número de cuarto;
- Puerto desde el cual se registra;
- Código de acceso utilizado;
- Código de autorización;
- Fecha y hora de registro; y
- Tipo de tarifa a cobrar.

En ciertos casos, algunos campos son NULOS. Por ejemplo, el código de acceso normalmente es NULO cuando se utiliza la identificación de puerto.

Demonio de línea de comando

El demonio tiene capacidad para manejar múltiples solicitudes simultáneas de otros sistemas, preservar cambios en los parámetros, y rastrear el estado de los backups del driver de registro. El demonio también permite el uso de SNMP 809 y el demonio de Sincronización 808.

Funciones de interfaz del driver de dispositivo de registro

El Demonio de Línea de Comando 807 es la interfaz primaria en el driver de dispositivo de registro 806. La funcionalidad del driver de dispositivo de registro da cabida al sistema de facturación.

El demonio de línea de comando apoya las siguientes operaciones:

- Determinar el cuarto original e identificación de puerto para un usuario especificado;
- Determinar el cuarto corriente e identificación de puerto para un usuario especificado
- Bloquear un usuario especificado, de modo tal que no pueda registrarse;
- Desbloquear un usuario especificado, de modo tal que pueda registrarse;
- marcar una entrada especificada como permanente;
- marcar una entrada especificada como una entrada que ya no es permanente; y
- Determinar un período de gracia (período de tiempo previo a la hora de salida, durante el cual los registros no caducan sino hasta la hora de salida del día siguiente).

ES 2 334 634 T3

Interfaz al demonio SNMP

El sistema de facturación se comunica con el Demonio SNMP 809 a través del Demonio de Línea de Comando 807. El Demonio de Línea de Comando 807 encauza todo el tráfico entre los otros componentes del sistema de facturación y el Demonio SNMP. El Demonio de Línea de Comando también el Driver de Dispositivo de Registro 806, cuando resulte aplicable, con los resultados recibidos del Demonio SNMP.

El demonio de línea de comando:

- responde a las solicitudes de resolución de identificación de puertos tanto para el servidor de registro como los drivers núcleo;

- transmite las solicitudes de resolución de identificación de puerto al Demonio SNMP;

- recibe las identificaciones de puerto del Demonio SNMP;

- pasa la información de puerto al solicitante; e

- informa al núcleo de información de identificación de puerto si el núcleo no fue quien solicitó la transacción.

Demonio SNMP

El objetivo del Demonio SNMP 809 es resolver las direcciones en relación con su número de puerto físico, o enviar un mensaje de error si esto no es posible. Este Demonio usa SNMP para interrogar a los conmutadores de red y hallar el puerto de conmutación al que está conectado el cliente, para luego usar las tablas de datos estáticos para asociar dicho puerto de conmutación a un número de puerto físico. Para este componente:

- los datos de configuración se obtienen de archivos de datos planos almacenados en el Servidor SolutionIP;

- los archivos de datos de configuración se derivan de tablas en la base de datos y son actualizados por el Demonio de Sincronización;

- cuando se modifican los archivos de Configuración, el Demonio de Sincronización informa al Demonio SNMP;

- las solicitudes y respuestas se manejan a través de Métodos de Comunicación Interproceso estándar con otros componentes del sistema.

Driver de dispositivo de registro

El Driver de Dispositivo de Registro apoya las necesidades de facturación y producción. El driver mantiene información sobre las direcciones MAC de los clientes, las direcciones IP originales, y las direcciones IP asignadas. Los parámetros temporales se incluyen para permitir una duración fija a los períodos de registro, al igual que períodos de terminación por inactividad para los clientes no registrados. Se incorpora un modo de caducidad de Hora del Día (Time of Day). El método de caducidad se determina a la hora de registro del cliente. En el modo de caducidad de Hora del Día, los registros caducan a la próxima hora de salida (o cualquier hora arbitraria de cada día). Al presente, los nuevos registros caducan al finalizar un intervalo de tiempo fijo, que típicamente es de 24 horas. El modo de caducidad de Hora del Día es más congruente con las rutinas normales de facturación del hotel. El modo de cálculo de caducidad existente se preserva como una opción.

Además del nuevo modo de caducidad, también se dispone de la capacidad de anular parámetros para clientes individuales. Los parámetros de driver existentes sirven como parámetros implícitos y afectan a todos los clientes. Un mecanismo de anulación permite a los administradores cambiar parámetros específicos entre un cliente y otro. Un ejemplo podría ser la extensión del tiempo de caducidad para un cierto cliente sin afectar los tiempos de caducidad de otros clientes.

Además de operar en base a información de dirección MAC y dirección IP, el driver incluye y opera en base a datos de cuarto y de puerto. La tarea de asociar los cuartos y puertos con los clientes en el driver es ejecutada por componentes externos (el sistema de facturación y el demonio SNMP). Las operaciones apoyadas por el driver, tales como el registro o la eliminación de entradas, permite ejecutar estas operaciones en todos los clientes asociados con un cuarto o puerto en particular.

Las necesidades de producción incluyen la capacidad de reservar direcciones específicas o efectuar entradas permanentes. Esto permite el acceso para el apoyo de mantenimiento de los dispositivos de red, tales como conmutadores, que residen en el lado del cliente de los servidores. También hay implementado un mecanismo para bloquear clientes en particular. Este mecanismo identifica a los clientes por cuarto, puerto, o MAC. Los clientes bloqueados pueden

ES 2 334 634 T3

tener acceso al servidor de registro y otros servicios disponibles a los huéspedes no registrados, pero no se les permite registrarse para el acceso total al sistema.

5 *Demonio de sincronización*

El fin del Demonio de Sincronización 808 es centralizar el acceso a la base de datos por los componentes del Servidor SolutionIP a través de una interfaz. El demonio emplea información almacenada en la base de datos para recrear archivos de configuración planos en el servidor SolutionIP. Esto permite centralizar en la base de datos la información de configuración de diversos componentes pero no excluye su mantenimiento en el servidor si una base de datos no se encuentra disponible o no se requiere en una instalación en particular.

15 Cuando el Demonio de Sincronización adapta los archivos, se informa a los procesos que los usan que hay una actualización disponible (los métodos para comunicarlo incluyen señales, semáforos IPC, o hacer que el proceso monitorice la última vez que se modificaron sus archivos de configuración). También es posible tener esta información de actualización de proceso en la base de datos con base en los archivos de estado del servidor SolutionIP.

20 *Proceso de registro del servidor WEB*

El proceso de registro aprovecha los métodos del sistema de facturación. Cuando un cliente intenta registrarse, el sistema primero intenta determinar si se está conectando desde un cuarto que permite la facturación a través del método de identificación de puerto. Si se identifica un cuarto facturable utilizando este método, entonces se presenta al usuario una Pantalla de Autorización - Confirmación. Si no se puede identificar un cuarto facturable mediante el Método de Identificación de Puerto, entonces se utiliza el método de Identificación de Código de Acceso. En consecuencia, se presenta al usuario una pantalla de introducción de código de acceso, y cuando el usuario introduce un código de acceso válido, se identifica el cuarto facturable, y se presenta al usuario la Pantalla de Autorización - Confirmación. La Pantalla de Autorización - Confirmación presenta al usuario el número de cuarto y tarifa, y cualquier otra información de importancia. A continuación se brinda al usuario la oportunidad de introducir un Código de autorización optativo. 30 Una vez que el usuario confirma su voluntad de pagar la tarifa especificada, éste pasa al Conserje Virtual, que le permite acceso a una diversidad de servicios ofrecidos a través del hotel, al igual que a www y correo electrónico.

35 *Ejemplos de usuarios en particular*

A fin de comprender mejor la operación del invento, citamos una serie de ejemplos específicos que explican en detalle los pasos desarrollados por el invento a fin de lograr los resultados deseados en los escenarios descritos en particular.

40 *Arranque del cliente*

Arranque del sistema

45 Escenario: El cliente arranca el ordenador.

IP fija

50 Escenario: El cliente está configurado con una configuración IP fija.

1. El cliente enciende el sistema.
2. El sistema genera una solicitud ARP para ver si su dirección IP ya está en uso.
3. El servidor SolutionIP recibe la solicitud ARP y la pasa al Driver de Paquete.
4. El Driver de Paquete solicita al Driver de Registro que busque la dirección IP Asignada para la MAC del paquete.
- 60 5. El Driver de Registro, sin poder hallar una entrada para esa MAC, asigna una nueva dirección IP del grupo de direcciones IP disponibles.
6. El Driver de Paquete ejecuta la NAT del paquete ARP (según sea necesario).
- 65 7. El paquete pasa al gestor ARP.
8. El Gestor ARP ve que la dirección IP Original es Igual a la dirección IP de Destino y abandona la solicitud ARP.

ES 2 334 634 T3

9. Eventualmente caduca el tiempo del cliente y supone que es el único propietario de dicha dirección IP en su red.

DHCP

- 5 Escenario: El cliente está configurado para DHCP.
1. El ordenador del cliente efectúa una solicitud de DESCUBRIR DHCP.
 - 10 2. El driver de paquete intercepta esta solicitud, e interroga al driver de registro en relación con la dirección IP asignada para esta MAC.
 3. El driver de registro intenta buscar la dirección IP asignada para la MAC, y si no la encuentra, crea una nueva asignación en base a su grupo de direcciones libres.
 - 15 4. El driver de paquete realiza la NAT de la solicitud según sea necesario, y la envía al servidor DHCP.
 5. El servidor DHCP busca la dirección IP asignada para la dirección MAC y envía una respuesta de OFERTA DHCP para dicha dirección.
 - 20 6. El gestor ARP busca la dirección MAC para la dirección de destino del Driver de Registro e inserta dicha dirección MAC en el paquete.
 7. El driver de paquete intercepta la respuesta y ejecuta la NAT, de ser necesario.
 - 25 8. El cliente DHCP del usuario responde con una SOLICITUD DHCP para la dirección IP asignada.
 9. El driver de paquete intercepta esta solicitud, ejecuta la NAT, de ser necesario, y envía la solicitud al servidor DHCP.
 - 30 10. El servidor DHCP busca la dirección IP asignada para la dirección MAC y envía una respuesta DHCP ACK para dicha dirección.
 11. El gestor ARP busca la dirección MAC para la dirección de destino del Driver de Registro e inserta dicha dirección MAC en el paquete.
 - 35 12. El driver de paquete intercepta la respuesta y ejecuta la NAT, de ser necesario.
 13. El cliente obtiene la dirección IP.
 - 40

Arranque de navegador

- 45 Escenario: El cliente arranca su navegador de WEB e intenta carga una página WEB.
1. El cliente arranca el navegador de WEB.
 2. El navegador precisa buscar la dirección IP del servidor WEB y por lo tanto genera una solicitud DNS.
 - 50 3. El servidor SolutionIP recibe la solicitud DNS y la pasa al Driver de Paquete.
 4. El Driver de Paquete solicita al Driver de registro buscar la dirección IP Asignada para la MAC del paquete.
 5. El Driver de Registro remite la IP Asignada al Driver de Paquete.
 - 55 6. El Driver de Paquete ejecuta la NAT, de ser necesario.
 7. El paquete pasa a un Filtro de Paquete que redirige la solicitud al servidor DNS de SolutionIP.
 - 60 8. El servidor DNS busca al servidor HTTP y crea una respuesta para el cliente.
 9. El paquete de respuesta pasa al gestor ARP, que solicita al Driver de registro buscar la dirección MAC para el cliente, y luego el gestor ARP la añade al paquete que sale.
 - 65 10. El paquete luego pasa al Driver de Paquete, que busca la dirección IP Original para la dirección IP Asignada y ejecuta la NAT, de ser necesario.
 11. La respuesta se envía al cliente.

ES 2 334 634 T3

12. El cliente genera una solicitud ARP para su servidor de portal (suponiendo que la dirección IP remitida al servidor HTTP no era local. Si es local, el cliente en cambio solicita la MAC del servidor HTTP).

13. El servidor SolutionIP recibe la solicitud ARP y la pasa al Driver de Paquete.

14. El Driver de Paquete solicita al Driver de Registro buscar la dirección IP Asignada para la MAC del paquete.

15. El Driver de registro remite la IP Asignada al Driver de Paquete.

16. El Driver de Paquete ejecuta la NAT, según necesario.

17. La solicitud ARP pasa al gestor ARP.

18. El gestor ARP genera una respuesta que dice que la MAC del servidor SolutionIP es la MAC para la dirección IP solicitada.

19. La respuesta ARP pasa de nuevo al Driver de Paquete.

20. El driver de Paquete busca la IP Original del destino del paquete mediante la IP Asignada y ejecuta la NAT, de ser necesario.

21. La respuesta ARP se remite nuevamente al cliente.

22. El cliente entonces envía una solicitud HTTP a la dirección IP provista por el DNS a la dirección MAC suministrada por la respuesta ARP.

23. La solicitud HTTP llega al servidor SolutionIP y pasa al Driver de Paquete.

24. El Driver de Paquete hace que el Driver de Registro busque la IP Asignada para la MAC y ejecuta la NAT, de ser necesario.

25. El Paquete pasa el Filtro de Paquete, que determina que el cliente no está registrado.

26. El Paquete se redirige al Servidor Web de Redirección (solhttpd).

27. El Paquete se redirige al Servidor Web de Registro.

28. El Servidor Web de Registro genera la respuesta a la solicitud HTTP.

29. El Paquete pasa de nuevo al Gestor ARP, que busca la MAC asociada con la IP Asignada del cliente y actualiza el paquete.

30. El Paquete pasa de nuevo al Driver de Paquete, que busca la IP Original asociada con la IP Asignada y ejecuta la NAT, de ser necesario.

31. La respuesta se remite al cliente.

La conversación prosigue después de este punto, pero la forma es similar a la descrita.

Registro de cliente

Escenario: después de ser redirigido a la Página Web de Registro, el cliente se registra para el servicio.

Con base en puerto

Escenario: el cliente se enchufa a un puerto de conmutación en el cual se ha configurado la autenticación en base a puerto

1. El cliente tiene acceso a la página web de registro, que provoca la ejecución del script CGI

2. El CGI inspecciona la base de datos y determina que se ha configurado la autenticación basada en puerto.

3. El CGI solicita la dirección MAC y la información de puerto físico para la dirección IP asignada del Demonio Soln.

4. El Demonio Soln solicita al driver de registro la dirección MAC asociada con la dirección IP asignada dada.

ES 2 334 634 T3

5. El driver de registro remite la dirección MAC asociada con la dirección IP asignada.

6. El Demonio Soln solicita a Solsnmpd el número de puerto físico asociado con la dirección MAC dada.

5 7. Solsnmpd remite la información de puerto físico tras resolver el puerto sobre la base de la dirección MAC dada.

8. El Demonio Soln remite la dirección MAC y la información de puerto físico sobre la base de la dirección IP asignada dada.

10 9. El CGI solicita información de número de cuarto y tarifa de la base de datos para el número de puerto físico.

10. La base de datos remite la información de número de cuarto y tarifa para el puerto físico dado.

15 11. El CGI dinámicamente genera HTML para el cliente que refleja la información de cuarto y tarifa remitida por la base de datos.

12. El cliente decide aceptar las tarifas y continúa con el registro.

20 13. El CGI solicita el registro de la dirección IP asignada del Demonio Soln.

14. El Demonio Soln solicita al driver registrar la entrada con la dirección IP asignada dada.

15. El CGI inserta la información del cliente en la base de datos y presenta al cliente la página de portal obligada.

25 *Código de acceso*

Escenario: el cliente está conectado a un puerto de conmutación para el cual no se ha configurado autenticación basada en puerto, pero con códigos de acceso habilitados en esta instalación.

30 1. El cliente tiene acceso a la página web de registro, lo cual activa la ejecución de un script CGI.

35 2. El CGI inspecciona la base de datos y determina que no se ha configurado la autenticación basada en puerto y que los códigos de acceso están habilitados.

3. El CGI dinámicamente genera HTML para el cliente, que refleja su necesidad de introducir información de código de acceso.

40 4. El cliente introduce en el formulario la información de código de acceso.

5. El CGI solicita información de número de cuarto y tarifa de la base de datos para el código de acceso dado.

6. La base de datos remite la información de número de cuarto y tarifa para el código de acceso dado.

45 7. El CGI dinámicamente genera HTML para el cliente, que refleja la información de cuarto y tarifa enviada por la base de datos.

8. El cliente decide aceptar las tarifas y continúa con el registro.

50 9. El CGI solicita el registro de la dirección IP asignada del Demonio Soln.

10. El Demonio Soln solicita al driver registrar la entrada con la dirección IP asignada dada.

55 11. El CGI inserta la información del cliente en la base de datos y presenta al cliente la página de portal obligada.

Automático

60 Escenario: el servidor está configurado para registrar automáticamente a los clientes nuevos. El efecto principal en este caso es que siempre se dirige a los clientes a la página de portal la primera vez que acceden a la WEB.

1. Se redirige al cliente a la página web de registro, que activa la ejecución del script CGI.

65 2. El CGI solicita el registro de la dirección IP asignada del Demonio Soln.

3. El Demonio Soln solicita al driver registrar la entrada con la dirección IP asignada dada.

4. El CGI presenta al cliente la página de portal obligada.

ES 2 334 634 T3

Correo electrónico del cliente

Registrado

5 *Envío*

Escenario: un cliente registrado está intentando enviar un mensaje de correo electrónico utilizando el software de correo electrónico del cliente (Netscape, Outlook, Pegasus, etc.)

- 10 1. El cliente envía el mensaje de correo electrónico utilizando el software y el servidor de correo de salida SMTP preferidos del cliente.
2. El cliente de correo busca la dirección IP del servidor SMTP utilizando DNS.
- 15 3. El cliente de correo busca la dirección MAC del servidor SMTP o de su portal utilizando ARP.
4. El Filtro de Paquete transparentemente redirige todo el tráfico SMTP de los clientes registrados al servidor SMTP local.
- 20 5. El servidor SMTP actúa como proxy y envía el mensaje en nombre del cliente.

No registrado

25 *POP*

Escenario: Un cliente no registrado intenta el envío POP de su correo electrónico a partir de su propio sistema utilizando su software de cliente de correo (Netscape, Outlook, Pegasus, etc.)

- 30 1. El cliente busca la dirección IP del servidor POP utilizando DNS.
2. El cliente de correo busca la dirección MAC del servidor POP o del portal utilizando ARP
3. El Filtro de Paquete transparentemente redirige todo el tráfico POP3 para los clientes no registrados al servidor POP3 local.
- 35 4. El servidor POP3 acepta cualquier combinación de nombre de usuario y contraseña y remite al cliente un nuevo y único mensaje de correo electrónico.
- 40 5. Este mensaje de correo electrónico típicamente informa al cliente que no se ha registrado para el servicio y le presenta instrucciones para hacerlo.

Tráfico del cliente (general)

45 *DHCP*

Escenario: un cliente configurado con DHCP envía y recibe paquetes a través del servidor SolutionIP.

50 *Enviar*

1. El cliente genera un paquete para un anfitrión remoto enrutado a través del Servidor SolutionIP.
- 55 2. El Servidor SolutionIP recibe el paquete y lo pasa al driver de paquete.
3. El driver de paquete examina el paquete y busca la IP Asignada en el Driver de Registro utilizando la dirección MAC.
- 60 4. El driver de paquete determina que la IP Asignada y la dirección de Fuente original son iguales y que no es necesaria la NAT.
5. El paquete pasa a los filtros de paquete. Consultar las secciones de clientes Registrados y No Registrados a continuación.

65

ES 2 334 634 T3

Recibir

1. El paquete pasa de los filtros de paquete al gestor ARP.
- 5 2. El gestor ARP busca la dirección MAC del anfitrión de destino de este paquete.
3. El paquete luego pasa al driver de paquete, que busca la entrada para la dirección IP Asignada y determina que no es necesaria la NAT.
- 10 4. El Paquete luego se transmite al cliente.

NAT

- 15 Escenario: un cliente configurado con IP Fija envía y recibe paquetes a través del servidor SolutionIP.

Enviar

- 20 1. El cliente genera un paquete para un anfitrión remoto enrutado a través de su portal (no obstante, el servidor SolutionIP afirmará ser dicho portal cuando el cliente efectúe su solicitud ARP)
2. El Servidor SolutionIP recibe el paquete y lo pasa al driver de paquete
- 25 3. El driver de paquete examina el paquete y busca la IP Asignada en el Driver de Registro utilizando la dirección MAC.
4. El driver de paquete determina que la IP Asignada y la dirección de Fuente original no son iguales y que es necesaria la NAT.
- 30 5. Se ejecuta la NAT del paquete, y luego éste pasa a los filtros de paquete. Consultar las secciones de clientes Registrados y No Registrados a continuación.

35 *Recibir*

1. El paquete pasa de los filtros de paquete al gestor ARP.
2. El gestor ARP busca la dirección MAC del anfitrión de destino de este paquete.
- 40 3. El paquete luego pasa al driver de paquete, que busca la entrada para la dirección IP Asignada y determina que es necesaria la NAT.
4. El driver de paquete ejecuta la NAT del paquete y transmite el paquete al cliente.
- 45

Registrado

Enrutable

- 50 Escenario: el servidor SolutionIP recibe y envía el tráfico de y a un cliente registrado con una dirección IP asignada enrutable.

55 *Enviar*

1. Los paquetes de filtro reciben el paquete.
2. Se determina que el paquete puede transmitirse.
- 60 3. El paquete se envía a la interfaz externa apropiada, a través del router apropiado. (Por lo general hay una sola interfaz externa y un solo router).

65 *Recibir*

1. La interfaz externa recibe el paquete.

ES 2 334 634 T3

2. El paquete pasa a los filtros de paquete y se determina que puede transmitirse.

3. El paquete pasa al gestor ARP para que se le añada la MAC apropiada (Consultar la sección sobre NAT o Recibo DHCP apropiada más arriba).

No enrutable (Enmascaramiento)

Escenario: el servidor SolutionIP recibe y envía el tráfico de y a un cliente registrado con una dirección IP asignada no enrutable configurado para enmascarar las direcciones no enrutables.

Enviar

1. La interfaz externa recibe el paquete.

2. Se determina que el paquete debe enmascarse.

3. Los filtros de paquete asignan un puerto en el servidor SolutionIP para el puerto de fuente de este cliente.

4. El paquete se transmite con NAT de modo tal que simula haber provenido del servidor SolutionIP en el puerto asignado.

Recibir

1. La interfaz externa recibe el paquete.

2. El paquete pasa a los filtros de paquete y se determina que este puerto es un puerto simulado y que debe efectuarse al paquete una NAT inversa, para que tenga el puerto de destino y la dirección IP apropiados.

3. Los filtros de paquete determinan que el paquete puede transmitirse.

4. El paquete pasa al gestor ARP para que se le añada la MAC apropiada. (Consultar la sección sobre NAT o Recibo DHCP apropiada más arriba).

No registrado

Las reglas de filtro de paquete del servidor SolutionIP bloquean en general el tráfico de un cliente no registrado.

Caducidad del cliente

No registrado

Escenario: un cliente no registrado ha cumplido el tiempo de caducidad de registro.

1. El cliente utiliza diversos servicios de Internet.

2. El Driver de Dispositivo de Registro (Dispositivo Soln) ejecuta su función de purga (NOTA: esto ocurre dentro de un período histórico configurable).

3. La función de purga determina que el tiempo de caducidad de registro del cliente es inferior tiempo actual.

4. La función de purga marca la entrada como no registrada y calcula el tiempo de caducidad de la entrada. (NOTA: la conducta real depende del modo de caducidad).

5. Los Filtros de Paquete permiten que todas las conexiones establecidas permanezcan abiertas.

6. La próxima solicitud http iniciada desde el cliente se gestiona de la forma ya descrita (Consulte el Arranque de Navegador).

Purga

Escenario: un cliente no registrado ha cumplido su tiempo de caducidad y está inactivo.

ES 2 334 634 T3

1. El cliente se ha desconectado de la red o está de cualquier otro modo inactivo.

2. El Driver de Dispositivo de Registro ejecuta su función de purga.

3. La función de purga determina que el tiempo de caducidad de entrada del cliente (calculado como el último tiempo de uso más el período de gracia de inactividad) es inferior al tiempo corriente.

4. La entrada se elimina del Driver de Registro.

5. Todo tráfico futuro del cliente se gestiona de la forma ya descrita (Consultar Arranque del Cliente).

Un experto en el campo podría pensar en muchas variaciones y modificaciones sin apartarse del invento.

REIVINDICACIONES

1. Un método para proveer a un usuario acceso a una red (104) para un ordenador (101, 201, 301, 401, 501, 601, 701, 811) configurado para una primera red,
5
siendo este método implementado por un (103, 801, 802) que permita al ordenador (101, 201, 301, 401, 501, 601, 701, 811) el acceso a la red (104) a través de una segunda red sin la necesidad de software existente iniciado por el usuario o modificaciones en la configuración de hardware existente,
10
y
el método que consta de los pasos de:
15
determinación y asignación automática de una dirección de Internet Protocol (IP) para el ordenador (101, 201, 301, 401, 501, 601, 701, 811) conectado a la segunda red;
registro del ordenador (101, 201, 301, 401, 501, 601, 701, 811) en relación con la información de dirección, incluyendo la dirección IP asignada y una dirección de Media Access Control o dirección MAC del ordenador (101, 201, 301, 401, 501, 601, 701, 811);
20
almacenaje y mantenimiento de la información de dirección para los ordenadores registrados;
filtro de paquete para permitir que sólo los ordenadores registrados tengan acceso a la red (104); y traducción de una dirección IP en un paquete en base a la dirección MAC, y el transparente direccionamiento de tráfico a y desde el ordenador (101, 201, 301, 401, 501, 601, 701, 811) desde y a la red (104) en base a la información de dirección,
25
y
en el cual el paso de registro incorpore el paso de recopilar y mantener información de estado de facturación y registro, en el cual el paso de recopilación y mantenimiento incluye el paso de identificar el ordenador para fines de facturación mediante el uso de un Simple Network Management Protocol SNMP (809) y una arquitectura de conmutación de red (810) para identificar un puerto de conmutador al cual el ordenador (101, 201, 301, 401, 501, 601, 701, 811) está conectado.
30
2. El método de la reivindicación 1 en el cual el paso de determinación y asignación automática incorpora el paso de examinar si un paquete de entrada del ordenador (101, 201, 301, 401, 501, 601, 701, 811) es un paquete IP o ARP, y el paso de determinar la dirección IP asignada sobre la base de la IP o ARP del paquete.
35
3. El método de la reivindicación 2 en el cual el paso de asignación automática incorpora el paso de asignar una dirección IP al ordenador (101, 201, 01, 401, 501, 601, 701, 811) proveniente de un grupo de direcciones IP para la red (104).
40
4. El método de la reivindicación 3 en el cual el paso de registro incorpora el paso de establecer un período de registro durante el cual se permite al ordenador (101, 201, 301, 401, 501, 601, 701, 811) acceso a la red (104).
45
5. El método de la reivindicación 4 en el cual el paso de mantenimiento incluye el paso de desregistrar el ordenador (101, 201, 301, 401, 501, 601, 701, 811) cuando caduca el período de registro.
50
6. El método de la reivindicación 1 en el cual el paso de mantenimiento de la información de facturación incluye el paso de almacenaje de la información recopilada en una base de datos (803).
7. El método de la reivindicación 1 en el cual los pasos de mantenimiento de información sobre el estado de dirección, facturación y registro incorpora el paso de efectuar un backup periódico de la información.
55
8. El método de la reivindicación 1 en el cual los pasos de mantenimiento de información sobre el estado de dirección, facturación y registro incorpora el paso de recargar la información de backup más corriente en el caso de fallo del ordenador.
60
9. El método de la reivindicación 6 en el cual el paso de recopilación y mantenimiento incluye el paso de identificar el ordenador para fines de facturación a través de un código de acceso previamente emitido.
10. Un medio de ordenador factible de lectura que contenga las instrucciones de ordenador que al ser ejecutadas en un ordenador desarrollan los pasos de la reivindicación 1.
65
11. Un servidor (103, 801, 802) para proveer a un usuario acceso a una red (104) para un ordenador (101, 201, 301, 401, 501, 601, 701, 811), con el ordenador (101, 201, 301, 401, 501, 601, 701, 811) configurado para la primera red, y el servidor (103, 801, 802) equipado para permitir al ordenador (101, 201, 301, 401, 501, 601, 701, 811) el acceso

ES 2 334 634 T3

a la red (104) a través de una segunda red sin necesidad de reconfigurar el ordenador (101, 201, 301, 401, 501, 601, 701, 811) a través del hardware o software existente; constando el servidor (103, 801, 802) de:

un módulo de registro (202) para registrar al ordenador (101, 201, 301, 401, 501, 601, 701, 811) para que tenga acceso a la red (104);

un driver de registro (304, 404, 504, 604, 704, 806) para la asignación transparente de una dirección IP al ordenador (101, 201, 301, 401, 501, 601, 701, 811), para el mantenimiento y acceso a información de dirección incluyendo la dirección IP asignada y una dirección MAC del ordenador (101, 201, 301, 401, 501, 601, 701, 811), y para recopilar y mantener información del estado de facturación y registro;

una interfaz interna (302, 402, 502, 602, 702) para conectar el servidor (103, 801, 802) al ordenador (101, 201, 301, 401, 501, 601, 701, 811);

una interfaz externa (308, 707) para conectar el servidor (103, 801, 802) a la red (104); un módulo de driver de paquete (303, 403, 503, 603, 703) para ejecutar la NAT en la interfaz interna (302, 402, 502, 602, 702) en base a la dirección MAC; un filtro de paquete (305, 306, 407, 606, 705, 706) para filtrar los paquetes y permitir la transmisión de los paquetes a y desde la interfaz externa (308, 707) desde y a la interfaz interna según el estado de registro;

un módulo DHCP (316, 405) para el procesamiento de la solicitud DHCP en base a la dirección IP asignada;

un módulo ARP (307, 408, 505, 605, 710) para detectar una solicitud ARP y para hacer que el driver de registro (304, 404, 504, 604, 704, 806) asocie la dirección MAC y la dirección IP asignada, y

un Demonio SNMP (809) para identificar el ordenador para fines de facturación mediante el uso de un Simple Network Management Protocol (SNMP) y una arquitectura de conmutación de red (810) para identificar un puerto de conmutación al cual el ordenador (101, 201, 301, 401, 501, 601, 701, 811) está conectado;

en el cual en respuesta al tráfico del ordenador (101, 201, 301, 401, 501, 601, 701, 811) a la red (104), el servidor (103, 801, 802) transparentemente redirige el tráfico y tiene acceso a la red (104) en base a la información de dirección.

12. El servidor de la reivindicación 11 en el cual el módulo de registro también incorpora una interfaz de usuario con base web (805).

13. El servidor de la reivindicación 12 en el cual se determina a través de la interfaz de usuario con base web si el ordenador está conectado desde un cuarto facturable mediante el uso del Demonio SNMP (809) y la arquitectura de conmutación de la red (810).

14. El servidor de la reivindicación 12 en el cual se determina a través de la interfaz de usuario con base web si el ordenador (101, 201, 301, 401, 501, 601, 701, 811) está conectado desde un cuarto facturable mediante el uso de un código de acceso previamente emitido.

15. El servidor de la reivindicación 11 en el cual la dirección de dirección mantenida por el driver de registro incluye una dirección IP original, la dirección IP asignada, y la dirección MAC del ordenador (101, 201, 301, 401, 501, 601, 701, 811), y el estado de registro, siendo la dirección IP original la dirección IP originalmente asignada al ordenador (101, 201, 301, 401, 501, 601, 701, 811) para la primera red cuando el ordenador es un cliente IP fijo, y siendo un valor implícito cuando el ordenador es un cliente DHCP.

16. El servidor de la reivindicación 15 en el cual el módulo de driver de paquete sólo traduce un encabezado de paquete si la dirección IP original no es igual a la dirección IP asignada.

17. El servidor de la reivindicación 11 en el cual el filtro de paquete también traduce un número de puerto a un encabezado TCP/UDP, según sea necesario.

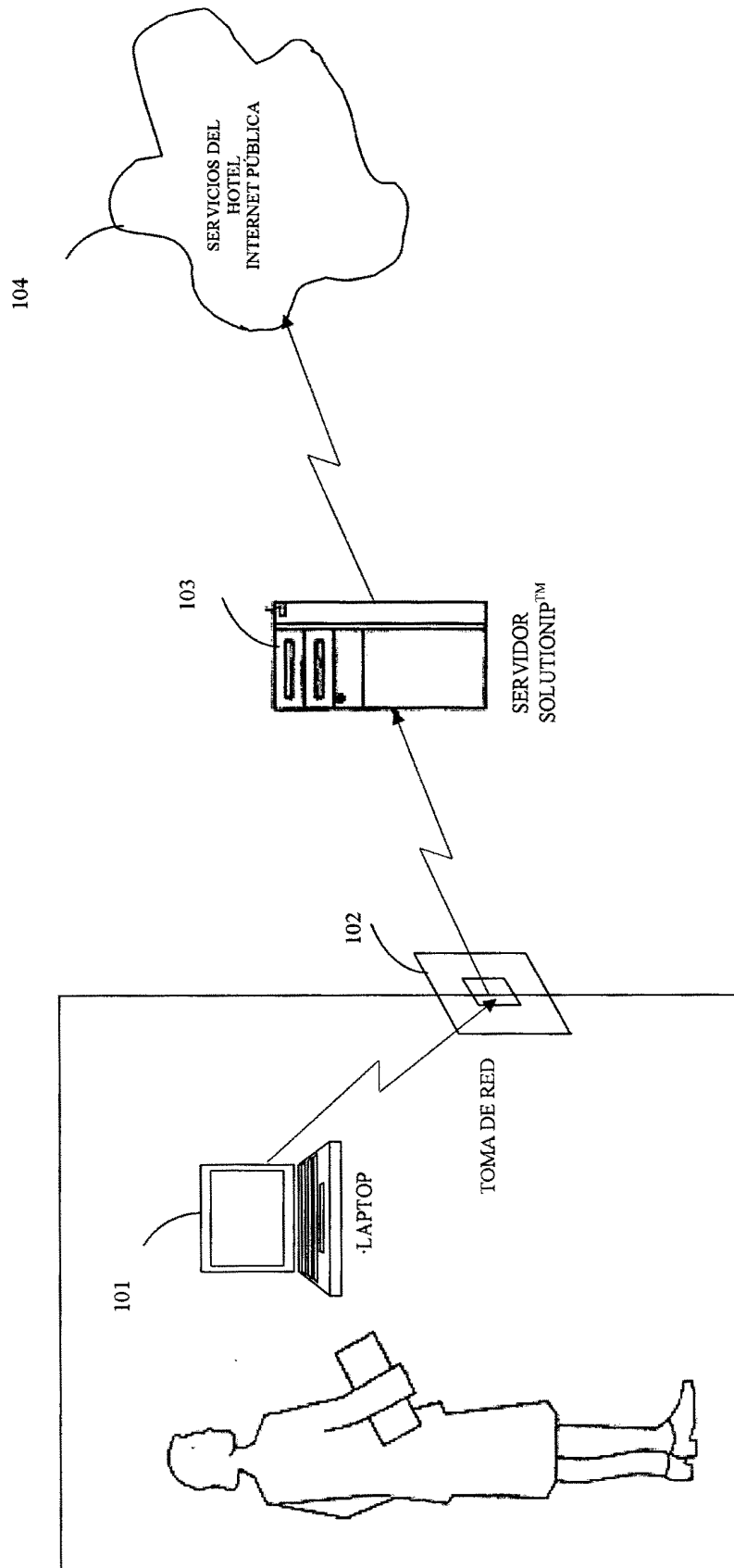


FIG. 1

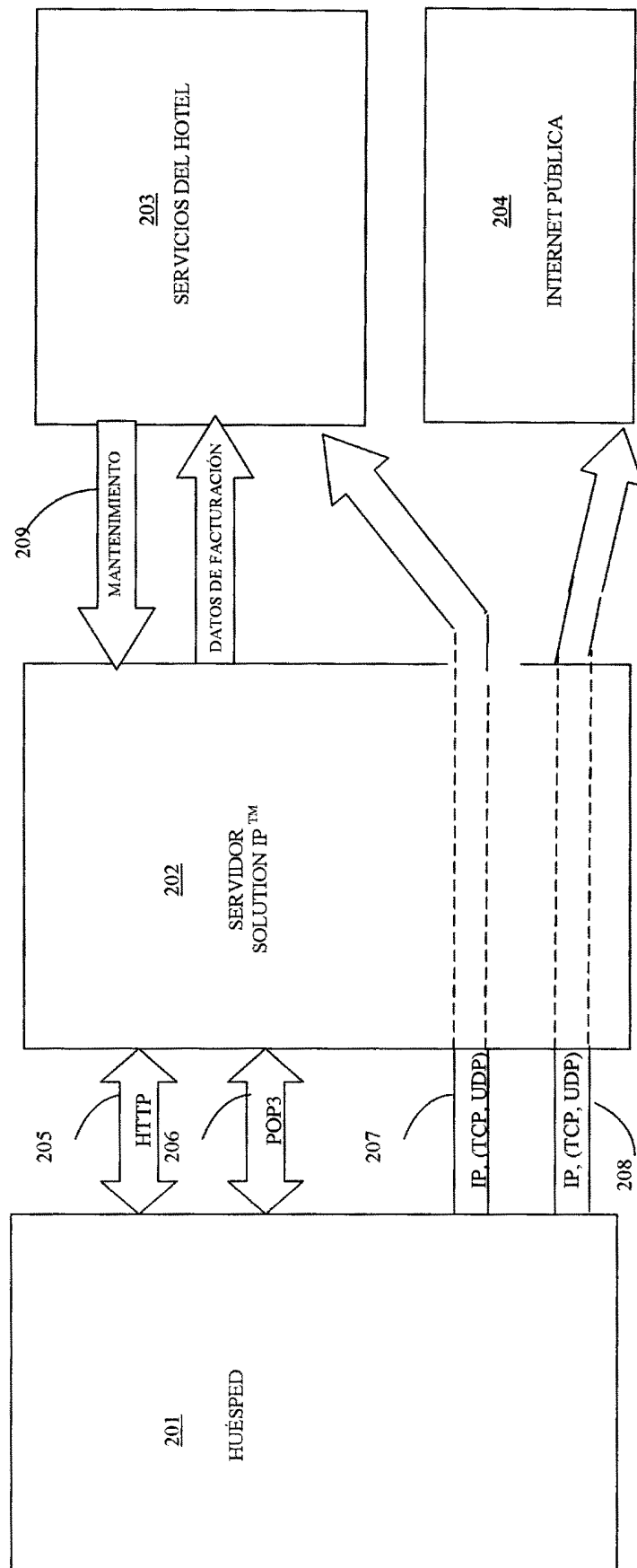


FIG. 2

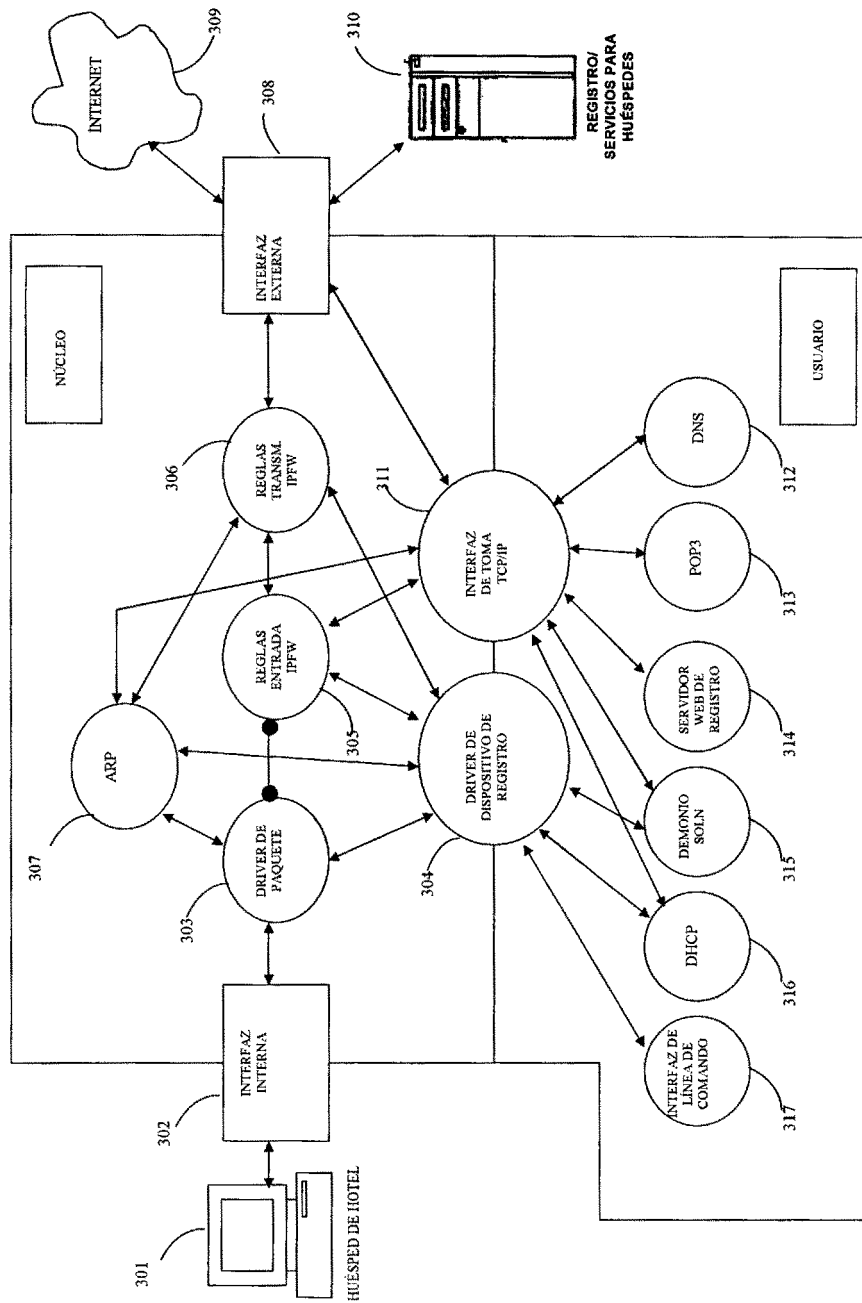


FIG. 3

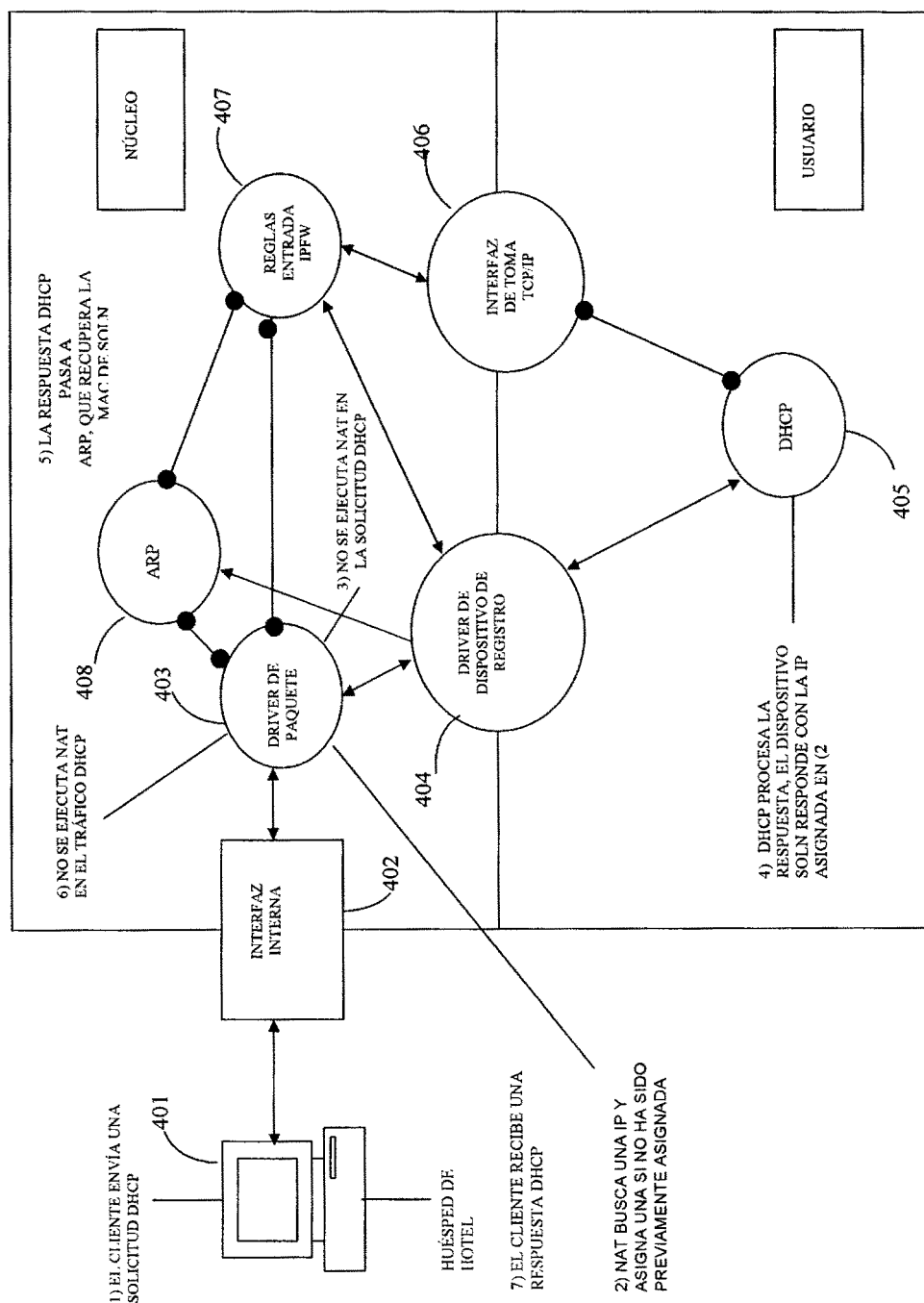


FIG. 4

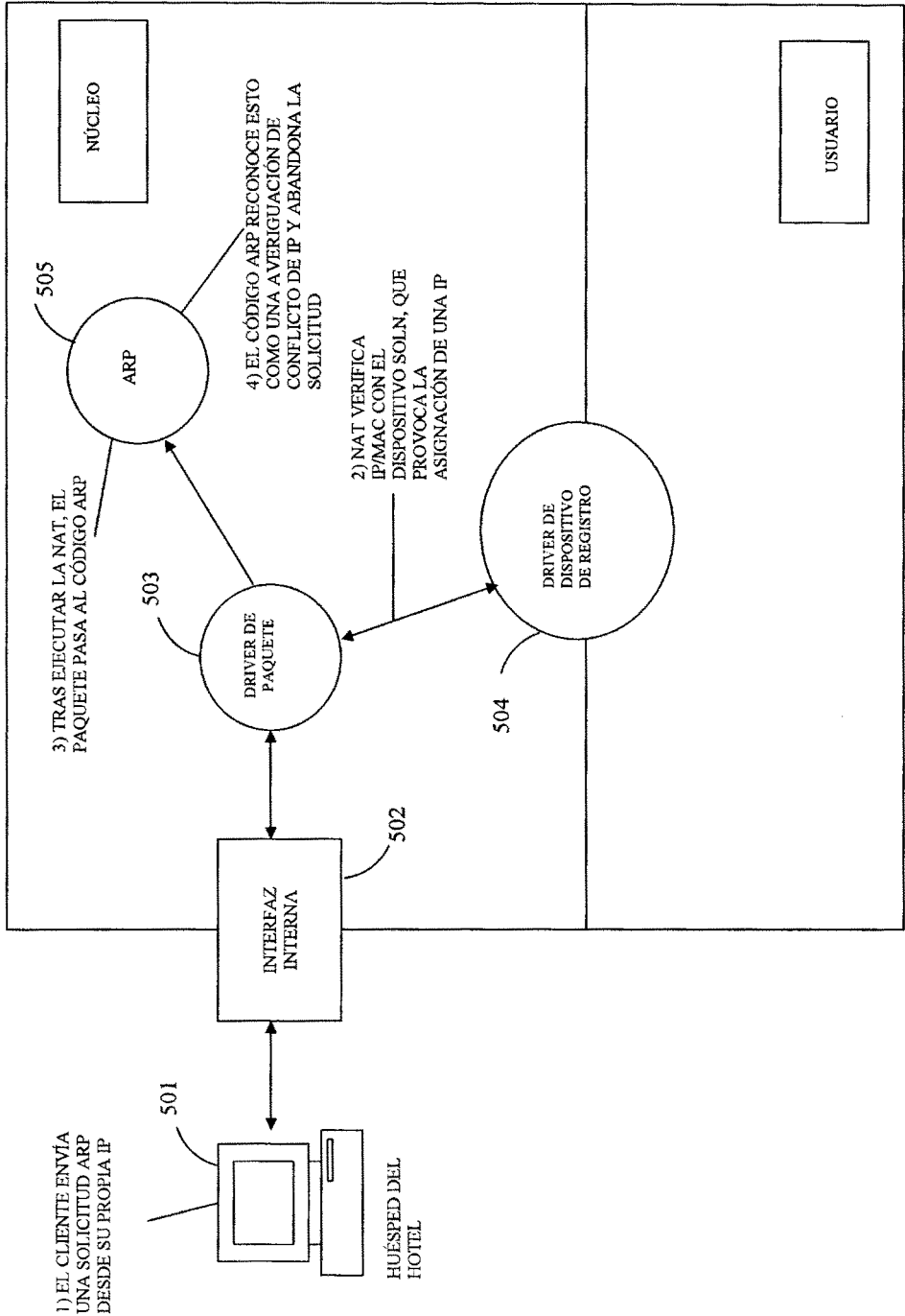


FIG. 5

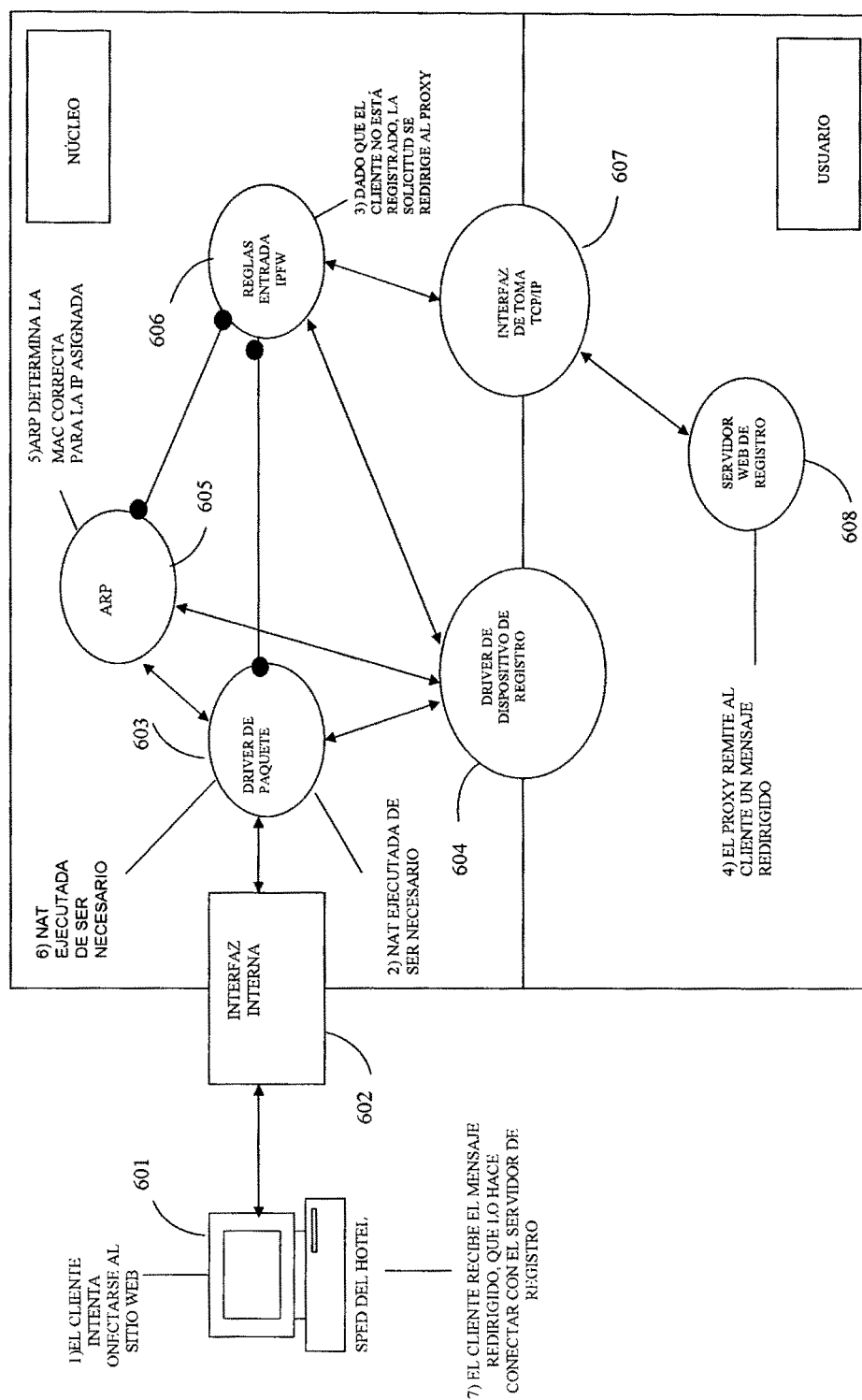


FIG. 6

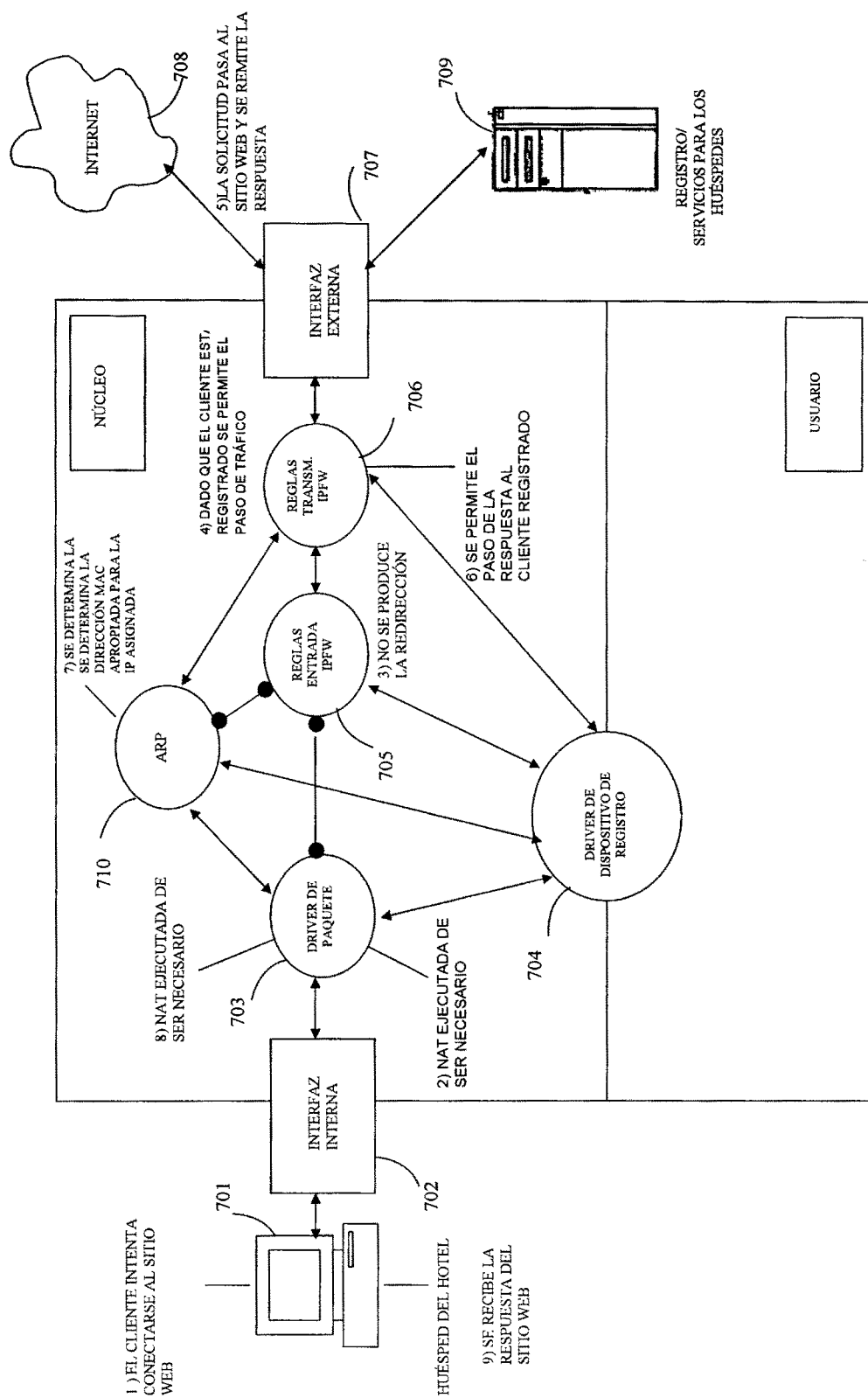


FIG. 7

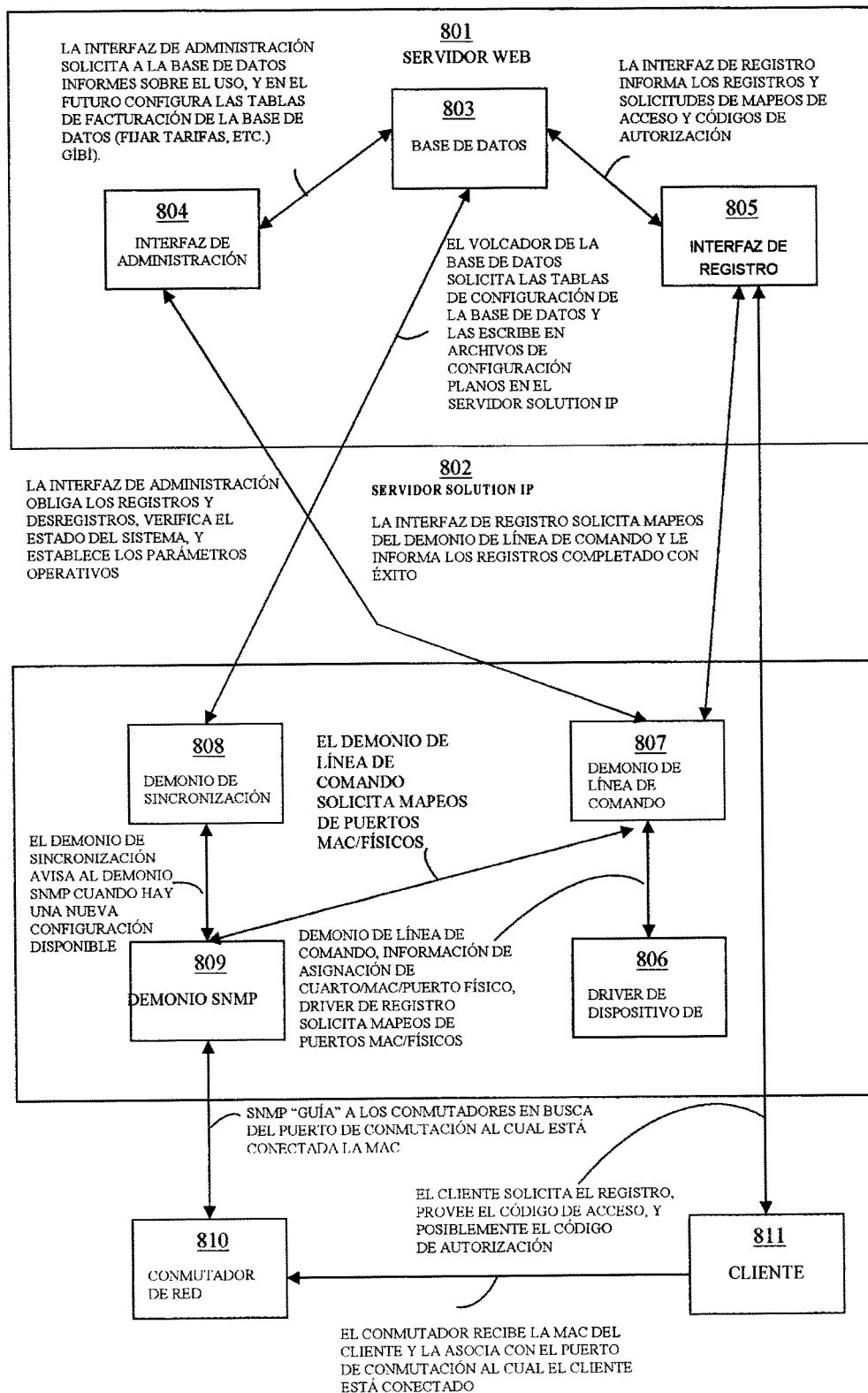


FIG. 8