(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 364 736**

(51) Int. Cl.:
H04L 12/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09005810 .8**
(96) Fecha de presentación : **20.10.2000**
(97) Número de publicación de la solicitud: **2093928**
(97) Fecha de publicación de la solicitud: **26.08.2009**

(54) Título: **Sistema y método para proporcionar una autorización, autenticación y contabilidad de red dinámicas.**

(30) Prioridad: **22.10.1999 US 161093 P**
22.10.1999 US 161181 P
22.10.1999 US 161182 P
22.10.1999 US 160890 P
22.10.1999 US 161139 P
22.10.1999 US 161189 P
22.10.1999 US 160973 P
08.12.1999 US 458602
08.12.1999 US 458569

(45) Fecha de publicación de la mención BOPI:
13.09.2011

(45) Fecha de la publicación del folleto de la patente:
13.09.2011

(73) Titular/es: **NOMADIX, Inc.**
30851 Agoura Road, Suite 102
Agoura Hills, California 91301, US

(72) Inventor/es: **Short, Joel E.;**
Pagan, Florence C. I. y
Goldstein, Josh J.

(74) Agente: **Morales Durán, Carmen**

DESCRIPCIÓN

Sistema y método para proporcionar una autorización, autenticación y contabilidad de red dinámicas

La invención se refiere en general a sistemas y métodos para el control del acceso a la red y, más particularmente, a sistemas y métodos para establecer un acceso dinámico del usuario a la red.

Antecedentes de la invención

El acceso de usuarios a redes de ordenadores se ha basado tradicionalmente en un proceso de autenticación en dos etapas que o bien proporciona a un usuario un acceso a la red total o rechaza cualquier acceso del usuario en cualquier circunstancia. En la primera etapa del proceso, un usuario establece un enlace de comunicación con una red a través de una línea de teléfono, una conexión de red dedicada (por ejemplo, banda ancha, Línea de Señal Digital (DSL)) u otra similar. En la segunda etapa del proceso de autenticación, el usuario debe introducir información de identificación para obtener acceso a la red. Típicamente, la información de identificación de entrada incluye un nombre de usuario y palabra clave. Usando esta información, la red o el proveedor de servicio verifica que el usuario tiene derecho al acceso a la red mediante la determinación de si la información de identificación coincide con la información de abonado contenida en una tabla (o base de datos) de abonados que almacena información de identificación para todos los usuarios autorizados para acceder a la red. Cuando la información de entrada del usuario coincide con los datos de abonado en la tabla de abonados, se autoriza al usuario para acceder a cualquiera y a todos los servicios en la red. Por otro lado, si la información de identificación de entrada del usuario no coincide con los datos de abonado en la tabla, el usuario tendrá denegado el acceso a la red. Por ello, una vez que la identidad del usuario se compara con los datos almacenados dentro de una tabla de abonados, o bien se le da al usuario derecho para acceder a la red o se le niega el acceso totalmente. Adicionalmente, cuando se autoriza al usuario a acceder a la red, el usuario está autorizado típicamente para acceder a cualquier destino accesible a través de la red. Por lo tanto, la autenticación convencional de usuarios se basa en un enfoque de todo o nada en el acceso a la red.

En muchas aplicaciones convencionales de acceso a la red, tales como en aplicaciones convencionales de acceso a Internet, la base de datos (o tabla) de abonados no sólo almacena datos que corresponden a la identidad de los abonados autorizados para acceder a la red, sino que también almacena información que puede variar en base al abonado particular. Por ejemplo, la base de datos de abonados puede incluir perfiles de abonado que indiquen el tipo de acceso que un abonado debería recibir y otra información relacionada, tal como las tarifas debidas por el abonado para el acceso a la red. Aunque la información en la base de datos de abonados puede variar de un usuario a otro, se usa generalmente una información única en la base de datos para finalidades de facturación o mantenimiento de la red. Por ejemplo, las bases de datos de abonados convencionales incluyen típicamente datos tales como el coste que el abonado está pagando para el acceso la red y la cantidad de tiempo que el abonado ha accedido a la red. Así, cuando un abonado a un Proveedor de Servicios de Internet (ISP) ha comprado un acceso a Internet, una base de datos de perfiles de origen puede contener información que permita a un usuario ser autenticado y hace un seguimiento del acceso del usuario con finalidades de contabilidad, tal como mantener un registro del tiempo del usuario en la red.

Adicionalmente, en sistemas convencionales de acceso a la red, para que un usuario se conecte a servicios en línea (por ejemplo, la Internet), el usuario debe instalar un software del lado de cliente en el ordenador del usuario. Este software del lado cliente se proporciona típicamente por un administrador de la red o proveedor de acceso a la red, tal como un ISP con el que el usuario ha suscrito un acceso a Internet y permite al cliente configurar su ordenador para comunicarse con ese proveedor de acceso a la red. Continuando con el ejemplo ilustrativo de un usuario que accede a Internet a través de un ISP, el usuario debe instalar un software del ISP en el ordenador del cliente y posteriormente establecer una cuenta con el ISP para acceso a Internet. Típicamente, un usuario se abona a un ISP tal como America Online™, Earthlink™, Compuserve™ u otro similar, mediante la contratación directamente con el ISP para el acceso a Internet. Normalmente, el usuario paga por tal acceso a Internet en base a una tasa fija mensual. Independientemente de la localización del usuario, el usuario puede marcar un número de acceso proporcionado por el ISP y obtener un acceso a Internet. La conexión se consigue frecuentemente por medio de un módem telefónico convencional, cable módem, conexión DSL u otra similar.

Debido a que el acceso de usuarios a la red a través de métodos convencionales, tales como a través de los ISP, o bien tienen permitido o denegado el acceso a la red en un enfoque todo o nada, los usuarios no pueden ser autorizados dinámicamente a acceder a la red de modo que el acceso del usuario y la autorización para redes o sitios particulares se pueda personalizar. Lo que se necesita es un método y sistema que permita un acceso dinámico de los usuarios y que se pueda personalizar que pueda variar en base a cualquier número de variables asociadas con un usuario, tal como una localización del usuario, nombre de usuario o palabra clave, ordenador del usuario u otros atributos. Por ejemplo, sería ventajoso para algunos usuarios tener el acceso autorizado a todos los sitios de Internet, mientras que otros pueden tener denegado el acceso a sitios particulares. Además de autorizar el acceso del usuario a una red, sería ventajoso para una red, tal como un ISP o redes de empresa, permitir selectivamente a los usuarios un intervalo de autorización, de modo que el acceso del usuario no se base en un enfoque de todo o nada.

El documento US-A-5950195 describe un método para determinar los derechos de acceso en base a una lista de control de acceso y en el que se transmiten paquetes a través de un cortafuegos. Se filtran las condiciones iniciales y si es necesaria una autenticación, se presenta una petición de nombre de usuario y se usa el nombre del usuario para realizar una comprobación en la lista de control de acceso.

El documento EP-A-0909073 describe técnicas para implementar cortafuegos de redes de ordenadores. El cortafuegos recibe paquetes y aplica reglas que corresponden a cada paquete en base a las interfaces de entrada y salida de la red, las direcciones de origen y destino de la red y el tipo de servicio.

El documento EP-A-0762707 describe una comprobación/control para acceso a redes IP por medio de una red de telecomunicaciones. Un filtro permite un acceso inicial a un servidor de comprobación/control que a su vez tiene comandos de funciones de bloqueo para el acceso a la red IP.

Sumario de la invención

La presente invención incluye un método y un sistema para la implementación y cumplimiento de una Autenticación, Autorización y Contabilidad (AAA) de usuarios que acceden a la red por medio de un dispositivo de pasarela. De acuerdo con la presente invención, un usuario puede ser primero autenticado para determinar la identidad del usuario. La capacidad de autenticación del sistema y el método de la presente invención se pueden basar en un ID de usuario, ordenador, localización o uno o más atributos adicionales de identificación de un origen (por ejemplo, un usuario, ordenador o localización particular) que solicita acceso a la red. Una vez autenticado, la capacidad de autorización del sistema y método de la presente invención se personaliza en base a la identidad del origen, tal como orígenes que tengan diferentes derechos de acceso en base a su identidad y el contenido y/o destino solicitado. Por ejemplo, los derechos de acceso permiten a un primer origen acceder a una dirección de destino de Internet particular, mientras que rechazan el acceso de un segundo origen a esa misma dirección. Además, la capacidad de autorización del sistema y método de la presente invención se puede basar en otra información contenida en la transmisión de datos, tal como un puerto de destino, dirección de Internet, puerto TCP, red o direcciones de destinos similares. Más aún, la AAA de la presente invención se puede basar en el tipo de contenido o protocolo que está siendo transmitido. Mediante la autenticación de los usuarios en esta forma, cada paquete se puede filtrar a través de un proceso de AAA selectivo, de modo que se puede identificar a un usuario y autorizarle el acceso a un destino particular. Por ello, cada vez que el usuario intenta acceder a un destino diferente, el usuario se somete a la AAA, de modo que se pueda impedir el acceso del usuario a un sitio particular que el sistema y método AAA considera inaccesible para el usuario en base a la autorización del usuario mientras que permite el acceso a otros sitios que el método y sistema AAA considera accesible. Adicionalmente, de acuerdo con una realización de la invención, la dirección de origen de la red se puede seguir y registrar mediante la presente invención con finalidades de contabilidad y de históricos.

De acuerdo con una realización de la invención, se describe un método para controlar y personalizar de modo selectivo el acceso de un origen a una red, en el que el origen se asocia con un ordenador de origen y en el que el ordenador de origen tiene un acceso transparente a la red por medio de un dispositivo de pasarela y no se necesita instalar ningún software de configuración en el ordenador de origen para acceder a la red. El método incluye la recepción en el dispositivo de pasarela de una solicitud para el acceso a la red desde el ordenador de origen, la identificación de un atributo asociado con el origen en base a un paquete transmitido desde el ordenador de origen y recibido por el dispositivo de pasarela y el acceso a un perfil de origen que corresponde al origen y que está almacenado en una base de datos de perfiles de origen, en el que se accede al perfil de origen en base al atributo y en el que la base de datos de perfiles de origen está localizada de modo externo al dispositivo de pasarela y en comunicación con el dispositivo de pasarela. El método incluye también la determinación de los derechos de acceso al origen en base al perfil de origen, en el que los derechos de acceso definen los derechos del origen para acceder a la red.

De acuerdo con un aspecto de la invención, la determinación de los derechos de acceso del origen en base al perfil de origen incluye la determinación de los derechos de acceso del origen en base al perfil de origen, en el que los derechos de acceso definen los derechos del origen para acceder al destino de red solicitado. De acuerdo con otro aspecto de la invención, el método incluye la asignación de un identificador de localización a la localización desde la que se transmite la solicitud para acceso a la red y el identificador de localización es el atributo asociado con el origen. Adicionalmente, de acuerdo con la invención, el acceso a un perfil de origen que corresponde al origen puede incluir el acceso a un perfil de origen almacenado en una base de datos de perfiles de origen, en la que la base de datos de perfiles de origen incluye un servicio de usuario de marcación para autenticación remota (RADIUS) o una base de datos del protocolo ligero de acceso a directorios (LDAP).

De acuerdo con otro aspecto más de la invención, el método incluye la actualización de la base de datos de perfiles de origen cuando un nuevo origen accede a la red. Adicionalmente, el método puede incluir el mantenimiento en la base de datos de perfiles de origen de un registro histórico de los accesos de los orígenes a la red. Más aún, el atributo asociado con el origen se puede basar en una dirección MAC, ID de usuario o ID de VLAN asociada con el ordenador de origen desde el que se transmitió la solicitud para acceso a la red. De acuerdo con otro aspecto más

de la invención, la recepción en el dispositivo de pasarela de una solicitud desde un origen para acceso puede incluir la etapa de recepción de una dirección de destino desde el origen.

De acuerdo con otra realización de la invención, se describe un sistema para el control y personalización de modo selectivo del acceso, a una red, mediante un origen, en el que el origen se asocia con un ordenador de origen en el que el ordenador de origen tiene acceso transparente a la red por medio de un dispositivo de pasarela y no se necesita instalar ningún software de configuración en el ordenador de origen para acceder a la red. El sistema incluye un dispositivo de pasarela para la recepción de las solicitudes del origen para el acceso a la red y una base de datos de perfiles de origen en comunicación con el dispositivo de pasarela y situada externamente al dispositivo de pasarela, en el que la base de datos de perfiles de origen almacena información de acceso identificable mediante un atributo asociado con el origen y en el que el atributo se identifica en base a un paquete de datos transmitido desde el ordenador de origen y recibido por el dispositivo de pasarela. El sistema también incluye un servidor de AAA en comunicación con el dispositivo de pasarela y base de datos de perfiles de origen, en el que el servidor de AAA determina si el origen tiene derecho a acceder a la red en base a la información de acceso almacenada dentro de la base de datos de perfiles de origen y en el que el servidor de AAA determina los derechos de acceso del origen con los derechos de acceso que definen los derechos del origen a acceder a los sitios de destino a través de la red.

De acuerdo con un aspecto de la invención, el paquete recibido por el dispositivo de pasarela incluye al menos un ID de VLAN, un ID de circuito y una dirección MAC. Adicionalmente, de acuerdo con otro aspecto de la invención, la base de datos de perfiles de origen incluye un servicio de usuario de marcación para autenticación remota (RADIUS) o una base de datos del protocolo ligero de acceso a directorios (LDAP). Adicionalmente, la base de datos de perfiles de origen puede incluir una pluralidad de perfiles de origen, en el que cada perfil de origen respectivo de la pluralidad de perfiles de origen contiene información de acceso. De acuerdo con la invención, cada perfil de origen respectivo puede contener también datos históricos en relación a la duración del acceso a la red para su uso en la determinación de los cargos debidos por el acceso a la red. De acuerdo con otro aspecto más de la invención, la base de datos de perfiles de origen se puede localizar dentro del servidor que AAA.

De acuerdo con otra realización de la presente invención, hay descrito un método para la redirección de un origen que intenta acceder a un destino a través de un dispositivo de pasarela, en el que el origen se asocia con un ordenador de origen y en el que el dispositivo de pasarela permite al origen comunicar con una red sin requerir que el ordenador de origen incluya software de red configurado para la red. El método incluye la recepción en el dispositivo de pasarela de una solicitud desde el origen para acceder a la red, la identificación del origen en base a un atributo asociado con el origen y el acceso a una base de datos de perfiles de origen localizada externamente al dispositivo de pasarela, en el que la base de datos de perfiles de origen almacena derechos de acceso para el origen. El método incluye además la determinación de los derechos de acceso del origen en base a la identificación del origen, en el que los derechos de acceso definen los derechos del origen para acceder a sitios de destino a través de la red.

De acuerdo con un aspecto de la invención, el acceso a una base de datos de perfiles de origen incluye el acceso a una base de datos de perfiles de origen que incluye un servicio de usuario de marcación para autenticación remota (RADIUS) o una base de datos del protocolo ligero de acceso a directorios (LDAP). De acuerdo con otro aspecto de la invención, el método puede incluir la asignación de un identificador de localización a la localización desde la que se transmite la solicitud para acceso a la red, en el que el identificador de localización es el atributo asociado con el origen. El método puede incluir también la actualización de la base de datos de perfiles de origen cuando un nuevo origen accede a la red y el mantenimiento en una base de datos de contabilidad de un registro histórico para el acceso del origen a la red, en el que la base de datos de contabilidad está en comunicación con la base de datos de perfiles de origen.

De acuerdo con otro aspecto más de la invención, la recepción en el dispositivo de pasarela de las solicitudes de un origen para acceso puede incluir la etapa de recepción de la dirección del destino desde el origen. Más aún, la determinación de si el ordenador de origen tiene derecho de acceso a la dirección de destino puede incluir además la denegación del acceso al ordenador de origen en el que el perfil de origen indica que el ordenador de origen tiene denegado el acceso. La determinación de si el origen tiene derecho a acceso a la red puede incluir también además el direccionamiento del origen a una página de registro cuando el perfil de origen no está situado dentro de la base de datos de perfiles de origen.

De acuerdo con otra realización más de la invención, hay descrito un sistema para permitir una comunicación transparente entre un ordenador y una red del proveedor de servicios. El sistema incluye un ordenador y un dispositivo de pasarela de red en comunicación con el ordenador para la conexión del ordenador a una red de ordenadores, en la que el dispositivo de pasarela de red recibe datos de origen que representan un usuario que intenta acceder a dicha red de ordenadores. El sistema incluye también una red del proveedor de servicios en comunicación con el dispositivo de pasarela de red, en el que la red del proveedor de servicios incluye un servidor de autenticación localizado externamente al dispositivo de pasarela de red y en comunicación con el dispositivo de pasarela de red. El servidor de autenticación tiene en él una base de datos de perfiles de origen que comprende perfiles de origen que representan a los usuarios autorizados para acceder a dicha red de ordenadores y compara

los datos de origen con dichos perfiles de origen para determinar si el usuario que intenta acceder a la red de ordenadores puede acceder a la red de ordenadores.

De acuerdo con un aspecto de la invención, el sistema puede incluir un sistema de contabilidad para el mantenimiento de datos históricos en relación con el uso de la red del proveedor de servicios. De acuerdo con otro aspecto de la invención, el servidor de autenticación incluye un servicio de usuario de marcación para autenticación remota (RADIUS) o una base de datos del protocolo ligero de acceso a directorios (LDAP). Adicionalmente, la base de datos de perfiles de origen puede incluir una pluralidad de perfiles de origen, en el que cada perfil de origen respectivo de la pluralidad de perfiles de origen contiene información de acceso. De acuerdo con otro aspecto más de la invención, los datos de origen incluyen un atributo asociado con el ordenador y transmitido desde el ordenador al dispositivo de pasarela. De acuerdo con otro aspecto de la invención, los datos de origen incluyen información de registro asociada con un usuario respectivo.

El método y sistema de Autenticación, Autorización y Contabilidad de acuerdo con la presente invención permite a los usuarios un acceso transparente a una red de ordenadores que emplea un dispositivo de pasarela. Por lo tanto, cada usuario puede tener diferentes derechos para acceder a servicios, sitios o destinos a través de la red. Por ello, la presente invención difiere de los métodos y sistemas convencionales de AAA mediante la oferta de servicios de AAA dinámicos que autentican usuarios y ofrecen a esos usuarios grados variables de autorización para utilizar la red accedida. Adicionalmente, la base de datos de perfiles de origen de la presente invención se puede localizar externamente al dispositivo de pasarela y en una red no local respecto a la red desde la que se solicita el acceso. Es deseable una base de datos de perfiles de origen externa porque cada dispositivo de pasarela permite el acceso a la red a un número finito de usuarios, de modo que se puedan requerir múltiples dispositivos de pasarela. Adicionalmente, la administración y mantenimiento de una base de datos consolidada de datos de autenticación es más fácil que múltiples bases de datos más pequeñas. Más aún, la localización de la base de datos externa a la red local permite a un ISP o a un tercer proveedor mantener la confidencialidad de la información almacenada dentro de la base de datos y mantener y controlar la base de datos en la forma que el tercer proveedor lo desee.

Breve descripción de los dibujos

La FIGURA 1 es un diagrama de bloques de un sistema de ordenadores que incluye un servidor de AAA para la autenticación, autorización y contabilidad de orígenes que acceden a redes y/o servicios en línea, de acuerdo con una realización de la presente invención.
La FIGURA 2 es un diagrama de flujo de un método en el que el servidor de AAA realiza la autenticación, autorización y contabilidad de acuerdo con un aspecto de la invención.

Descripción detallada de las realizaciones preferidas

La presente invención se describirá ahora más completamente en el presente documento a continuación con referencia a los dibujos adjuntos, en los que se muestran las realizaciones preferidas de la invención. Esta invención puede, sin embargo, realizarse de muchas formas diferentes y no se debería interpretar como limitada a las realizaciones expuestas en el presente documento; por el contrario, estas realizaciones se proporcionan de modo que esta descripción sea global y completa y transmita totalmente el alcance de la invención para los expertos en la técnica. Los números similares se refieren a elementos iguales en toda ella.

Con referencia ahora a la FIGURA 1, se ilustra un sistema de ordenadores en la forma de un diagrama de bloques. El sistema de ordenadores **10** incluye una pluralidad de ordenadores **14** que pueden comunicar con uno o más servicios en línea **22** o redes por medio de un dispositivo de pasarela **12** que proporciona la interfaz entre los ordenadores **14** y las varias redes **20** o servicios en línea **22**. Una realización de un dispositivo de pasarela así se ha descrito en el documento U.S.-A-61308892.

Brevemente, el dispositivo de pasarela **12** facilita el acceso transparente del ordenador **14** a los servicios en línea **22** o redes **22**, de modo que los ordenadores **14** puedan acceder a cualquiera de las redes por medio del dispositivo **12** independientemente de sus configuraciones de red. Adicionalmente, el dispositivo de pasarela **12** incluye la capacidad para reconocer a los ordenadores que intentan acceder a una red **12**, la localización de los ordenadores que intentan acceder a la red, la identidad de los usuarios que intentan obtener acceso a la red y atributos adicionales como se explicará a continuación con relación a los métodos y sistemas de AAA dinámicos de la presente invención.

Como se ilustra en la FIGURA 1, el sistema de ordenadores **10** incluye también un concentrador de acceso **16** situado entre los ordenadores **14** y el dispositivo de pasarela **12** para multiplexar las señales recibidas desde la pluralidad de ordenadores sobre un enlace al dispositivo de pasarela **12**. Dependiendo del método mediante el que los ordenadores **14** se conectan al concentrador de acceso, el concentrador de acceso **16** se puede configurar en diferentes formas. Por ejemplo, el concentrador de acceso puede ser un multiplexor de acceso a línea de abonado digital (DSLAM) para señales transmitidas por medio de líneas telefónicas regulares, un extremo de cabecera de cable (una Plataforma de Terminación de Módem por Cable (CXMTS)) para señales transmitidas por medio de cables coaxiales, un punto de acceso inalámbrico (WAP) para señales transmitidas por medio de la red inalámbrica,

un conmutador u otro similar.

El sistema de ordenadores **10** incluye además un servidor de AAA **30** que auténtica y autoriza el acceso de usuarios dinámicamente, como se explica en detalle a continuación, esos usuarios se someten a un proceso de AAA tras el intento de obtener acceso a una red a través del dispositivo de pasarela **12**. Finalmente, como se muestra en la FIGURA 1, el sistema de ordenadores **10** incluye típicamente uno o más enrutadores **18** y/o servidores (no mostrado en la FIGURA 1) para controlar o dirigir el tráfico a y desde una pluralidad de redes de ordenadores **20** u otros servicios en línea **22**. Mientras que el sistema de ordenadores **10** se representa como que tiene un único enrutador, el sistema de ordenadores **10** puede tener una pluralidad de enrutadores, conmutadores, puentes u otros similares que se disponen en alguna forma jerárquica para enrutar adecuadamente el tráfico a y desde las varias redes **20** o servicios en línea **22**. En este sentido, el dispositivo de pasarela **12** establece típicamente un enlace con uno o más enrutadores. Los enrutadores, a su vez, establecen enlaces con los servidores de las redes **20** o servicios en línea **22**, en base en a la selección del usuario. Se apreciará por un experto en la técnica que se pueden combinar los uno o más dispositivos ilustrados en la FIGURA 1. Por ejemplo, aunque no se muestra, el enrutador **18** se puede localizar totalmente dentro del dispositivo de pasarela **12**.

Los usuarios de ordenadores que intentan acceder a una red **20** o servicio en línea **22** por medio del dispositivo de pasarela **12** se denominan en el presente documento a continuación como orígenes. De acuerdo con los métodos y sistemas de AAA de la presente invención, un origen que intenta acceder a una red por medio de un dispositivo de pasarela **12** se autentica en base a atributos asociados con él. Estos atributos pueden incluir la identidad de un usuario u ordenador particular, la localización a través de la que se solicita el acceso, red o destino solicitado y otros similares. Como se explica en detalle en el documento US-A-6130892, estos atributos se identifican mediante paquetes de datos transmitidos al dispositivo de pasarela **12** desde los ordenadores a través de los que se solicita el acceso. De acuerdo con una realización, los métodos y sistemas de la presente invención proporcionan una autenticación, autorización y contabilidad dinámica en base a estos atributos. Generalmente, como se usa en el presente documento, la autenticación se refiere a la identificación del origen, la autorización se refiere a la determinación del acceso que se permite al origen y la contabilidad se refiere al seguimiento del acceso del origen a la red.

Con referencia ahora a la función de autenticación de los sistemas y métodos de la presente invención, se apreciará que la autenticación de un origen que intenta acceder a la red es frecuentemente crucial para la administración de la red, dado que el acceso a la red y los servicios no se dejan típicamente abiertos para todos los usuarios independientemente de la identidad o del pago. Como se ha establecido anteriormente, un origen se puede identificar por el dispositivo de pasarela **12** mediante uno o más atributos contenidos dentro de los paquetes de datos transmitidos al dispositivo desde el ordenador asociado con el origen que intenta acceder a una red o servicio, denominado de aquí en adelante como el ordenador de origen. Por ejemplo, cuando el origen es un usuario, el ordenador de origen es el ordenador a través del que el usuario está intentando acceder a una red o destino de red. Por otro lado, cuando el origen es un ordenador al través del que uno o más usuarios pueden solicitar acceso a una red, el ordenador de origen es aquel ordenador a través del que se solicita el acceso.

De acuerdo con un aspecto de la invención, un ordenador de origen que intenta acceder a una red a través de un dispositivo de pasarela **12** puede tener identificados uno más atributos que incluyen un ID de circuito, dirección MAC, nombre de usuario, ID y/o palabra clave o situación particular (por ejemplo un puerto de comunicaciones en una habitación de hotel) u otra similar, transmitida al dispositivo de pasarela **12** por medio de paquetes de datos generados por el ordenador de origen, como se describe en el documento U.S. -A-2006/0239254.

Se apreciará que uno o más de estos atributos se pueden usar en la presente invención para identificar el origen que accede a la red. Por medio de un ejemplo ilustrativo, en el que los orígenes son usuarios diferentes que tienen derechos de autenticación y autorización no similares, los usuarios pueden identificarse a sí mismos mediante su respectiva información de registro (por ejemplo nombre de usuario y palabra clave) de modo que serán identificados independientemente a pesar del uso del mismo equipo tal como el mismo ordenador. Por otro lado, cuando el origen es un ordenador, diversos usuarios que usen el ordenador tendrán derechos similares de autenticación y autorización independientemente de los derechos individuales de cada usuario, dado que los derechos se asocian con el ordenador (por ejemplo identificado por la dirección MAC), más que con los usuarios respectivos.

La autenticación de orígenes por medio de un atributo asociado con el origen se realiza mediante el servidor de AAA **30**, ilustrado en la FIGURA 1. El servidor de AAA **30** almacena perfiles de origen que corresponden a los orígenes identificados por el servidor de AAA **30**. De acuerdo con un aspecto de la presente invención, el servidor de AAA **30**, se sitúa totalmente dentro del dispositivo de pasarela **12**. De acuerdo con otro aspecto de la invención, el servidor de AAA **30** puede comprender una pluralidad de componentes, al menos algunos de los cuales son externos al dispositivo de pasarela **12** o, alternativamente, el servidor de AAA **30** puede situarse completamente externo al dispositivo de pasarela **12**. Por ejemplo, la situación del servidor de AAA **30** puede ser tal que el dispositivo de pasarela **12** comunique con el servidor de AAA **30** a través del protocolo de Internet. De acuerdo con una realización de la invención, el servidor de AAA **30** se puede mantener por un ISP, que identifica los orígenes autorizados para comunicar con la red a través del ISP. Por lo tanto, se apreciará que el servidor de AAA **30** se puede situar en cualquier dirección de Internet y estar almacenado en cualquier ordenador accesible por medio del protocolo de

Internet.

De acuerdo con un aspecto de la invención, existe un perfil de orígenes separado para cada origen que accede al sistema. Los perfiles de origen se mantienen en una base de datos de perfiles de origen, que puede ser un componente interno del servidor de AAA **30**, un componente externo del servidor de AAA **30** o un componente separado en comunicación con el servidor de AAA **30**. Preferiblemente, la base de datos de perfiles de origen se sitúa externamente al dispositivo de pasarela y a la red para aliviar el esfuerzo administrativo en la red de modo que la red no tenga que establecer y mantener bases de datos de autenticación separadas en cada red o dispositivo de pasarela. Esto es también preferible porque cada dispositivo de pasarela **12** permite el acceso a la red a un número finito de usuarios, lo que requiere múltiples dispositivos de pasarela para adaptarse a un gran número de orígenes. En segundo lugar, la administración y mantenimiento de una base de datos consolidada de datos de autenticación es más fácil que múltiples bases de datos más pequeñas. Finalmente, la localización de la base de datos de perfiles de usuario externamente a la red local puede permitir a un ISP o tercer proveedor mantener la confidencialidad de la información almacenada dentro de la base de datos y mantener y controlar la base de datos en cualquier manera que el tercer proveedor desee.

El perfil de origen incluye uno o más nombres, palabras clave, direcciones, etiquetas VLAN, direcciones MAC y otra información pertinente para identificar y, si así se desea, facturar, un origen. Tras un intento del origen para acceder a una red por medio de un dispositivo de pasarela **12**, el servidor de AAA **30** intenta autenticar el origen mediante la comparación de los perfiles de origen almacenados en la base de datos de perfiles de origen con los atributos recibidos desde el dispositivo de pasarela **12** u origen para determinar la identidad del origen. Como un ejemplo ilustrativo, cuando un usuario intenta acceder a la red mediante la introducción de un ID de usuario y palabra clave, el ID de usuario y la palabra clave se comparan contra todos los ID y palabras claves almacenados en la base de datos de perfiles de origen para determinar la identidad del usuario. Como tal, la base de datos de perfiles de usuario generalmente comprende una base de datos o medio de almacenamiento de datos en comunicación con los medios de procesamiento situados dentro del servidor de AAA **30** o dispositivo de pasarela **12**, en donde la base de datos de perfiles de usuario y el procesador trabajan conjuntamente para comparar los atributos recibidos con la información de perfiles de origen almacenada, como es bien conocido en la técnica.

La base de datos de perfiles de origen puede comprender un hardware de almacenamiento programable o medios similares situados en un ordenador personal convencional, ordenador central u otro dispositivo de almacenamiento adecuado conocido en la técnica. Adicionalmente, los medios para la comparación de los datos recibidos con los datos dentro de la base de datos pueden comprender cualquier software, tal como un programa de software ejecutable, que pueda comparar los datos. Por ejemplo, el servidor de AAA **30** puede almacenar perfiles de origen en un disco duro de un ordenador personal y los medios para la comparación de los datos del origen recibidos con los perfiles de orígenes residentes en el ordenador pueden incluir software de ordenador tal como Microsoft Excel (Microsoft Excel es una marca registrada de Microsoft Corporation, Redmond, Washington). De acuerdo con otra realización de la invención, el servidor de AAA **30** o base de datos de perfiles de origen puede comprender un servicio de usuario de marcación para autenticación remota (RADIUS) o una base de datos del protocolo ligero de acceso a directorios (LDAP), que son bien conocidos para los expertos en la técnica.

Si un origen falla en la correspondencia con un perfil de origen en el servidor de AAA **30** en el momento de la autenticación, no se permitirá al origen el acceso a la red. Cuando esto sucede, se puede solicitar a un usuario o usuario asociado con un origen no de usuario que introduzca una información de perfil de origen en el servidor de AAA **30** de modo que el servidor de AAA **30** pueda añadir el perfil del origen al servidor de AAA **30** y, más específicamente, a la base de datos de perfiles de origen. Por ejemplo, esto puede suceder la primera vez que un usuario intenta acceder al dispositivo de pasarela **12**. De acuerdo con otro aspecto de la invención, cuando no se puede identificar el origen, se puede dirigir al origen a una página de registro para recoger información adicional para identificar el origen. Por ejemplo, la información se puede introducir con la ayuda de una página web, un panel de control emergente o una interfaz de usuario, que se puede abrir cuando el origen se conecta inicialmente al dispositivo de pasarela **12**, como la efectuada por una capacidad de redireccionamiento de página inicial, descrita en el presente documento y en el U.S. - A - 6 6 36894.

De acuerdo con un aspecto de la invención, el servidor de AAA **30** puede identificar el origen en comunicación con el dispositivo de pasarela en una forma que es transparente para los usuarios del ordenador. Esto es, de acuerdo con un aspecto de la invención, no se requerirá a un usuario que introduzca información de identificación, reconfigure el ordenador de origen o cambie en otro modo los ajustes primarios de red del ordenador de origen. Adicionalmente, no se tendrá que añadir ningún software de configuración adicional al ordenador de origen. Después de que se recibe el paquete por el dispositivo de pasarela, los atributos identificados por el paquete de datos se pueden comparar con los datos contenidos en la base de datos de perfiles de origen. Por lo tanto, además de no requerir la reconfiguración del acceso a la red de los ordenadores, los servidores de AAA de la presente invención tienen la capacidad de autenticar los orígenes sin requerir etapas interactivas por parte del usuario del ordenador, tal como la introducción de un ID de usuario. Por ejemplo, el servidor de AAA **30** puede identificar automáticamente el origen en base a una dirección MAC, de modo que la autorización del origen se pueda determinar fácilmente. Por lo tanto, se apreciará que el servidor de AAA **30** puede determinar el usuario, ordenador o localización desde la que se solicita el acceso mediante la comparación de los atributos asociados con el paquete de datos recibidos (tal como en la

cabecera del paquete de datos) con los datos extraídos de la base de datos de perfiles de origen. Como se describirá a continuación, los derechos de acceso asociados con el origen se pueden almacenar también dentro de la base de datos de perfiles de origen de modo que el sistema y el método de la presente invención puedan autorizar dinámicamente el acceso a servicios o destinos particulares.

Una vez que el origen ha establecido la conexión con el servicio de red por medio del proceso de autenticación explicado anteriormente y se ha abierto un túnel para facilitar una línea de comunicación entre el ordenador de origen y una red, el dispositivo de pasarela se comunica con el servidor de AAA **30** para ensamblar la información de perfil de origen o datos específicos de origen. La información del perfil de origen que el dispositivo de pasarela ensambla puede incluir una dirección MAC, nombre o ID, ID de circuito, datos relacionados con el esquema de facturación, datos del nivel de servicio, datos del perfil de usuario, datos relacionados con el emplazamiento remoto y datos similares relacionados con el origen. Como tal, el servidor de AAA **30** puede transmitir al dispositivo de pasarela **12** cualquier información de requisitos en relación con los derechos de autorización del origen y uso de la red, como se explica a continuación en detalle.

Además de la autenticación de usuarios, el servidor de AAA **30** de la presente invención proporciona una función de autorización, en la que se determinan los derechos de acceso del origen. La presente invención permite la autorización dinámica a los orígenes, de modo que cada origen pueda tener diferente uso o derechos de acceso de la red respectivos. Después de la autenticación, el servidor de AAA **30** compara los atributos del origen con los derechos de acceso del origen asociados con el usuario, ordenador, localización o atributo(s). Los derechos de acceso se pueden almacenar dentro de la base de datos de perfiles de origen o dentro de una base de datos de abonado separada localizada internamente o externamente al dispositivo de pasarela **12**. Por lo tanto, se pueden utilizar bases de datos separadas, en las que se almacena información de identificación sobre orígenes para la autenticación y otra base de datos almacena los derechos de acceso para esos orígenes que se han autenticado. Sin embargo, debido a que los perfiles de todos los orígenes, identificados por el atributo o una combinación de atributos, se almacenan en una base de datos de perfiles de origen, puede ser ventajoso localizar la información en relación con los derechos de acceso en la base de datos de perfiles de origen, que ya contiene información en relación con cada origen autenticado, como se ha descrito anteriormente.

De acuerdo con un aspecto de la invención la base de datos de perfiles de origen almacena información que define los derechos de acceso de origen. Por ejemplo, una base de datos de perfiles de origen puede contener información que indique que un origen que tenga una dirección MAC particular ha comprado un acceso prepagado o que un ID de circuito dado tiene acceso libre o acceso ilimitado. Los huéspedes en una habitación con habitaciones particulares de un hotel, por ejemplo, suites y áticos de lujo, pueden recibir un acceso a Internet ilimitado y libre. Por lo tanto, los derechos de acceso se pueden estar disponibles supeditados a la localización del origen (por ejemplo habitación) o estatus de la localización (por ejemplo suite). En este caso, no se requiere una identificación adicional, dado que la localización desde la que el origen está solicitando acceso es conocida para el dispositivo de pasarela y está almacenada en la base de datos de perfiles de origen.

Además de almacenar información en relación con qué origen tiene autorizado el acceso, la base de datos de perfiles de origen puede incluir información de acceso especializada asociada con una origen particular, tal como el ancho de banda de acceso del origen o una página inicial a la que se debe dirigir al origen. Por ejemplo, un usuario que accede a la red desde un ático de lujo puede recibir una tasa de baudios de acceso mayor que alguien que accede a la red desde una habitación de hotel típica. Por ejemplo, donde un usuario está accediendo de modo transparente al dispositivo de pasarela desde una habitación de hotel, el administrador de la red del hotel puede introducir información de acceso del usuario en una base de datos de perfiles de origen basada en los derechos de acceso asociados con una habitación en el hotel. Esto se puede realizar también automáticamente por el dispositivo de pasarela o un sistema de gestión local, tal como un sistema propietario de gestión del hotel, cuando el usuario se registra en su habitación. Adicionalmente, el usuario puede establecer la información a ser contenida dentro de la base de datos de perfiles de origen tras su primer acceso al dispositivo de pasarela. Por ejemplo, se puede indicar a un nuevo usuario para que introduzca un número de tarjeta de crédito, información de contabilidad de un monedero electrónico, número de tarjeta de llamadas de prepago o información de facturación similar para tener acceso al sistema. Un perfil de origen puede incluir también datos históricos en relación con el acceso del origen a la red, incluyendo la cantidad de tiempo que el origen ha accedido a la red. Se puede establecer el acceso especializado o la información de contabilidad contenida dentro de la base de datos de perfiles de origen por el administrador del sistema o mediante el origen que ha comprado o establecido en otro modo el acceso a la red.

De acuerdo con un aspecto de la invención, la capacidad de autorización del servidor de AAA **30** se puede basar en el tipo de servicios a los que el origen está intentando acceder, tal como una dirección de destino, identificada por el dispositivo de pasarela **12** basado en los datos recibidos desde el ordenador de origen. El destino puede ser un puerto de destino, dirección de Internet, puerto TCP, red u otro similar. Más aún, la capacidad de autorización del servidor de AAA **30** se puede basar en el tipo de contenido o protocolo que se está transmitiendo. De acuerdo con el sistema y método de la presente invención, cada paquete se puede filtrar a través de un proceso de AAA selectivo, de modo que cualquiera o todos los orígenes pueden tener autorizado el acceso a un destino particular en base a los derechos de acceso asociados con los orígenes respectivos. Por lo tanto, de acuerdo con la presente invención, cada vez que el origen intenta acceder a un destino diferente, el origen se somete al AAA, de modo que se puede

impedir al origen el acceso desde un sitio particular que el servidor de AAA **30** considera inaccesible para el origen en base a la autorización del origen. Alternativamente, el método de AAA, de acuerdo con la presente invención, permite a algunos o a todos los orígenes conectarse directamente a un sitio específico, tal como a servidores de tarjetas de crédito o facturación para la recogida de información de facturación, que pueden recoger información de pago o facturación de modo que se pueda actualizar el perfil del origen y se pueda autorizar posteriormente el acceso del origen a las redes. De acuerdo con el sistema y método de la presente invención, una autorización del origen puede depender también de criterios objetivos, tal como una hora específica, de modo que la sesión se pueda terminar a una hora específica, después de que haya transcurrido un tiempo específico o de acuerdo con otra información dinámica determinada por el proveedor de la red. Adicionalmente, la autorización puede estar asociada con una combinación de atributos. Por ejemplo, un usuario puede tener autorizado el acceso a una red en la que el usuario ha introducido la identificación del usuario y ha accedido a la red desde una habitación particular. Tal requisito podría impedir a los usuarios no autorizados que también permanecen en una habitación particular que obtengan acceso a la red. Por lo tanto, el AAA se puede basar en el origen, destino y tipo de tráfico.

A modo de explicación adicional, se describirá un diagrama de flujo del funcionamiento del servidor de AAA **30** con respecto a la FIGURA 2, de acuerdo con un aspecto de la invención. Durante el funcionamiento, un ordenador de origen solicita (bloque **200**) acceso a la red, destino, servicio u otro similar. Tras la recepción de un paquete transmitido al servidor de AAA **30**, el servidor de AAA **30** examina el paquete para determinar la identidad del origen (bloque **210**). Los atributos transmitidos por medio del paquete se almacenan temporalmente en la base de datos de perfiles de origen de modo que los datos se puedan examinar para su uso en la determinación de los derechos de autorización del origen. Los atributos contenidos en el paquete pueden incluir información de la red, dirección IP del origen, puerto de origen, información de la capa de enlace, dirección MAC del origen, etiqueta VLAN, ID del circuito, dirección IP del destino, puerto de destino, tipo de protocolo, tipo de paquete y otros similares. Después de que esta información se haya identificado y almacenado, se compara el acceso solicitado desde un origen contra la autorización de ese origen (bloque **230**).

Una vez que el perfil de origen se ha determinado mediante el acceso a los derechos de autorización almacenados en la base de datos de perfiles de origen, pueden resultar tres acciones posibles. Específicamente, una vez que los derechos de autorización del origen se han recuperado, el servidor de AAA **30** puede determinar que un origen tiene acceso **222**, está pendiente o en progreso **224** o no tiene acceso **226**. En primer lugar, se considera que el origen es válido (es decir tiene acceso) en donde la base de datos de perfiles de origen así lo establece. Si se determina que un origen es válido, se puede permitir que prosiga el tráfico del origen desde el dispositivo de pasarela a las redes o servicios en línea que el usuario asociado con el origen desea acceder (bloque **230**). Alternativamente, se puede redirigir al origen a una página de un portal, como se describe en la Aplicación de Redirección, previamente a que se le permita el acceso a la red solicitada. Por ejemplo, se puede dirigir automáticamente a un usuario a la dirección de destino introducida por el usuario, tal como una dirección de Internet, por ejemplo, en donde un usuario tiene un acceso libre asociado con la habitación de hotel del usuario. Alternativamente, esto puede suceder en donde el usuario ha comprado ya el acceso y el usuario no ha consumido el tiempo de acceso disponible. Adicionalmente, se puede iniciar un mensaje de contabilidad **230** para registrar la cantidad de tiempo que el usuario está utilizando el dispositivo de pasarela de modo que se puede facturar al usuario o localización por el acceso.

Si sucede el segundo escenario, en el que se considera el origen pendiente **224** o en progreso, el origen puede realizar las etapas para llegar a estar autenticado (bloque **240**) de modo que se registre la información del origen en la base de datos de perfiles de origen. Por ejemplo, un usuario puede haber entrado en un acuerdo de compra, que requiere al usuario introducir un número de tarjeta de crédito. Si el usuario necesita comprar el acceso o si el sistema necesita información adicional acerca del usuario, el usuario puede ser redirigido desde la página del portal a través de la Redirección de Página Inicial (HPR) y la Traducción de Direcciones en Pila (SAT) a una localización, tal como una página de registro, establecida para validar nuevos usuarios. Las SAT y HPR pueden intervenir para dirigir al usuario a un servidor web (externo o interno) en la que el usuario haya de registrarse e identificarse a sí mismo. Este proceso se describe en detalle en la Aplicación de Redirección. Después de la introducción de cualquier información necesaria y suficiente, se permite entonces el acceso al usuario a una dirección de destino (bloques **230**, **250**). Si la información proporcionada es insuficiente el usuario no tendrá autorizado el acceso (bloque **260**). Finalmente, puede suceder un tercer escenario en el que se considera que un origen no tiene acceso **226** de modo que el usuario no tiene permitido el acceso a un destino a través de la red (bloque **260**).

Con referencia ahora a la función de contabilidad de los sistemas y métodos de la presente invención, tras la autorización de un acceso a la red del origen, el servidor de AAA **30** puede registrar un inicio de contabilidad para identificar que el origen está accediendo a la red. Similarmente, cuando el origen sale o termina la sesión de red, se puede registrar una parada de contabilidad por el servidor de AAA **30**. El inicio o parada de la contabilidad se puede identificar por el dispositivo de pasarela **12** o por el servidor de AAA **30** tras la autenticación del origen o la autorización de acceso a un destino deseado. Adicionalmente, el inicio y parada de la contabilidad se pueden registrar en el perfil del origen o se pueden almacenar en una base de datos separada del servidor de AAA **30** y localizada externamente a la red. Típicamente, los inicios y paradas de la contabilidad incluyen marcas de tiempo que indican la cantidad de tiempo que un origen ha estado accediendo a la red. Usando estos datos, se pueden contabilizar los tiempos entre el inicio de la contabilidad y la parada de la contabilidad de modo que se pueda calcular el tiempo de conexión total del origen. Tal información es valiosa cuando se factura al origen por

incrementos de tiempo, tales como una hora. Un paquete de facturación, como es bien conocido en la técnica, podría cuadrar entonces el tiempo total de acceso a la red del usuario a través del periodo fijado, tal como cada mes, de modo que se pueda crear una factura para el origen. Debido a que las redes y los ISP pueden facturar a menudo una tasa fija para una duración de tipo específica (es decir precios de tarifas planas), tal como una vez al mes, independientemente de cuanto tiempo se haya utilizado del acceso a la red, puede que no se requiera la contabilidad de los inicios y paradas con finalidades de facturación. Independientemente, se puedan registrar en general la contabilidad de inicios y paradas por el proveedor de la red o ISP para estadísticas de uso.

Un ISP o proveedor de acceso similar podría beneficiarse adicionalmente de ser capaz de seguir el uso del abonado de la ISP para establecer facturas, informes históricos y otra información relevante. Preferiblemente, el servidor de AAA **30** está en comunicación con uno o más procesadores para la determinación de cualquier tarifa que se pueda facturar al origen, o debidas por el origen, por accesos o servicios de la red. El servidor de AAA **30** recupera los datos de contabilidad históricos en tiempo real o después de que haya transcurrido un intervalo específico de tiempo. Preferiblemente, el servidor de AAA **30** retiene tales datos en un formato fácilmente accesible y manipulable de modo que el proveedor de acceso (por ejemplo, un ISP) pueda producir informes representativos de cualquier tipo deseado de datos históricos. Por ejemplo, para proyectar el uso futuro del proveedor de acceso, el servidor de AAA **30** produce informes que contabilizan el número de usuarios que acceden a la Internet en ciertos periodos de tiempo y desde localizaciones específicas. Más aún, cuando el proveedor de acceso proporciona acceso alternativo a los usuarios, tal como la carga para conexiones más rápidas (por ejemplo una tasa de baudios más alta) con tarifas adicionales, el proveedor de accesos puede desear analizar los datos históricos usando el servidor de AAA **30** para satisfacer mejor las demandas futuras de clientes. Tales datos se pueden relacionar con sesiones de red actualmente en marcha, la duración de estas sesiones, el ancho de banda actualmente usado, el número de bytes que se han transferido y cualquier otro tipo de información pertinente. El servidor de AAA **30** puede ser implementado usando programas bien conocidos, tal como Eclipse Internet Billing System, Kenan Broadband Internet Billing Software (fabricado por Lucent Technologies) o TRU RADIUS Accountant.

Se apreciará que el servidor de AAA **30** puede contabilizar dinámicamente el acceso del origen a una red en la misma manera en la que se puede personalizar el acceso en una forma de origen a origen. Esto es, el servidor de AAA **30** puede mantener registros de contabilidad que varían dependiendo de la identidad de un origen, localización del origen, destino solicitado por el origen u otros similares. Como los derechos de acceso y autorización, esta información se puede mantener en la base de datos de perfiles de origen o una base de datos de contabilidad similar. Por ejemplo, el servidor de AAA **30** puede determinar que un origen particular sólo sea facturado por sitios particulares de acceso y registra solamente un sitio de contabilidad cuando se accede a esos sitios particulares. Por lo tanto, el servidor de AAA **30** identificará la información de contabilidad almacenada en el perfil del origen del abonado para determinar el inicio de la contabilidad, detención de la contabilidad, tasas de facturación y otros similares.

A los expertos en la materia se les ocurrirán muchas modificaciones y otras realizaciones de la invención a las que pertenece esta invención que tiene el beneficio de las enseñanzas presentadas en las descripciones precedentes y los dibujos asociados. Por lo tanto, se ha de comprender que la invención no está limitada a las realizaciones específicas descritas y que se pretende que las modificaciones y otras realizaciones se incluyan dentro del alcance de las reivindicaciones adjuntas. Aunque se emplean en el presente documento términos específicos, se usan en un sentido genérico y descriptivo solamente y no con finalidades de limitación.

REIVINDICACIONES

1. Un método para el control de accesos a una red, que comprende:

la recepción en un dispositivo de pasarela (12) de una solicitud desde un ordenador de origen (14) para el acceso a una red de ordenadores (20);
permitir, por medio del dispositivo de pasarela, al ordenador de origen (14) acceder a la red de ordenadores (20);
recepción, en el dispositivo de pasarela (12), de un paquete transmitido desde un ordenador de origen (14);
caracterizado porque el método comprende además:
la determinación de una localización del ordenador de origen (14) mediante la comparación de los atributos asociados con el paquete con los datos extraídos desde una base de datos de perfiles de origen y
la determinación de los derechos de acceso del ordenador de origen (14) en base al menos a la localización determinada del ordenador de origen, en la que los derechos de acceso definen los derechos del ordenador de origen (14) para acceder a un destino de red solicitado en la red de ordenadores (20), siendo determinados los derechos de acceso sin requerir etapas interactivas por parte de un usuario del ordenador.

2. El método de la reivindicación 1, en el que la localización es una habitación en un hotel.

3. El método de la reivindicación 1, en el que la determinación de una localización del ordenador de origen (14) comprende el acceso a un servicio de usuario de marcación para autenticación remota (RADIUS).

4. El método de la reivindicación 1, en el que la determinación de una localización del ordenador de origen (14) comprende el acceso a una base de datos del protocolo ligero de acceso a directorios (LDAP).

5. El método de la reivindicación 1, que comprende además la actualización de la base de datos de perfiles de origen cuando un nuevo origen accede a la red de ordenadores (20).

6. El método de la reivindicación 1, que comprende además el mantenimiento en la base de datos de perfiles de origen de un registro histórico del acceso del ordenador de origen (14) a la red de ordenadores (20).

7. El método de la reivindicación 1, que comprende además la redirección del ordenador de origen a una página de portal previamente a que se permita al ordenador de origen el acceso a la red solicitada.

8. Un sistema para el control del acceso a una red, que comprende:

medios para la recepción en un dispositivo de pasarela (12) de una solicitud desde un ordenador de origen (14) para el acceso a una red de ordenadores (20);
medios para permitir, por medio del dispositivo de pasarela, al ordenador de origen (14) acceder a la red de ordenadores (20);
medios para la recepción, en el dispositivo de pasarela (12), de un paquete transmitido desde un ordenador de origen (14);
caracterizado porque el sistema comprende además:
medios para la determinación de una localización del ordenador de origen (14) mediante la comparación de los atributos asociados con el paquete con los datos extraídos desde una base de datos de perfiles de origen y
medios para la determinación de los derechos de acceso del ordenador de origen (14) en base al menos a la localización determinada del ordenador de origen (14), en la que los derechos de acceso definen los derechos del ordenador de origen (14) para acceder a un destino de red solicitado en la red de ordenadores (20), siendo determinados los derechos de acceso sin requerir etapas interactivas por parte de un usuario del ordenador.

9. El sistema de la reivindicación 8, en el que la localización es una habitación en un hotel.

10. El sistema de la reivindicación 8, en el que los medios para determinación de una localización del ordenador de origen (14) comprenden medios para el acceso a un servicio de usuario de marcación para autenticación remota (RADIUS).

11. El sistema de la reivindicación 8, en el que los medios para determinación de una localización del ordenador de origen (14) comprenden medios para el acceso a una base de datos del protocolo ligero de acceso a directorios (LDAP).

12. El sistema de la reivindicación 8, que comprende además medios para la actualización de la base de datos de perfiles de origen cuando un nuevo origen accede a la red de ordenadores (20).

13. El sistema de la reivindicación 8, que comprende además medios para el mantenimiento en la base de datos de perfiles de origen de un registro histórico del acceso del ordenador de origen (14) a la red de ordenadores (20).

14. El sistema de la reivindicación 8, que comprende además medios para la redirección del ordenador de origen a una página de portal previamente a que se permita al ordenador de origen el acceso a la red solicitada.

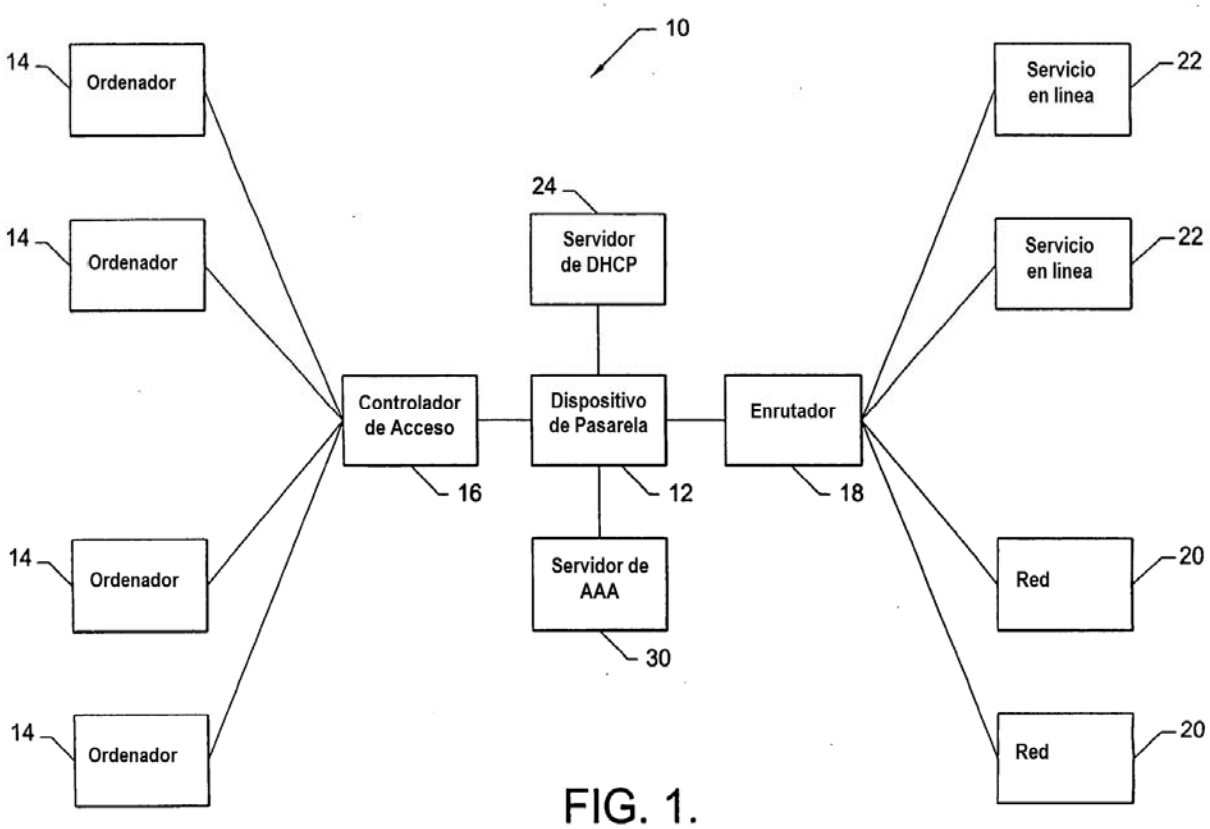
10
14
Ordenador
14
Ordenador
14
Ordenador
14
Ordenador
24
Servidor de DHCP
Controlador de Acceso
16
Dispositivo de Pasarela
12
Servidor de AAA
30
Enrutador
18
Servicio en linea
22
Servicio en linea
22
Red
20
Red
20

FIG. 1.

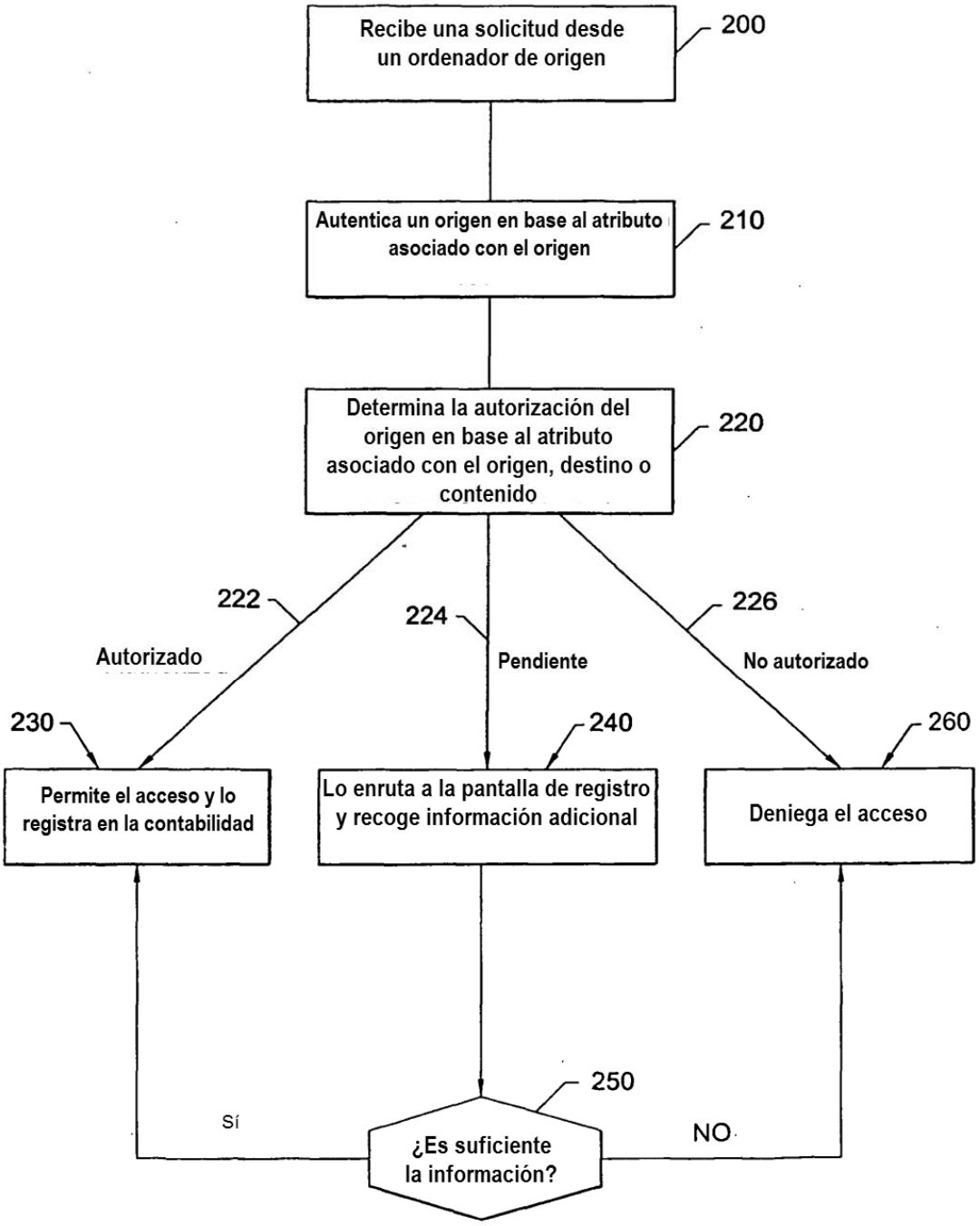
Recibe una solicitud desde un ordenador de origen
200
Autentica un origen en base al atributo asociado con el origen
210
Determina la autorización del origen en base al atributo asociado con el origen, destino o contenido
220
222
Autorizado
224
Pendiente
226
No autorizado
230
Permite el acceso y lo registra en la contabilidad
240
Lo enruta a la pantalla de registro y recoge información adicional
260
Deniega el acceso
250
Sí
NO
¿Es suficiente la información?

FIG. 2.