(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 303 098**

(51) Int. Cl.:
G06F 1/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04783772 .9**
(86) Fecha de presentación : **10.09.2004**
(87) Número de publicación de la solicitud: **1671204**
(87) Fecha de publicación de la solicitud: **21.06.2006**

(54) Título: **Métodos y aparatos para acceso seguro remoto a escritorios de manera ajustable a escala.**

(30) Prioridad: **10.10.2003 US 683544**

(45) Fecha de publicación de la mención BOPI:
01.08.2008

(45) Fecha de la publicación del folleto de la patente:
01.08.2008

(73) Titular/es: **Citrix Systems, Inc.**
851 W. Cypress Creek Road
Fort Lauderdale, Florida 33309, US

(72) Inventor/es: **Panasyuk, Anatoliy;**
Sirjani, Abolfazl;
Walters, Ben;
Burr, Michael y
Earl, Min-Chih, Lu

(74) Agente: **González Palmero, Fe**

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).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Métodos y aparatos para acceso seguro remoto a escritorios de manera ajustable a escala.

Solicitudes relacionadas

Esta solicitud reivindica el beneficio de la solicitud de patente estadounidense n° de serie 10/683.544 presentada el 10 de octubre de 2003.

Campo técnico

La presente invención se refiere en general a las conexiones de redes informáticas, y más específicamente a la protección de un método de concesión de acceso remoto a escritorios de ordenador.

Antecedentes

Numerosos usuarios de ordenadores en empresas dependen habitualmente de las aplicaciones y los archivos almacenados en el disco duro de sus ordenadores personales de oficina para sus necesidades informáticas. Sin embargo, la mayoría de estos ordenadores carecen de portabilidad, o si son portátiles, no pueden proporcionar un acceso adecuado a los recursos disponibles para sus ordenadores personales de oficina. La publicación de patente internacional n° WO02/21414 da a conocer un sistema de registro para conceder acceso remoto a un recurso conectado en red.

Para proporcionar a los usuarios de ordenadores acceso a los recursos de sus ordenadores personales de oficina desde dispositivos remotos, tales como ordenadores o portátiles desde sus casas, los programadores han desarrollado diversas tecnologías para acceder de manera remota a los recursos de un ordenador, denominado ordenador central (*host*), desde un segundo dispositivo remoto, denominado cliente. Utilizando tales tecnologías, una pantalla del cliente del usuario remoto muestra lo que puede verse en la pantalla del ordenador central si el usuario estuviese visualizando físicamente la pantalla del ordenador central. Además, el software de acceso remoto permite a los usuarios remotos interactuar con el ordenador central con los medios de entrada del cliente, tales como un teclado o un ratón, como si el usuario estuviese utilizando el dispositivo de entrada del ordenador central. Cualquier cálculo que se inicie por los medios de entrada del usuario se lleva a cabo en el ordenador central y los resultados se visualizan en la pantalla del cliente como si ésta fuese la pantalla del ordenador central.

Aunque estas tecnologías han tenido éxito y han sido útiles a escala limitada, pueden presentar cargas administrativas en sistemas de empresa de mayor escala. Los sistemas de empresa grandes requieren un acceso seguro regulado para gran número de usuarios a gran número de recursos conectados en red. Algunos sistemas permiten especificar reglas de acceso amplias que se aplican a grupos de usuarios o recursos, pero que normalmente no imponen limitaciones de acceso a un individuo o recurso individual. Algunos sistemas tienen métodos basados en permisos individuales que normalmente requieren un administrador de sistema para especificar las limitaciones de acceso para todos y cada uno de los usuarios y los recursos. Los primeros métodos proporcionan a menudo insuficiente seguridad puesto que las reglas de acceso tienden a ser demasiado amplias, y el segundo método generalmente requiere un alto nivel poco habitual de sobrecarga administrativa en grandes sistemas.

Sumario de la invención

Un objeto de la invención es proporcionar métodos y sistemas seguros ajustables a escala y fácilmente administrables para proporcionar acceso remoto a recursos conectados en red combinando aspectos de las medidas de limitación de acceso físico con medidas tradicionales de limitación de acceso informático.

En un aspecto, la invención se refiere a un método de administración de una red informática. El método incluye proporcionar un sistema de administración de registro para especificar reglas de registro, y un sistema de registro configurado para comunicarse con el sistema de administración de registro para permitir registrar un primer recurso conectado en red si lo permiten las reglas de registro especificadas. El método también incluye proporcionar un sistema de acceso remoto para conceder a un usuario acceso remoto al primer recurso conectado en red si el usuario registró con éxito el primer recurso conectado en red. En una realización, el recurso conectado en red es un ordenador.

En una realización, el sistema de acceso remoto está previsto para instalarse en el primer recurso conectado en red. En otra realización, el sistema de acceso remoto está previsto para instalarse en un recurso de red compartido. En esta realización, el sistema de acceso remoto concede acceso remoto al primer recurso conectado en red y a un segundo recurso conectado en red con sujeción a las reglas de registro especificadas y al registro del usuario de los recursos conectados en red primero y segundo. En otra realización, el sistema de acceso remoto deniega el acceso remoto a un usuario que no haya registrado el primer recurso conectado en red. En una realización adicional, el acceso remoto incluye acceso remoto al escritorio del primer recurso conectado en red.

En otra realización, el sistema de registro desautoriza el registro del primer recurso conectado en red desde un puesto de mando remoto. En otra realización, el sistema de registro requiere el registro del primer recurso conectado en red desde un puesto de mando que esté físicamente interconectado al primer recurso conectado en red. En otra realización más, el sistema de registro es una aplicación de red. En una realización, el método incluye además pro-

porcionar un sistema localizador para determinar la ubicación de un usuario que intenta registrar el primer recurso conectado en red. En una realización adicional, el registro del primer recurso conectado en red está sujeto además a la ubicación determinada.

En otro aspecto, la invención se refiere a un sistema informático que incluye un sistema de administración de registros para especificar reglas de registro. El sistema informático también incluye un primer recurso conectado en red que está configurado para comunicarse con el sistema de administración de registros y un dispositivo remoto configurado para comunicarse con el primer recurso conectado en red a través de un canal de comunicaciones, tal como una red. Además, el sistema informático incluye además un sistema de registro para registrar el primer recurso conectado en red si lo permiten las reglas de registro especificadas y un sistema de acceso remoto para conceder a un usuario del dispositivo remoto acceso remoto al primer recurso conectado en red si el primer recurso conectado en red se registró con éxito. En una realización, el sistema informático también incluye una base de datos de registros que almacena una lista de recursos conectados en red que un usuario ha registrado.

En otro aspecto más, la invención se refiere a un método de administración de red que incluye especificar una regla de registro y registrar un primer recurso conectado en red si lo permite la regla de registro especificada. El método también incluye conceder a un usuario acceso remoto al primer recurso conectado en red desde un dispositivo remoto si el usuario ha registrado previamente con éxito el primer recurso conectado en red, y de lo contrario denegar a un usuario el acceso al primer recurso conectado en red desde el dispositivo remoto. En una realización, especificar una regla de registro incluye definir una pluralidad de grupos de usuarios, definir una pluralidad de grupos de recursos conectados en red, y especificar un grupo de recursos conectados en red que está permitido que un grupo de usuarios registre.

Breve descripción de los dibujos

La explicación anterior se entenderá más fácilmente a partir de la siguiente descripción detallada de la invención, tomada junto con los dibujos adjuntos:

La figura 1 es una representación esquemática de acceso remoto a escritorios según una realización ilustrativa de la invención.

La figura 2 es un diagrama esquemático que representa una red informática según una realización ilustrativa de la invención.

La figura 3A es un diagrama de un conjunto de agrupaciones de recursos de red informática según una realización ilustrativa de la invención.

La figura 3B es un diagrama de un conjunto de agrupaciones de usuarios de red informática según una realización ilustrativa de la invención.

La figura 4 es una tabla que representa reglas de registro de ejemplo según una realización ilustrativa de la invención.

La figura 5 es un diagrama de flujo de un método de registro de un recurso conectado en red según una realización ilustrativa de la invención.

La figura 6 es una base de datos de registros que representa un conjunto de ejemplo de registros según una realización ilustrativa de la invención; y

la figura 7 es un diagrama de flujo de un método de concesión de acceso remoto a un ordenador según una realización ilustrativa de la invención.

Descripción detallada

En el mundo físico, los recursos se protegen implementando limitaciones de acceso físico. Se cierran armarios de archivos con cerrojo, se precintan cámaras, y se cierran las puertas de las oficinas. En cualquiera de estos casos, tener la llave únicamente no es suficiente para acceder a los recursos dentro del armario, cámara u oficina. Debe tenerse la llave y al mismo tiempo se ha de estar físicamente presente en el armario, cámara u oficina. En un entorno informático conectado en red tradicional, sin embargo las mejoras en las restricciones de acceso se han centrado en crear bloqueos y claves más complejos (por ejemplo sistemas de contraseña/PIN de usuario, verificación de identidad biométrica, verificación de voz, etc.) y han ignorado en gran medida los beneficios de seguridad que pueden proporcionar las limitaciones de acceso físico. Es decir, para muchos sistemas informáticos, si un usuario tiene la "clave" apropiada, el usuario puede acceder a un recurso conectado en red sin necesidad de haber estado nunca presente físicamente cerca del recurso. Un objeto de la presente invención es proporcionar métodos y sistemas seguros ajustables a escala y fácilmente administrables para proporcionar acceso remoto a recursos conectados en red combinando aspectos de las medidas de limitación de acceso físico con medidas tradicionales de limitación de acceso informático. Tal combinación combina las ventajas con poca sobrecarga de las limitaciones de acceso basadas en reglas con las ventajas de seguridad individualizadas de limitaciones basadas en permisos individuales, sin incurrir en los costes administrativos adicionales asociados.

En referencia a la figura 1, un primer recurso 100 conectado en red está ubicado físicamente en una ubicación particular, por ejemplo en una oficina. Los recursos conectados en red pueden incluir, por ejemplo, ordenadores de sobremesa, estaciones de trabajo, ordenadores portátiles, ordenadores de mano, teléfonos móviles, asistentes digitales personales, dispositivos informáticos que pueden conectarse en red, impresoras, dispositivos de almacenamiento, periféricos, etc. y cualquier dato, aplicación o capacidad disponible en o desde los recursos. El primer recurso 100 conectado en red puede tener acceso a otros recursos 104 conectados en red a través de una red 106. Un dispositivo 102 remoto se comunica con el primer recurso 100 conectado en red a través de un enlace 108 de comunicación, tal como una red informática. El dispositivo 102 remoto puede ser un ordenador tal como una estación de trabajo, ordenador de sobremesa, ordenador portátil, ordenador de mano, o cualquier otra forma de dispositivo informático o de telecomunicaciones que pueda comunicarse y que tenga suficiente potencia de procesamiento y capacidad de memoria para realizar las operaciones descritas en la presente memoria (por ejemplo un teléfono móvil o asistente digital personal). El enlace 108 de comunicación puede implementarse con cualquiera de una variedad de tecnologías adecuadas, por ejemplo sobre líneas de telefonía estándar, enlaces LAN o WAN (utilizando, por ejemplo, los protocolos 502.11, T1, T3, 56 kb o X.25), conexiones de banda ancha (utilizando por ejemplo, los protocolos RSDI, *Frame Relay*, o ATM), y conexiones inalámbricas o alguna combinación de cualquiera o todas las anteriores.

En una realización ilustrativa de la invención, el primer recurso 100 conectado en red es un ordenador que hace de ordenador central, y el dispositivo 102 remoto hace de cliente. Se concede a un usuario del dispositivo 102 remoto acceso al primer recurso 100 conectado en red de modo que el usuario tiene acceso al escritorio del primer recurso 100 conectado en red. Es decir, en lugar de sólo tener acceso a los servicios del primer recurso 100 conectado en red, la pantalla del dispositivo 102 remoto muestra lo que un usuario podría ver en el monitor del puesto de mando del primer recurso 100 conectado en red. Asimismo, el usuario puede proporcionar entradas (por ejemplo, entradas de teclado y ratón) al primer recurso 100 conectado en red desde el dispositivo 102 remoto que se interpretan por el primer recurso 100 conectado en red como si tales entradas se hubiesen realizado desde un puesto de mando físicamente interconectado al primer recurso conectado en red.

En una realización de este tipo, el acceso remoto se lleva a cabo utilizando Metaframe Presentation Server®, fabricado por Citrix Systems, Inc. de Ft. Lauderdale, Florida, en el primer recurso 100 conectado en red junto con el uso de clientes con Independent Computing Architecture® (ICA) de Citrix en el dispositivo 102 remoto.

En una realización alternativa, el acceso remoto se proporciona mediante software de escritorio remoto. El escritorio remoto es una propiedad incluida en el sistema operativo Windows XP® Professional, fabricado por Microsoft Corporation de Redmond, Washington, que permite a un ordenador central, tal como el primer recurso 100 conectado en red, proporcionar acceso al escritorio de ese ordenador central a clientes, tal como el dispositivo 102 remoto, que tengan instalado el software de cliente de escritorio remoto. El software de cliente de escritorio remoto está incluido en el sistema operativo Windows XP® y está disponible para ordenadores que ejecuten los sistemas operativos Windows 950, Windows 98®, Windows Me®, Windows NT® 4.0 o Windows 2000®. El escritorio remoto utiliza el protocolo de usuario remoto, también conocido como RDP, para la comunicación entre el ordenador central y el cliente.

Ha de entenderse que las realizaciones de la invención pueden implementarse utilizando otro software y protocolos de comunicaciones adecuados. Por ejemplo, el ordenador central podría operar un servidor web al que podría conectarse un cliente para utilizar protocolos de Internet normalizados tales como HTTP. Otros sistemas para acceso remoto a escritorios incluyen pcAnywhere®, fabricado por Symantec Corporation de Cupertino, California.

Además, o en lugar de conceder acceso remoto a escritorios, otras realizaciones de la invención proporcionan acceso remoto más limitado a recursos conectados en red. Por ejemplo, en una realización, la invención proporciona acceso remoto a archivos almacenados en un ordenador. En otra realización, la invención proporciona acceso remoto a aplicaciones almacenadas en un recurso, pero no a cualquier archivo de datos almacenado en el mismo. En otra realización, la invención proporciona acceso remoto a una impresora, pantalla u otro dispositivo de salida.

En otra realización, la invención proporciona sólo acceso remoto limitado a escritorios. Por ejemplo, un usuario puede ser capaz de acceder a archivos físicamente almacenados en el ordenador a cuyo escritorio está accediendo, pero el acceso a otros recursos conectados en red, tales como servidor de archivos, a través del escritorio, está limitado. En referencia a la figura 2, un sistema 200 informático ilustrativo incluye un número de recursos conectados en red, mostrados en la figura como ordenadores a modo de ejemplo TermA 202, TermB 204, TermC 206, CAD A 208, CAD B 210, CAD C 212, AdminA 214, AdminB 216, AdminC 218, y que se denominan conjuntamente como los "ordenadores". Los ordenadores 202, 204, 206, 208, 210, 212, 214, 216 y 218 pueden estar geográficamente próximos o dispersados. Por ejemplo, algunos o todos los ordenadores en el sistema 200 informático pueden estar ubicados en una ubicación diferente de los demás ordenadores en el sistema informático. Por ejemplo, Term 202 podría estar alejado de TermB 204 y de los demás ordenadores 206, 208, 210, 212, 214, 216 y 218.

Tal como se representa en la figura, sin embargo, los ordenadores TermA 202, TermB 204, CADC 212 y AdminC 218 están ubicados en un primer edificio 220, y los ordenadores TermC 206, CAD A 208, CAD B 210, AdminA 214 y AdminB 216 están ubicados en un segundo edificio 222. Los ordenadores 202, 204, 206, 208, 210, 212, 214, 216 y 218 están conectados entre sí a través de una red 224 de tipo empresarial. El sistema 200 informático también proporciona acceso para que un dispositivo 201 remoto se conecte a la red 224 para acceder a uno de los ordenadores 202, 204, 206, 208, 210, 212, 214, 216 y 218 y a los recursos conectados en red. El dispositivo 201 remoto puede formar parte

de o ser externo al sistema 200 informático, y se conecta al sistema 200 informático a través de un enlace 203 de comunicaciones.

El sistema 200 informático incluye un sistema 226 de administración de acceso. En general, el sistema 226 de administración de acceso es una agrupación lógica de varios sistemas relacionados que se utilizan para determinar y regir las capacidades de usuarios para acceder y usar recursos conectados en red. Cada sistema puede estar ubicado y/o ejecutarse en un ordenador en el primer o el segundo edificio 220 y 222, en un ordenador ubicado en un tercer edificio (no mostrado), en cualquiera de los ordenadores 202, 204, 206, 208, 210, 212, 214, 216 y 218 anteriormente descritos, o distribuido a través de cualquiera o todos los ordenadores anteriores.

El sistema 226 de administración de acceso incluye un sistema 228 de administración de registro para especificar reglas de registro. En una realización el sistema 228 de administración de registro es un módulo o programa de software disponible para los administradores de sistemas, para especificar tales reglas, si bien son posibles otras implementaciones. Las reglas de registro especifican qué usuarios o grupos de usuarios tienen permiso para registrar recursos conectado en red individuales o grupos de los mismos, siendo el registro el acto de obtener autorización para un acceso posterior a un recurso conectado en red desde un dispositivo 102 remoto. Un administrador de sistema especifica una regla de registro definiendo grupos de uno o más usuarios, definiendo grupos de recursos conectados en red, y entonces especificando qué grupo o grupos de usuarios tienen permiso para registrar qué grupo o grupos de recursos conectado en red.

Para facilitar la definición de grupos y especificar reglas, en una realización el sistema 228 de administración de registro proporciona una interfaz de usuario gráfica que permite al administrador de sistema arrastrar y soltar usuarios y recursos en grupos y arrastrar y soltar grupos en reglas de registro. En otra realización, la interfaz de usuario gráfica proporciona una interfaz de señalar y hacer clic que permite a un administrador de sistema formar grupos y reglas a partir de listas de usuarios, recursos y grupos. En otras realizaciones más, un administrador de sistema forma un grupo tecleando identificadores de usuario o recurso en una lista (por ejemplo nombres, nombres de usuario, direcciones de correo electrónico, números de empleado, direcciones IP, nombres de recursos, etc.). Cualquiera que sea la interfaz empleada, la interfaz también permite eliminar usuarios o recursos de los grupos o cambiarlos a otros grupos y alterar las reglas.

En una realización adicional, el administrador puede utilizar agrupaciones previamente definidas. Grandes organizaciones tienen a menudo agrupaciones de usuarios y recursos definidos para otros fines informáticos. Tales grupos se definen por ejemplo utilizando diversos dominios, directorio activo, o directorios de protocolo de acceso a directorios de poco peso (LDAP). Los grupos de recursos pueden definirse también proporcionando intervalos de direcciones IP.

En una realización, las reglas de registro son distintas de otras reglas de acceso. Por ejemplo, un administrador de sistema puede especificar reglas de registro que permitan a un grupo de usuarios registrar un grupo de recursos conectados en red para acceso remoto que los usuarios no estarían autorizados de lo contrario a usar directamente. Asimismo, un grupo de usuarios que puede estar autorizado a acceder directamente a un grupo de recursos conectados en red puede no estar autorizado a registrar esos recursos conectados en red para acceso remoto si no se ha especificado dicha regla de registro. En una realización, el sistema de administración de registro almacena las reglas de registro en una base de datos de reglas de registro. En otra realización, el sistema 228 de administración de registro también incluye una base de datos de registro que identifica cada recurso conectado en red que ha registrado cada usuario.

El sistema 226 de administración de acceso incluye un sistema 230 de registro configurado para comunicarse con el sistema 228 de administración de registro para permitir registrar un primer recurso conectado en red si lo permiten las reglas de registro especificadas. En una realización, el sistema 230 de registro es una aplicación de red, en particular una aplicación JAVA® almacenada en un servidor central y descargada a un recurso conectado en red en respuesta a una solicitud del usuario para registrar un recurso conectado en red. La solicitud de registro puede iniciarse, por ejemplo, haciendo clic sobre un icono en el escritorio del recurso conectado en red, haciendo clic sobre un hyperlink de una página web, o solicitando el registro del ordenador desde un menú.

En realizaciones alternativas, el sistema 230 de registro opera en un servidor conectado en red y el usuario se comunica con el sistema 230 de registro a través de una interfaz de puerta común (CGI) a través de un navegador de Internet utilizando HTTP, HTML, XML u otro protocolo de red conocido. En todavía otra realización adicional, el sistema 230 de registro está instalado en un recurso conectado en red mediante transmisión del código de software que implanta el sistema 230 de registro sobre el recurso conectado en red desde un medio de almacenamiento electrónico (por ejemplo un disco flexible, un disco zip, CD-ROM, DVD-ROM, etc.).

El sistema 230 de registro proporciona una interfaz para que un usuario que solicita un registro se identifique a sí mismo y al recurso que el usuario solicita registrar. El sistema 230 de registro se comunica con el sistema 228 de administración de registro para determinar si un usuario tiene permiso de hecho para registrar ese recurso. En una realización, la comunicación incluye enviar un mensaje al sistema 228 de administración de registro que contiene la identificación del usuario que solicita el registro del recurso conectado en red y la identificación del recurso conectado en red que el usuario solicita registrar. La comunicación, en una realización, incluye transmitir una consulta de la base de datos, por ejemplo empleando lenguaje de consulta estructurado (SQL), al sistema 228 de administración de registro. En otra realización, la comunicación incluye que se ejecute una llamada de procedimiento remoto en el sistema 228 de administración de registro, cuyo resultado es un valor booleano que indica si el usuario tiene permiso

para registrar el recurso. En una realización adicional, la comunicación incluye transmitir una instrucción de lógica de negocio que debe interpretarse por el sistema 228 de administración de registro.

En otra realización más, el sistema 228 de administración de registro transmite una base de datos de reglas de registro actualizada al sistema 230 de registro. En esta realización, tras recibir la base de datos de reglas de registro actualizada, el sistema 230 de registro consulta la base de datos de reglas de registro (por ejemplo empleando SQL) para determinar si el usuario tiene permiso para registrar la base de datos. Las comunicaciones pueden tener lugar a través de una variedad de conexiones por cable (utilizando, por ejemplo protocolos TCP/IP, RDSI, Frame Relay, o ATM) y conexiones inalámbricas o alguna combinación de cualquiera o todas las anteriores.

En una realización, el sistema 230 de registro también es responsable de verificar la identidad del usuario. La verificación de la identidad del usuario puede realizarse, por ejemplo, recopilando combinaciones de contraseña/PIN de usuario, recopilando datos biométricos de usuario, recopilando una muestra de la voz del usuario, etc.

El sistema 226 de administración de acceso también incluye un sistema 232 de acceso remoto para conceder acceso remoto al primer recurso conectado en red si el usuario registró con éxito el primer recurso conectado en red. En una realización, el sistema 226 de administración de acceso controla el acceso general a la red (es decir, no a un recurso específico), además de controlar el acceso remoto a recursos conectados en red individuales o a grupos de los mismos. En una realización, el sistema 232 de acceso remoto es un módulo de software que opera en un servidor de red central. Si un usuario intenta acceder remotamente a un recurso conectado en red, el usuario primero se pone en contacto con el sistema 232 de acceso remoto en el servidor central. En otra realización, cada recurso conectado en red registrable tiene instalada una copia del sistema 232 de acceso remoto, o bien el recurso conectado en red puede descargar una copia del sistema 230 de registro desde un servidor al recibir una solicitud de acceso remoto.

En una realización, el sistema 232 de acceso remoto recibe la solicitud de acceso remoto, verifica la identidad del usuario que solicita el acceso y determina si ese usuario ha registrado el recurso conectado en red para el que el usuario está solicitando acceso remoto consultando una base de datos de registro mantenida por el sistema 228 de administración de registros. Si el usuario ha registrado el recurso conectado en red, el sistema 232 de acceso remoto concede permiso al usuario para acceder al recurso conectado en red y se inicia tal acceso.

En las realizaciones descritas anteriormente, los sistemas 226, 228, 230 y 232 se implementan como módulos o programas de software. Un experto en la técnica debería apreciar que algunas o todas las funcionalidades del sistema pueden por el contrario implementarse de formas distintas de las descritas, por ejemplo en hardware, tal como un circuito integrado específico de la aplicación (ASIC) y similares.

El funcionamiento de los sistemas del sistema 226 de administración de acceso puede entenderse adicionalmente con referencia a las figuras 3 a 7.

En referencia a las figuras 3A y 3B, para aliviar la carga sobre los administradores de sistemas, los administradores de sistemas pueden utilizar el sistema 226 de administración de acceso o uno de sus sistemas constituyentes para añadir usuarios y recursos en grupos que comparten características comunes, puesto que a medida que aumenta el número de recursos y usuarios de red de un sistema 200 informático, lleva cada vez más tiempo asignar individualmente derechos de acceso a cada usuario. En referencia a la figura 3A, un conjunto 300 ilustrativo de recursos de red del sistema 200 informático puede agruparse en estaciones 302 de trabajo que incluye TermA 202, TermB 204 y TermC 206; terminales 304 CAD que incluye CAD A 214, CAD B 216 y CAD C 218; y terminales de auxiliares administrativos AdminA 208, AdminB 210 y AdminC 212. En referencia a la figura 3B, un conjunto 307 ilustrativo de usuarios de ordenador pueden agruparse como sigue: Tara 314, Tom 316 y Ted 318 pueden agruparse como miembros del personal 208 de tecnología de la información (IT); Ellie 320, Erica 322 y Edward 324 pueden agruparse como ingenieros 310, y Alex 326, Amy 328 y Andrew 330 pueden agruparse como Auxiliares 312 administrativos.

En una realización, un administrador de sistemas puede especificar agrupaciones de usuarios y/o recursos utilizando el sistema 226 de administración de acceso. En una realización, el sistema 226 de administración de acceso proporciona una interfaz de usuario gráfica con la que un administrador de sistemas puede arrastrar y soltar, o señalar y hacer clic para añadir usuarios o recursos a grupos. En otra realización, el sistema 228 de administración de registro también proporciona funcionalidad de gestión de grupos a través de una interfaz similar. Los grupos creados con el fin de especificar reglas de registro pueden ser diferentes de los grupos creados para especificar otras reglas de acceso.

Una vez definidos los grupos de usuarios y recursos, pueden especificarse reglas para limitar la capacidad de un grupo 308, 310 ó 312 de usuarios para acceder tanto directa como remotamente y utilizar un grupo 302, 304 y 306 de recursos de red. Por ejemplo, puesto que los miembros 314, 316 y 318 del personal 308 IT son responsables de mantener los ordenadores 202, 204, 206, 208, 210, 212, 214, 216 y 218, un administrador de sistemas probablemente querrá dar al personal 308 IT acceso a todos los ordenadores 202, 204, 206, 208, 210, 212, 214, 216 y 218. Por el contrario, un administrador de sistemas puede querer limitar a los auxiliares 312 administrativos para que sólo puedan acceder a los terminales de auxiliares administrativos con menos capacidades. A los ingenieros 310 se les puede conceder acceso a estaciones 302 de trabajo y a los terminales 304 CAD, pero no a los terminales 306 de auxiliares administrativos utilizados por los auxiliares 312 administrativos.

En una realización, un administrador de sistema puede restringir la capacidad de un usuario para acceder remotamente a un recurso conectado en red sin especificar limitaciones de usuario/recurso individuales. Tal como se mencionó anteriormente, el sistema 200 informático opera presuponiendo que un usuario de ordenador sólo podrá acceder remotamente a un ordenador para el que el usuario sea capaz de lograr acceso físico directo. Si un usuario no tiene acceso físico a un recurso conectado en red, ese usuario no debería poder burlar las medidas de seguridad físicas accediendo al recurso conectado en red de manera remota. A este respecto, acceso físico significa acceder a un dispositivo de entrada (tal como un teclado, ratón, bola de seguimiento, micrófono, pantalla táctil, joystick, etc.) conectado a un puesto de mando que está físicamente interconectado al recurso conectado en red. La conexión puede incluir comunicación inalámbrica en caso de que los dispositivos de entrada se comuniquen con un recurso utilizando una señal inalámbrica de corto alcance (por ejemplo, un teclado o un ratón inalámbricos). En un ejemplo sencillo, los ingenieros 310, en general, tienen acceso a los terminales 304 CAD pero sólo en los edificios en los que trabajan. El ingeniero Ellie 320, que trabaja en el segundo edificio 222, no tiene acceso físico a CAD C 212, porque éste está ubicado en el primer edificio 220. Asimismo, si Ellie encierra su estación 302 de trabajo, TermA 402, en una oficina cerrada por motivos de privacidad o seguridad, otros usuarios no tendrán acceso físico a esa estación 302 de trabajo.

Según una realización de la invención, para hacer efectiva esta extensión de limitaciones de acceso físico al entorno de acceso remoto, el sistema 200 informático incluye la funcionalidad de registro descrita anteriormente. Concretamente, un usuario no puede obtener acceso remoto a un recurso conectado en red del sistema 200 informático si el usuario no ha registrado primero el recurso conectado en red. Preferiblemente, un usuario puede registrar sólo un recurso conectado en red si el usuario solicita el registro utilizando un dispositivo de entrada (por ejemplo, teclado, ratón, micrófono, pantalla, etc.) conectado a un puesto de mando que está físicamente interconectado al recurso conectado en red. Como tal, si un usuario no puede acceder físicamente a un dispositivo de entrada de este tipo, el usuario no podrá registrar el recurso conectado en red y no podrá acceder al recurso conectado en red de manera remota.

En una realización de este tipo, no todos los usuarios que tienen acceso físico directo a un ordenador pueden registrar el ordenador. Las reglas de registro especifican qué usuarios o grupos de usuarios están autorizados a registrar qué recurso conectado en red o grupos de recursos conectados en red. Preferiblemente, las reglas de registro están especificadas a un nivel de grupo de usuarios/recursos más que a un nivel de usuario/recursos individual, a efectos de eficacia. Los grupos pueden ser los mismos grupos empleados para especificar otras reglas de acceso o pueden ser diferentes.

En referencia a la figura 4A, una tabla 400 representa reglas de registro ilustrativas, en la que las filas representan grupos 308, 310 y 312 de usuarios y las columnas representan grupos 302, 304 y 306 de recursos conectados en red. Un administrador de sistemas especifica reglas de registro, por ejemplo utilizando el sistema 228 de administración de registro. Para ello, el administrador de sistemas define una pluralidad de grupos 308, 310 y 312 de usuarios y también define grupos 302, 304 y 306 de recursos conectados en red tal como se describió anteriormente con respecto a las figuras 3A y 3B. El administrador de sistemas especifica entonces qué grupos de usuarios pueden registrar qué grupos de recursos conectados en red. Por ejemplo, en la tabla 400, un administrador de sistemas ha especificado que los miembros 208 del personal IT pueden registrar las estaciones 302 de trabajo, los terminales 304 CAD y los terminales 306 de auxiliares administrativos, tal como se indica mediante las "X" en las intersecciones de la fila personal 308 IT y las columnas de cada uno de los grupos de recursos conectados en red. De manera similar, los ingenieros 310 pueden registrar las estaciones 302 de trabajo y los terminales 304 CAD, y los auxiliares 312 administrativos sólo pueden registrar los terminales 306 de auxiliares administrativos.

Ha de entenderse que estas reglas pueden especificarse en forma de tabla tal como acaba de describirse, pero también o en lugar de ello mediante el uso de instrucciones, listas de datos, archivos de datos, etiquetas XML o cualquier otro mecanismo adecuado para la especificación de reglas.

Utilizando el sistema 228 de administración de registro, los administradores de sistemas pueden alterar fácilmente las reglas de registro una vez especificadas. Por ejemplo, para reflejar cambios en el personal (por ejemplo el despido, contratación o cambio de puesto de un empelado) el administrador de sistemas puede añadir o eliminar usuarios de los grupos de usuarios. Lo mismo puede hacerse para los grupos de recursos conectados en red. Las decisiones de política que afecten a todos los grupos pueden implementarse cambiando los grupos de recursos conectados en red que un grupo de usuarios tiene permiso para registrar. Por ejemplo, si el administrador de sistemas que especificó las reglas de registro en la tabla 400 decidiera que los auxiliares 312 administrativos también deberían poder registrar todas las estaciones de trabajo, la regla para los auxiliares 312 administrativos puede alterarse de manera correspondiente. En el caso de que un administrador de sistemas elimine la capacidad de uno o más usuarios, o grupos de usuarios, para registrar uno o más recursos conectados en red, los usuarios afectados ya no serán capaces de registrar esos recursos conectados en red. En algunas realizaciones, si los recursos conectados en red ya habían sido registrados por los usuarios afectados, el cambio en la regla de registro puede provocar que los recursos conectados en red pierdan el registro.

En referencia a la figura 5, un diagrama de flujo de un método 500 de registro de un recurso conectado en red (por ejemplo, ordenadores 202, 204, 206, 208, 210, 212, 214, 216 y 218), empieza con la especificación de reglas de registro (etapa 502), por ejemplo por un administrador de sistemas tal como se ha descrito anteriormente. Cuando un usuario solicita registrar un recurso conectado en red (etapa 504), el sistema 230 de registro verifica la identidad del usuario (etapa 506). La verificación de la identidad (etapa 506) puede lograrse mediante cualquier medio de autentificación de la identidad, incluyendo por ejemplo la autentificación mediante contraseñas o PIN de usuario, identificación biométrica, identificación de voz, etc.

El sistema 230 de registro y el sistema 228 de administración de registro determinan si las reglas de registro permiten al usuario registrar el recurso conectado en red que el usuario solicita registrar (etapa 508). En la realización ilustrativa, el sistema 230 de registro envía una solicitud de registro al sistema 228 de administración de registro. La solicitud de registro incluye la identificación del recurso conectado en red que el usuario solicita registrar y la identificación del usuario. El sistema 228 de administración de registro compara entonces la pareja usuario/recurso conectado en red con las reglas de registro para determinar si el usuario es miembro de un grupo que tiene permiso para registrar cualquiera de los recursos conectados en red del grupo al que pertenece el recurso conectado en red en cuestión.

Pueden descargarse copias de un solo uso de las reglas de registro al recurso conectado en red desde el sistema 228 de administración de registro cada vez que un usuario intenta registrar un recurso conectado en red, y en otras implementaciones un recurso conectado en red puede mantener un conjunto permanente de reglas de registro que se actualiza por el sistema 228 de administración de registro cuando un administrador de sistemas altera las reglas de registro. En cualquiera de estos casos, la verificación de permiso (etapa 508) se realiza en el recurso conectado en red.

Si el usuario tiene permiso para registrar el recurso conectado en red basándose en las reglas de registro, se determina la ubicación del usuario (etapa 510). En una realización, un sistema localizador determina la ubicación del usuario recuperando la dirección IP del recurso conectado en red desde el que se envió la solicitud de registro, normalmente incluida en la cabecera de los paquetes que constituyen la comunicación, y ejecutando una rutina de consulta de servidor de nombre de dominio (DNS) inversa para determinar la fuente de la solicitud. El sistema 228 de administración de registro determina entonces si el usuario solicitó el registro del recurso conectado en red desde un puesto de mando que está físicamente interconectado al recurso conectado en red que el usuario está solicitando registrar (etapa 512) comparando la fuente de la solicitud de registro determinada con el recurso conectado en red que está identificado en la solicitud de registro. En otra realización, el sistema localizador, transmite y provoca la ejecución de un *applet* JAVA® o control ActiveX® en el recurso solicitado para determinar si el usuario está actualmente conectado en un puesto de mando que está físicamente interconectado al recurso. En una realización adicional, la fuente de la solicitud puede verificarse transmitiendo y provocando la ejecución de un *applet* JAVA® o control ActiveX® en la fuente de la solicitud que obligue a la fuente a identificarse a sí misma. El sistema 228 de administración de registro compara entonces la identificación obligatoria con el recurso conectado en red que el usuario ha solicitado registrar. En una realización, el sistema de administración de registro lleva a cabo una combinación de dos o más de los métodos de verificación enumerados anteriormente para garantizar una identificación de la fuente de la solicitud robusta.

Si se determina que el usuario envió la solicitud de registro desde un puesto de mando que está físicamente interconectado al recurso conectado en red que el usuario solicita registrar (etapa 512), el sistema 228 de administración de registro registra el recurso conectado en red para el usuario (etapa 514) actualizando una base de datos de registros (véase la figura 6 más abajo). Si el usuario no tiene permiso para registrar el recurso conectado en red basándose en las reglas de registro, o si se determina que el usuario está intentando registrar el ordenador desde una ubicación remota, se deniega el registro (etapa 516).

En una realización alternativa, el sistema 228 de administración de registro determina la ubicación del usuario y verifica que el usuario está solicitando el registro de un recurso conectado en red desde el que se originó la solicitud de registro antes de determinar si el usuario tiene permiso para registrar el recurso conectado en red según las reglas de registro. En una realización adicional, el sistema 228 de administración de registro habilita a un administrador de sistemas para especificar reglas de registro que permitan a un grupo de usuarios registrar de manera remota recursos conectados en red o para especificar grupos de recursos que pueden registrarse de manera remota. Por ejemplo, en una realización, las reglas de registro permiten a un usuario registrar un servidor de archivos (o una parte de un servidor. de archivos) que forma parte de una red segura desde un puesto de mando que forma parte de esa red segura pero que no está físicamente interconectado al servidor de archivos.

En referencia a la figura 6, el sistema 228 de administración de registro mantiene la información sobre recursos registrados y usuarios. Este almacenamiento puede implementarse de diversas formas, incluyendo en forma de archivos de datos en una base de datos. Tal como se muestra en la representación ilustrativa del contenido de una base de datos 600 de registro, en la figura, la base de datos 600 almacena datos de registro para cada usuario individual y cada recurso conectado en red. Cuando un usuario registra con éxito un recurso conectado en red (etapa 514), el registro se almacena en la base de datos 600 de registros. Por ejemplo, según la base de datos 600 de registros, el ingeniero Ellie 320 ha registrado TermA, CAD A y CAD B. La tabla se consulta cuando un usuario intenta acceder remotamente a un recurso conectado en red.

En referencia a la figura 7, el método 700 de concesión de acceso remoto a un recurso conectado en red incluye consultar la base de datos de registros por ejemplo, la base de datos 600 de registros. Cuando un usuario intenta acceder remotamente al primer recurso 100 conectado en red, la solicitud de acceso se recibe en el sistema 232 de acceso remoto (etapa 702). El sistema 232 de acceso remoto verifica la identificación del usuario (etapa 703) también denominada autentificación. Tal como se describió anteriormente con relación a la verificación de una identidad de un usuario en el contexto del registro, el sistema 232 de acceso remoto puede autentificar un usuario utilizando cualquier medio de autentificación de identidad adecuado, incluyendo parejas contraseña/PIN de usuario, certificados, datos biométricos, claves de un solo uso, muestras de voz, etc. El sistema 232 de acceso remoto determina entonces si el usuario ha registrado previamente el primer recurso 100 conectado en red (etapa 706). Si el usuario ha registrado previamente el primer recurso conectado en red, el sistema 232 de acceso remoto concede el acceso al primer recurso

100 conectado en red (etapa 708), de lo contrario el sistema 232 de acceso remoto deniega el acceso remoto al primer recurso 100 conectado en red.

En realizaciones alternativas, un administrador de sistemas podría establecer reglas de acceso remoto adicionales que limiten qué dispositivos remotos pueden utilizar los usuarios para acceder de manera remota a recursos conectados en red. Por ejemplo, un administrador de sistemas puede especificar una regla que sólo permita a usuarios o grupos de usuarios acceder remotamente a recursos conectados en red o a un grupo de recursos conectados en red desde un recurso conectado en red directamente conectado al sistema 200 informático. Según dicha regla, Tara 314, por ejemplo, quien según la base de datos 600 de registros ha registrado AdminC 218, podría acceder remotamente a AdminC 218 desde AdminA 214, pero Ted 318, quien también ha registrado AdminC 218, no podría acceder remotamente a AdminC desde el dispositivo 102 remoto.

Un experto en la técnica se dará cuenta de que la invención puede realizarse en otras formas específicas sin alejarse del espíritu o las características esenciales de la misma. Las realizaciones anteriores han de considerarse por tanto a todos los efectos como ilustrativas más que limitativas de la invención. El alcance de la invención no está limitado sólo la descripción anterior.

REIVINDICACIONES

1. Método para proporcionar un sistema, comprendiendo el método:

Proporcionar un sistema (232) de acceso remoto para conceder a un usuario acceso remoto a un primer recurso (202) conectado en red si el usuario registró con éxito el primer recurso (202) conectado en red;

caracterizado por

proporcionar un sistema (228) de administración de registro para especificar reglas de registro;

proporcionar un sistema (230) de registro configurado para comunicarse con el sistema (228) de administración de registro para permitir registrar el primer recurso (202) conectado en red si lo permiten las reglas de registro especificadas.

2. Método según la reivindicación 1, en el que el recurso (202) conectado en red es un ordenador.

3. Método según cualquiera de las reivindicaciones 1 ó 2, en el que el sistema (232) de acceso remoto deniega el acceso remoto al primer recurso (202) conectado en red a un usuario que no haya registrado el primer recurso (202) conectado en red.

4. Método según cualquier reivindicación anterior, en el que el sistema (232) de acceso remoto está previsto para instalarse en el primer recurso (202) conectado en red.

5. Método según cualquier reivindicación anterior, en el que el sistema (232) de acceso remoto está previsto para instalarse en un recurso de red compartido, y el sistema (232) de acceso remoto concede acceso remoto al primer recurso (202) conectado en red y a un segundo recurso (204) conectado en red con sujeción a las reglas de registro especificadas y al registro por el usuario del primer recurso (202) conectado en red y del segundo recurso (204) conectado en red.

6. Método según cualquier reivindicación anterior, en el que el sistema (230) de registro no autoriza el registro del primer recurso (202) conectado en red desde un puesto (201) de mando remoto.

7. Método según cualquier reivindicación anterior, en el que el registro del primer recurso (202) conectado en red requiere que el usuario lo registre desde un puesto de mando físicamente interconectado al primer recurso (202) conectado en red.

8. Método según cualquier reivindicación anterior, en el que el sistema (230) de registro requiere el registro del primer recurso (202) conectado en red desde un puesto de mando físicamente interconectado al primer recurso (202) conectado en red.

9. Método según cualquier reivindicación anterior, en el que el acceso remoto comprende el acceso remoto al escritorio del primer recurso (202) conectado en red.

10. Método según cualquier reivindicación anterior, en el que el sistema (230) de registro es una aplicación de red.

11. Método según la reivindicación 10, que comprende además proporcionar un sistema localizador para determinar la ubicación de un usuario que intenta registrar el primer recurso (202) conectado en red.

12. Método según la reivindicación 11, en el que el registro del primer recurso (202) conectado en red está sujeto además a la ubicación determinada.

13. Método según cualquier reivindicación anterior, que comprende especificar una regla de registro y registrar un primer recurso (202) conectado en red si lo permite la regla de registro especificada.

14. Método según la reivindicación 13, en el que especificar la regla de registro comprende además: definir una pluralidad de grupos de usuarios; definir una pluralidad de grupos de recursos conectados en red; y especificar un grupo de recursos conectados en red que un grupo de usuarios tiene permiso para registrar.

15. Método según cualquier reivindicación anterior, que comprende conceder a un usuario acceso remoto al primer recurso (202) conectado en red desde un dispositivo remoto si el usuario había registrado con éxito previamente el primer recurso (202) conectado en red.

16. Método según la reivindicación 15, en el que conceder acceso al primer recurso (202) conectado en red comprende conceder acceso al escritorio del primer recurso (202) conectado en red.

17. Método según cualquiera de las reivindicaciones 15 ó 16, que comprende denegar a un usuario el acceso al primer recurso (202) conectado en red desde el dispositivo remoto si el usuario no había registrado con éxito previamente el primer recurso (202) conectado en red.

18. Sistema informático que comprende:

un dispositivo (201) remoto configurado para comunicarse con un primer recurso (202) conectado en red a través de un canal (203) de comunicaciones;

un sistema (232) de acceso remoto para conceder a un usuario del dispositivo (201) remoto acceso remoto al primer recurso (202) conectado en red si el primer recurso (202) conectado en red se registró con éxito;

caracterizado por

un sistema (228) de administración de registro para especificar reglas de registro;

el primer recurso (202) conectado en red configurado para comunicarse con el sistema (228) de administración de registro; y

un sistema (230) de registro para registrar el primer recurso (202) conectado en red si lo permiten las reglas de registro especificadas.

19. Sistema informático según la reivindicación 18, en el que el primer recurso (202) conectado en red es un ordenador.

20. Sistema informático según cualquiera de las reivindicaciones 18 ó 19, en el que el sistema (232) de acceso remoto deniega el acceso remoto al primer recurso (202) conectado en red a un usuario del dispositivo (201) remoto que no haya registrado el primer recurso (202) conectado en red.

21. Sistema informático según una cualquiera de las reivindicaciones 18 a 20, en el que el sistema (232) de acceso remoto está instalado en el primer recurso (202) conectado en red.

22. Sistema informático según una cualquiera de las reivindicaciones 18 a 21, en el que el sistema (232) de acceso remoto está instalado en un recurso de red compartido, y el sistema de acceso remoto concede a un usuario del dispositivo (201) remoto acceso al primer recurso (202) conectado en red y a un segundo recurso (204) conectado en red con sujeción a las reglas de registro y al registro por el usuario del primer y segundo recurso (202, 204) conectado en red.

23. Sistema informático según una cualquiera de las reivindicaciones 18 a 22, en el que el sistema (230) de registro no autoriza el registro del primer recurso (202) conectado en red desde un puesto (201) de mando remoto.

24. Sistema informático según una cualquiera de las reivindicaciones 18 a 23, en el que el sistema (230) de registro requiere el registro del primer recurso (202) conectado en red desde un puesto de mando físicamente interconectado al primer recurso (202) conectado en red.

25. Sistema informático según una cualquiera de las reivindicaciones 18 a 24, en el que el acceso remoto al primer recurso (202) conectado en red comprende acceso remoto al escritorio del primer recurso (202) conectado en red.

26. Sistema informático según las reivindicaciones 18 a 25, en el que el sistema (230) de registro es una aplicación de red.

27. Sistema informático según la reivindicación 26, que comprende además un sistema localizador para determinar la ubicación de un usuario que intenta registrar el primer recurso (202) conectado en red.

28. Sistema informático según la reivindicación 27, en el que el registro del primer recurso (202) conectado en red está sujeto además a la ubicación de usuario determinada.

29. Sistema informático según cualquiera de las reivindicaciones 27 ó 28, en el que el sistema (230) de administración de registros comprende una base de datos de registros que almacena una lista de recursos (202) conectados en red que un usuario ha registrado.

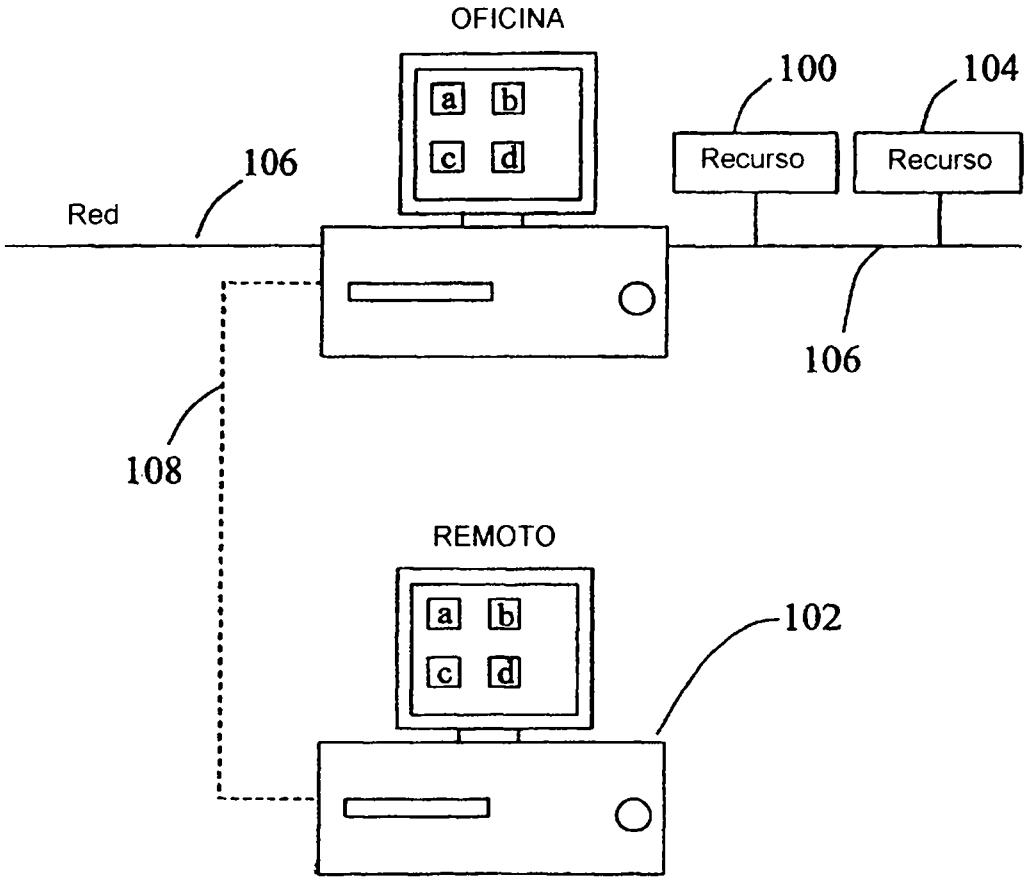

OFICINA
a
b
c
d
100
104
Recurso
Recurso
106
Red
106
108
REMOTO
a
b
c
d
102

Fig. 1

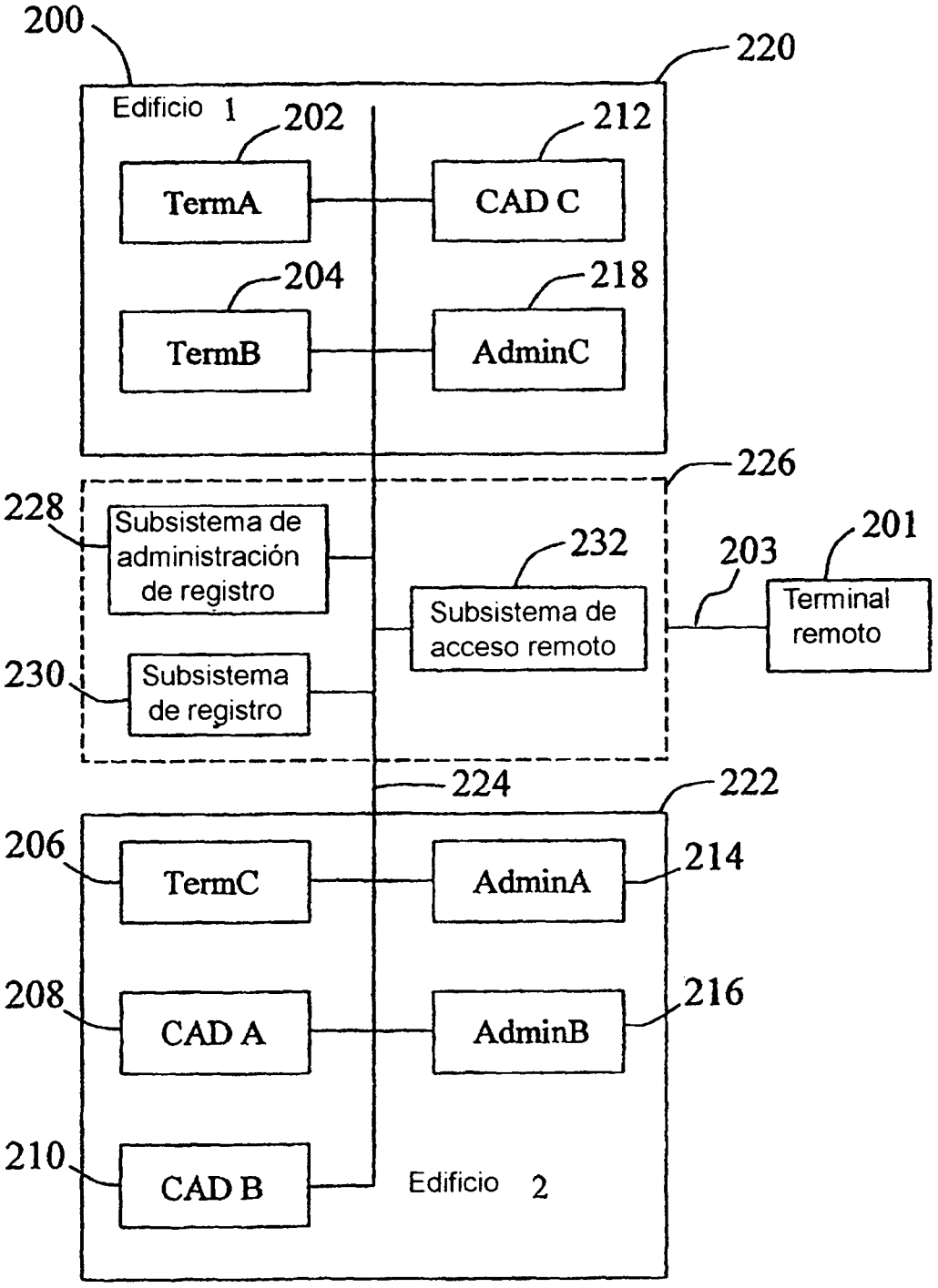

200
220
Edificio 1
202
212
TermA
CAD C
204
218
TermB
AdminC
226
228
Subsistema de administración de registro
232
203
201
Subsistema de acceso remoto
Terminal remoto
230
Subsistema de registro
224
222
206
TermC
AdminA
214
208
CAD A
AdminB
216
210
CAD B
Edificio 2

Fig. 2

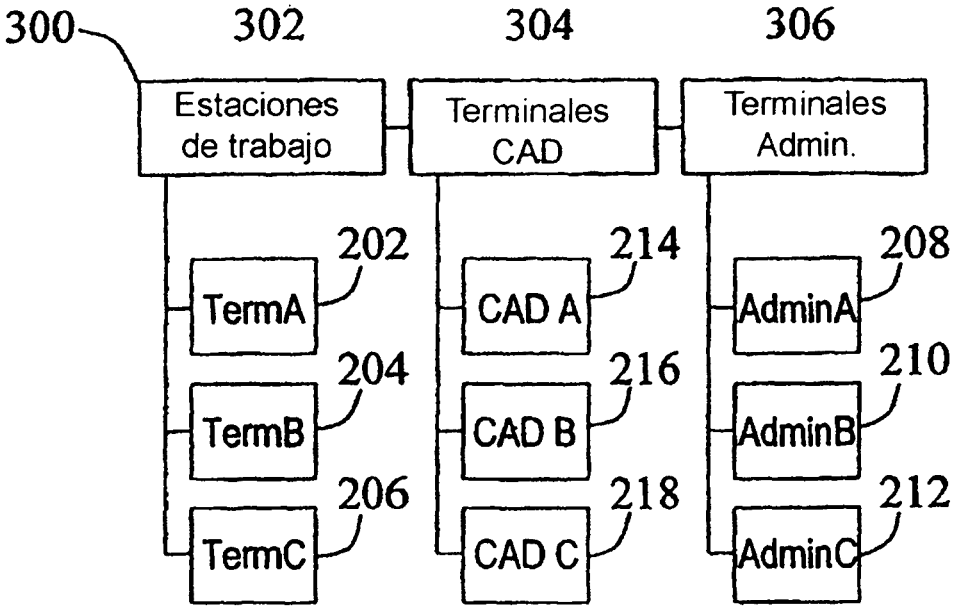

300
302
304
306
Estaciones de trabajo
Terminales CAD
Terminales Admin.
TermA
TermB
TermC
CAD A
CAD B
CAD C
AdminA
AdminB
AdminC
202
204
206
214
216
218
208
210
212

Fig. 3A

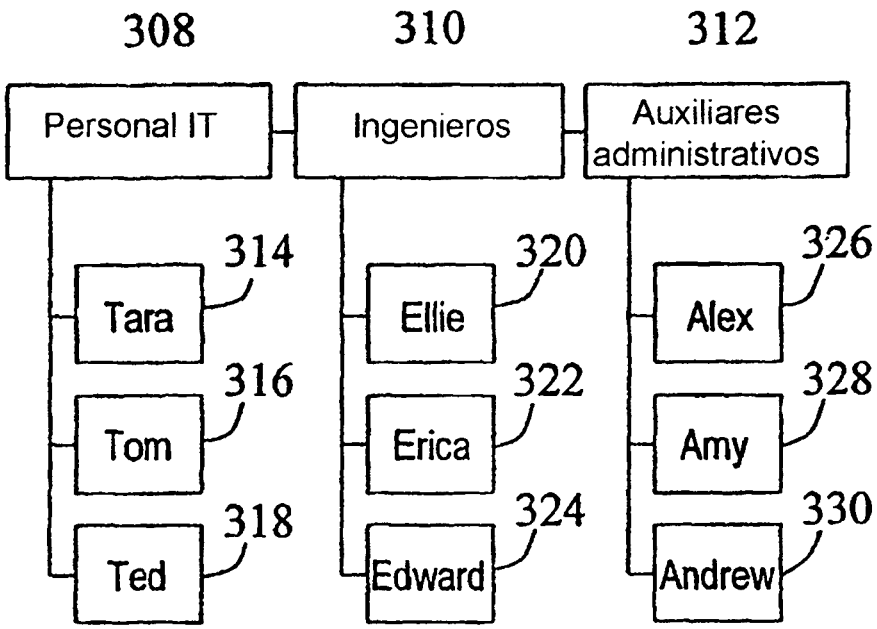

308
310
312
Personal IT
Ingenieros
Auxiliares administrativos
Tara
Tom
Ted
Ellie
Erica
Edward
Alex
Amy
Andrew
314
316
318
320
322
324
326
328
330

Fig. 3B

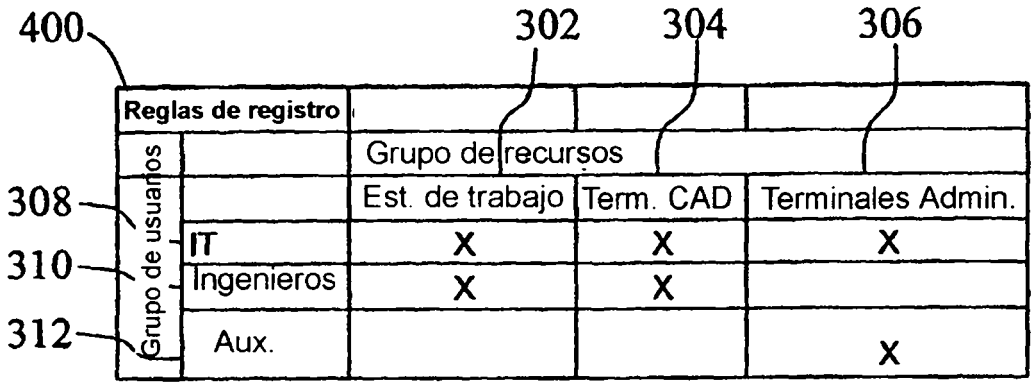

400
302
304
306
308
310
312
Reglas de registro
Grupo de usuarios
Grupo de recursos
Est. de trabajo
Term. CAD
Terminales Admin.
IT
Ingenieros
Aux.
X
X
X
X
X
X

Fig. 4

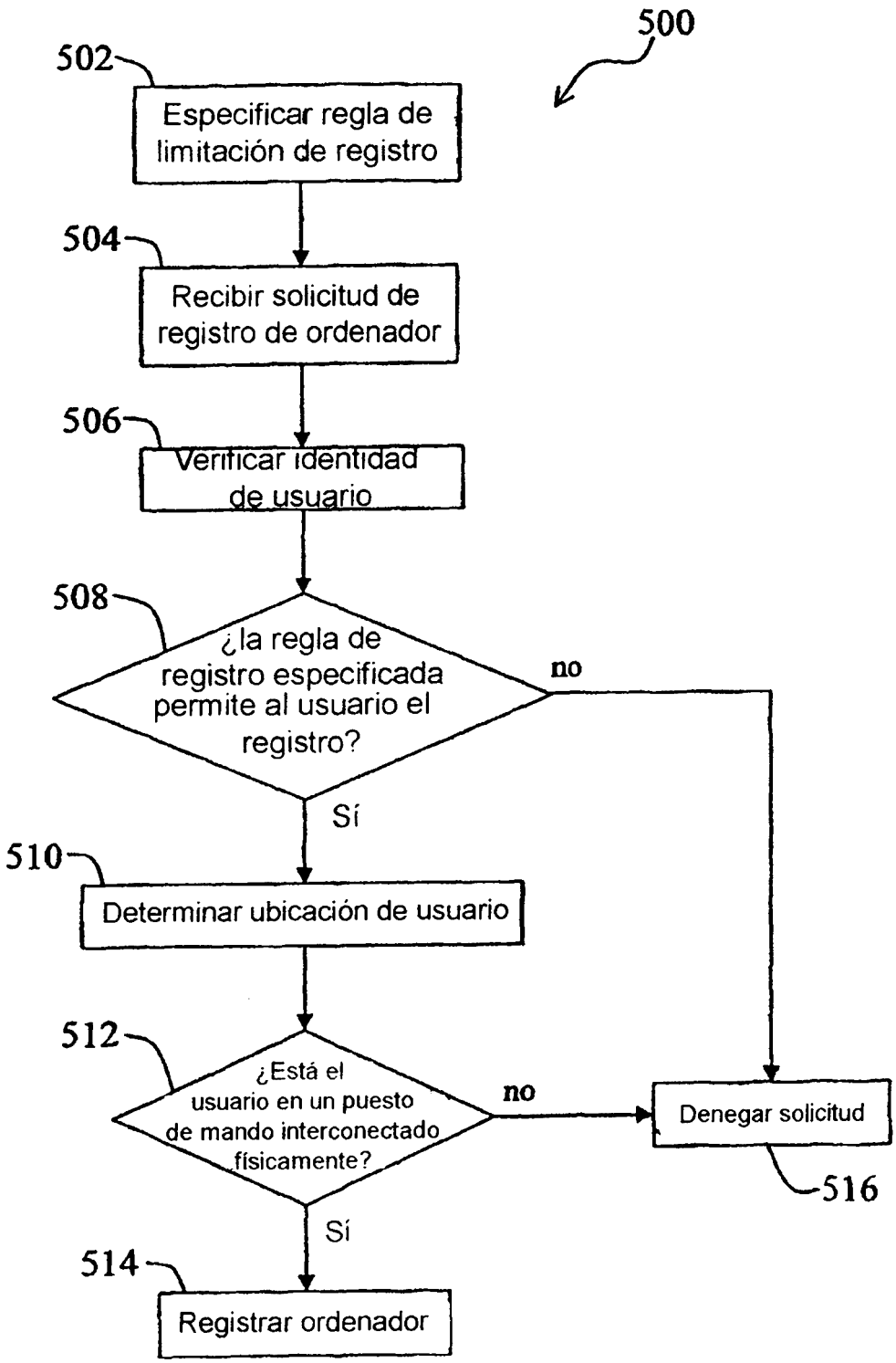

500
502
Especificar regla de limitación de registro
504
Recibir solicitud de registro de ordenador
506
Verificar identidad de usuario
508
¿la regla de registro especificada permite al usuario el registro?
no
Sí
510
Determinar ubicación de usuario
512
¿Está el usuario en un puesto de mando interconectado físicamente?
no
Denegar solicitud
516
Sí
514
Registrar ordenador

Fig. 5

600

320

	Equipos registrados								
Usuarios	TermA	TermB	TermC	AdminA	AdminB	AdminC	CAD A	CAD B	CAD C
Tara		x	x	x		x	x	x	x
Tom	x			x	x			x	x
Ted	x	x	x	x	x	x	x	x	x
Ellie	x						x	x	
Erica		x						x	x
Edward			x	x			x	x	x
Alex					x				
Amy						x			
Andrew									

Fig. 6

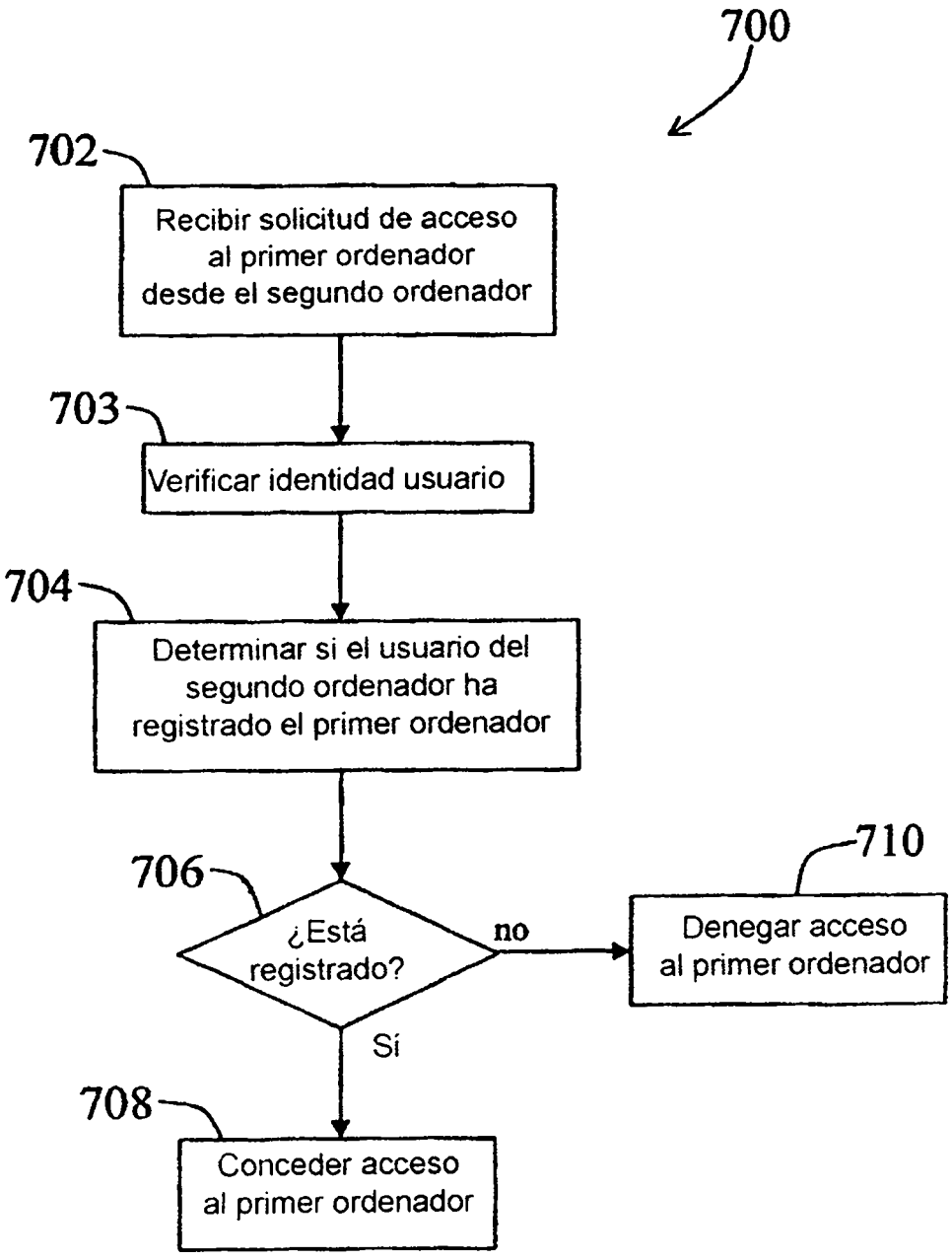

700
702
Recibir solicitud de acceso al primer ordenador desde el segundo ordenador
703
Verificar identidad usuario
704
Determinar si el usuario del segundo ordenador ha registrado el primer ordenador
706
¿Está registrado?
no
710
Denegar acceso al primer ordenador
Sí
708
Conceder acceso al primer ordenador

Fig. 7