(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 394 260**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04W 12/12 (2009.01)
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.04.2003 E 03718482 (7)**

(97) Fecha y número de publicación de la solicitud europea: **26.01.2005 EP 1500206**

(54) Título: **Sistema y procedimiento para la gestión de dispositivos inalámbricos en una corporación**

(30) Prioridad:

19.04.2002 US 373787 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.01.2013

(73) Titular/es:

GOOGLE INC. (100.0%)
1600 Amphitheatre Parkway
Mountain View, CA 94043, US

(72) Inventor/es:

VAN DE GROENENDAAL, JOHAN;
FRY, MICHAEL;
JAIN, SANDEEP;
ZALEWSKI, ANDRZEJ;
SABOROWSKI, RALF y
SRINIVAS, DAVANUM

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Sistema y procedimiento para la gestión de dispositivos inalámbricos en una corporación

Referencia cruzada a solicitudes relacionadas

La presente solicitud reivindica prioridad respecto de la solicitud provisional titulada “Wireless Enterprise Management System and Method”, número de serie 60/373.787, presentada el 19 de abril de 2002.

Campo técnico

Los sistemas y procedimientos descritos están por lo general relacionados con entornos de procesamiento de información de corporación. Más específicamente, los sistemas y procedimientos descritos están relacionados con la gestión de dispositivos inalámbricos en un entorno de procesamiento de información de corporación.

Antecedentes

En los últimos años, el uso de tecnologías móviles ha aumentado de manera sostenida tanto en el uso de corporación como personal. Los teléfonos móviles son comúnmente utilizados, y muchas personas emplean dispositivos de gestión de información personal (“PIM”) u ordenadores de bolsillo para gestionar su agenda, contactos, información financiera y otros datos. Tales dispositivos son particularmente útiles para empleados cuyas responsabilidades laborales les requieren viajar. Algunas corporaciones animan a sus empleados a conectarse periódicamente con su entorno de procesamiento de información de corporación a través de los dispositivos inalámbricos para aumentar la capacidad de respuesta y la productividad. Las conexiones periódicas móviles fomentan la comunicación entre empleados y mejoran la puntualidad de los datos recogidos a través de los procesos de organización entre los dispositivos móviles y la corporación.

La creciente proliferación de agendas digitales personales habilitadas inalámbricas (PDA), dispositivos móviles de correo electrónico y ordenadores portátiles ha animado a las compañías proveedoras de telefonía celular a ofrecer transmisión no solo de voz, sino también de señales de datos a/desde dispositivos inalámbricos móviles. Aunque la integración de estos dispositivos inalámbricos en un entorno de procesamiento de información de corporación promueve una mayor productividad y eficiencia, tal integración puede dar como resultado mayores amenazas contra la seguridad y la privacidad de la información almacenada en y transmitida a/desde tales dispositivos móviles.

Las corporaciones que emplean dispositivos inalámbricos móviles que se pueden conectar a la corporación esperan ciertos beneficios que se derivan del uso de tales dispositivos. Tales beneficios, por ejemplo, pueden incluir la capacidad de los ordenadores portátiles de estar conectados de manera inalámbrica para permitir que el trabajo se haga desde virtualmente cualquier lugar. Otro beneficio de la conectividad inalámbrica es el acceso flexible a los procesos de corporaciones. Otro beneficio adicional de la conectividad inalámbrica es la capacidad para recibir alertas y mensajes apropiados en el dispositivo móvil para llevar a cabo funciones laborales requeridas con una eficiencia mejoradas.

Además de los beneficios de la conectividad inalámbrica, los empleados que emplean dispositivos inalámbricos conectables se enfrentan a ciertos desafíos. Uno de los desafíos, por ejemplo, es el desafío de proteger adecuadamente la información en los dispositivos inalámbricos para garantizar que la información de la corporación y personal confidencial no se pierde o es robada. Otro desafío es la sincronización en tiempo real de la información para garantizar la precisión y la consistencia.

Para limitar las amenazas a la seguridad y la privacidad asociadas a la conexión de dispositivos móviles a la corporación, algunas compañías utilizan dos entornos de procesamiento de información separados: uno para dispositivos por cable y un segundo para dispositivos inalámbricos. Las compañías que mantienen dos entornos distintos pierden los beneficios de la integración y la sincronización de la que pueden beneficiarse las que utilizan un entorno combinado.

Una segunda solución de la técnica anterior para la integración de dispositivos inalámbricos en un entorno de procesamiento de información de corporación es funcionar en un modo híbrido en el cual se guardan recursos dedicados separados para ambos dispositivos por cable e inalámbricos. El empleo de tales recursos separados en un entorno combinado da a menudo como resultado una incompatibilidad entre dispositivos y/o una seguridad debilitada.

En consecuencia, existe una necesidad de un sistema y un procedimiento de gestión de los dispositivos inalámbricos en un entorno de procesamiento de información de corporación que permita la integración y la sincronización de los dispositivos inalámbricos a la vez que la protección de la seguridad y la privacidad de los datos en dispositivos conectados, bien por cable o de manera inalámbrica.

El documento EP 1 081 895 se refiere a una LAN en la que un punto de acceso y un dispositivo inalámbrico incluyen cada uno dispositivos de autenticación. El dispositivo inalámbrico recibe un mensaje de autenticación de parte del punto de acceso y determina si el punto de acceso es un punto de acceso válido a una LAN por cable.

El documento “AirWave Rogue Access Point Detection” (XP-002319028) se refiere a un sistema en el cual un punto de acceso o un dispositivo centinela explora las ondas de radio para todos puntos de acceso dentro de una corporación. Si se informa de cualesquiera puntos de acceso desconocidos, el sistema genera una alerta de que puede haber un punto de acceso intruso.

El documento de IBM Research News “IBM Research Demonstrates Industry’s First Auditing Tool for Wireless Network Security” (XP-002263357) se refiere a una herramienta de verificación que puede controlar 802.11 redes inalámbricas y recoger información relacionada con la seguridad. La información de comprobación está presente en una interfaz de usuario codificada por colores en una pequeña PDA inalámbrica.

El documento US 2001/0007818 se refiere a un procedimiento de control de fallo para un terminal de comunicación portátil por radio. Cuando una operación de retransmisión (reintento) se produce en el terminal durante una comunicación con una estación base debido a una no-respuesta, se considera un fallo o una operación anormal, si el reintento supera un número predeterminado de veces.

El documento WO 01/41485 se refiere a un procedimiento para examinar la conformidad del equipo de radio. Una estación secundaria recibe una secuencia de comandos de control de la potencia de transmisión. La potencia de salida de la estación secundaria es entonces examinada para ver si existe un rango predeterminado relativo a la potencia de salida al inicio del examen.

El documento DE 198 54 177 se refiere a un procedimiento en el cual un canal de frecuencias en un sistema de comunicaciones móviles es reconocido como afectado u ocupado cuando hay una diferencia significativa de un parámetro de informes de mediciones o un valor de umbral.

Sumario

Lo que sigue a continuación presenta un sumario simplificado de sistemas y procedimientos asociados con dispositivos inalámbricos de gestión en un entorno de procesamiento de corporación. Este sumario no es una visión general extensiva y no está destinado a identificar elementos claves o críticos de los procedimientos y/o sistemas o determinar el alcance de los soportes, procedimiento y sistemas. Identifica conceptualmente los procedimientos y sistemas de una manera simplificada como una introducción a la descripción más detallada que se presenta más adelante.

De acuerdo con la invención, se proporciona: un procedimiento de acuerdo con la reivindicación 1; un medio legible por ordenador de acuerdo con la reivindicación 11; y un aparato de acuerdo con la reivindicación 12.

Un procedimiento ejemplar es divulgado para gestionar un dispositivo inalámbrico en una red. El procedimiento incluye identificar una pluralidad de puntos de acceso inalámbricos lógicos autorizados dentro de una red. El procedimiento también incluye detectar una pluralidad de puntos de acceso inalámbricos físicos dentro de la red, y determinar, para cada uno de la pluralidad de puntos de acceso inalámbricos físicos, si el punto de acceso inalámbrico físico, está asociado con uno de la pluralidad de puntos de acceso inalámbricos lógicos autorizados. El procedimiento incluye, además, informar de cada punto de acceso inalámbrico que no está asociado con un punto de acceso inalámbrico lógico autorizado.

Un procedimiento ejemplar es divulgado para gestionar un dispositivo inalámbrico en una red. El procedimiento incluye definir un conjunto de recursos asociados autorizados con un dispositivo inalámbrico en una red. El procedimiento también incluye detectar el dispositivo inalámbrico en la red, y determinar los propios recursos asociados con el dispositivo inalámbrico. El procedimiento incluye, además, analizar el conjunto de recursos autorizados y los propios recursos para identificar al menos un recurso señalizado. El procedimiento incluye además informar de al menos un recursos señalizado.

Un procedimiento ejemplar es divulgado para gestionar un dispositivo inalámbrico en una red. El procedimiento incluye detectar un dispositivo en una red, y determinar que el dispositivo es un dispositivo inalámbrico. El procedimiento también incluye determinar que el dispositivo ha recibido datos de un ordenador. El procedimiento incluye, además, ejecutar una rutina de exploración de virus asociada con el dispositivo inalámbrico.

Un procedimiento ejemplar es divulgado para gestionar un dispositivo inalámbrico en una red. El procedimiento incluye definir una política de copia de seguridad de datos con un dispositivo inalámbrico en una red. El procedimiento también incluye detectar el dispositivo inalámbrico en la red, y analizar la política de copia de seguridad de datos para determinar que se debería hacer una copia de seguridad de los datos que residen en el dispositivo inalámbrico. El procedimiento incluye, además, hacer una copia de seguridad de los datos que residen en el dispositivo inalámbrico.

Ciertos aspectos ilustrativos de los procedimientos y sistemas son descritos en el presente documento junto con la siguiente descripción y los dibujos adjuntos. Estos aspectos son indicativos, sin embargo, de unas pocas maneras en las que los principios de los procedimientos, sistemas y soportes se pueden emplear y de este modo los ejemplos están destinados a incluir tales aspectos y equivalentes. Otras ventajas y características novedosas pueden ponerse de manifiesto en la siguiente descripción detallada cuando se considera junto con los dibujos.

Breve descripción de los dibujos

Para una mayor comprensión de los presentes procedimientos y sistemas, se hace ahora referencia a la siguiente descripción tomada conjuntamente con los dibujos adjuntos en los cuales los números de referencia iguales indican características iguales y en los cuales:

la figura 1 es un diagrama de bloques que ilustra un entorno de procesamiento de información de corporación ejemplar, de acuerdo con los sistemas y procedimientos descritos en la presente solicitud;
la figura 2 es un diagrama de bloques que ilustra una red inalámbrica entre pares;
la figura 3 es un diagrama de bloques que ilustra una LAN inalámbrica que tiene una arquitectura de infraestructura;
la figura 4 es un diagrama de flujo que ilustra una metodología ejemplar para detectar automáticamente puntos de acceso inalámbricos en una red;
la figura 5 es un diagrama de flujo que ilustra una metodología ejemplar para gestionar recursos de un dispositivo inalámbrico en una red;
la figura 6 es un diagrama de flujo que ilustra una metodología ejemplar para mantener la seguridad de un dispositivo inalámbrico en una red; y
la figura 7 es un diagrama de flujo que ilustra una metodología ejemplar para realizar una copia de seguridad de los datos de un dispositivo inalámbrico en una red.

Descripción detallada

Ahora se describirán procedimientos y sistemas ejemplares con referencia a los dibujos, donde los números de referencia iguales se usan para referirse a elementos iguales a lo largo de todos os dibujos. En la siguiente descripción, por motivos explicativos, numerosos detalles específicos son presentados para facilitar globalmente la comprensión de los procedimientos y sistemas. Puede ser evidente, sin embargo, que los procedimientos y sistemas puedan ser llevados a la práctica sin estos detalles específicos. En otros casos, se muestran estructuras y dispositivos bien conocidos en forma de diagrama de bloques para simplificar la descripción.

La figura 1 ilustra un entorno de procesamiento de información de corporación ejemplar 100. El entorno de corporación incluye una porción de un entorno de corporación 110 que incluye una intranet 115 que gestiona y proporciona acceso a datos 120 y aplicaciones 125. A la intranet 115 se puede acceder por uno o más dispositivos que comprenden una red de área local inalámbrica (“LAN”) 135 por la pasarela 130. La LAN inalámbrica 135 puede ser cualquier tipo de LAN inalámbrica conocida por el experto en la técnica, y puede ser propietaria o cumplir con un número de estándares de LAN inalámbrica establecidos.

Actualmente, los organismos de estándares para entorno de negocio electrónico inalámbrico están centrados en asuntos relacionados con el hardware y las infraestructuras. Ejemplos de tales organismos de estándares incluyen la Alianza de Compatibilidad Ethernet Inalámbrica (“WECA”), el Instituto de Ingenieros Eléctricos y Electrónicos (“IEEE”), el Grupo de Interés Especial *(*SIG*)* de Bluetooth, y el Foro de Protocolo de Aplicaciones Inalámbricas (“WAP”).

WECA busca legalizar la interoperabilidad de los productos basados en la especificación 802.11b. WECA certifica tales productos como compatibles con fidelidad inalámbrica (Wi-Fi). WECA sustenta Wi-Fi como el estándar de LAN inalámbrica global en todos los segmentos comerciales.

IEEE realiza investigaciones extensivas en tecnología abarcando un gran espectro. IEEE creó el estándar 802.11 para redes inalámbricas, y es también instrumental en la creación de protocolos de seguridad tales como Privacidad equivalente de cable (WEP). El IEEE no proporciona certificaciones de ningún tipo para sus especificaciones.

SIG es una organización de voluntarios gestionada por empleados de compañías miembros.

Los miembros apoyan un número de grupos de trabajo que se basan en áreas específicas, tales como ingeniería, cualificación y comercialización. Las compañías miembros construyen y cualifican productos bajo procedimientos estrictos de cualificación con exámenes regulares de los productos en eventos patrocinados por Buetooth.

El foro WAP ofrece un programa de certificación y examen de interoperabilidad que cubre el examen del dispositivo, la verificación de contenidos y un conjunto de directrices de autor para ayudar a los promotores a proporcionar aplicaciones y servicios WAP interoperables.

La LAN inalámbrica 135 puede emplear cualquier arquitectura de red conocida, tal como por ejemplo, una arquitectura entre pares o una arquitectura de infraestructura. Como se ha ilustrado en la figura 2, cada dispositivo inalámbrico o cliente (210, 215 y 220) en una red inalámbrica entre pares 200 comunica con otros dispositivos en la red dentro de un rango o célula de transmisión especificado. Si un cliente inalámbrico tiene que comunicarse con un dispositivo exterior a la célula especificada, un cliente dentro de esa célula debe actuar como una pasarela y llevar a cabo el enrutamiento necesario.

La figura 3 ilustra una LAN inalámbrica 300 que tiene una arquitectura de infraestructura. En la LAN inalámbrica 300, las comunicaciones entre múltiples clientes inalámbricos 310, 315 y 320 son enrutadas por una estación central conocida como un punto de acceso 325. El punto de acceso 325 actúa como un puente y envía todas las comunicaciones al cliente apropiado en la red ya sea por cable o de manera inalámbrica. Aparte de tener mecanismos de enrutado, el punto de acceso 325 también incluye un servidor DHCP y otras características que facilitan las comunicaciones inalámbricas en entorno de pequeñas y medianas corporaciones. Las pasarelas residenciales son similares a los puntos de acceso, pero no tienen las características de gestión avanzadas requeridas para las redes de grandes corporaciones o entornos de tráfico elevado. Un cliente inalámbrico es en primer lugar autenticado, y a continuación asociado a un punto de acceso antes de llevar a cabo cualquier comunicación.

Volviendo a la figura 1, el entorno de corporación 100 incluye una red inalámbrica de área extendida ("WAN") 140. La WAN inalámbrica 140 incluye dispositivos inalámbricos que están fuera del área de cobertura de una LAN inalámbrica y está respaldada por un operador inalámbrico 145. WAN 140 puede ser cualquier tipo de WAN inalámbrica conocida por el experto en la técnica, y puede ser propietaria o cumplir con un número de protocolos inalámbricos.

Ejemplos de protocolos WAN que pueden usarse por la WAN 140 incluyen acceso múltiple por división de código ("CDMA") y sistema global para móvil ("GSM"). En una red CDMA, un gran número de usuarios son capaces de acceder a canales inalámbricos bajo pedido. La CDMA es usada típicamente por compañías de telefonía móvil digital, y el rendimiento es aproximadamente entre 8 y 10 veces mejor que los sistemas de telefonía celular analógicos tradicionales. La última generación de esta tecnología se denomina 3G y es muy esperada por muchos usuarios de móviles.

GSM es una plataforma inalámbrica que proporciona soporte completo de voz y datos con capacidades de itinerancia por todo el mundo. La familia de GSM incluye la plataforma de Servicio General de paquetes vía radio ("GPRS") para suministrar contenido de internet sobre dispositivos móviles, la plataforma de velocidades de datos mejoradas para la evolución de GSM ("EDGE") y la plataforma de tercera generación (3GSM) para proporcionar multimedia móvil. Algunas compañías proveedoras de telefonía celular basan sus servicios en las plataformas anteriores, aprovechando la fuerza del protocolo implementado.

El operador inalámbrico 115 puede ser cualquier organización o sistema que proporciona la infraestructura de hardware y comunicación para permitir la transmisión inalámbrica en una LAN inalámbrica y/o un entorno WAN inalámbrico. Habitualmente, el operador inalámbrico 145 proporciona servicios de telefonía inalámbrica, y puede ofrecer servicios para transmitir datos de varias maneras.

En esta realización ejemplar, los datos son transferidos entre el operador inalámbrico 145 y la porción del entorno de corporación 110 por una pasarela inalámbrica 150, internet 155 y un cortafuegos 160.

Importantes desafíos para corporaciones que implementan redes que incluyen dispositivos inalámbricos se refiere a la gestión de redes inalámbricas y la gestión de dispositivos móviles. Los componentes que constituyen una infraestructura inalámbrica incluyen los componentes de cable tales como los servidores, ordenadores de sobremesa complementarios, y puntos de acceso, por ejemplo. Estos componentes debería ser controlado y gestionados efectivamente para mantener un entorno de trabajo productivo. Con varios dispositivos móviles que proliferan a través de toda la corporación, es importante asegurar, gestionar y controlar el uso de estos dispositivos. Dispositivos móviles tales como PDA, teléfonos celulares, y ordenadores portátiles, por ejemplo, así como los recursos almacenados en los mismos deberían estar protegidos y gestionados. Es importante considerar que una gran parte de la infraestructura inalámbrica es realmente de cable. Todos los recursos de corporación dentro de las infraestructura existente pueden conectarse a través de una intranet de cable, que está entonces conectada a puntos de acceso que proporcionan acceso inalámbrico a dispositivos móviles.

Consideraciones de gestión de redes inalámbricas

Según la presente invención, ciertos sistemas y procedimientos para gestionar una red inalámbrica mejoran su rendimiento y permiten que un equipo de administración responda rápidamente a las cuestiones. Además de proporcionar una visión entiempo real de la red inalámbrica, una solución de gestión debería proporcionar también una visión futura, de manera que se puedan tomar medidas proactivas para prevenir problemas antes de que ocurran. Importantes consideraciones en la gestión de redes inalámbricas incluyen:

- Detección y seguridad de puntos de acceso: Los puntos de acceso a la red inalámbrica deberían ser conocidos, controlados y considerados. Debido a que los puntos de acceso son económicos y fáciles de instalar, los empleados o departamentos individuales pueden comprar uno y configurar su propia red inalámbrica no autorizada. Siendo vulnerable en sus configuraciones por defecto, los puntos de acceso no autorizados presentan a menudo violaciones de seguridad en la red. En las redes actuales, los puntos de acceso no autorizados se pueden añadir a una red, pero pueden seguir sin ser descubiertos, haciendo que de este modo medidas de seguridad sean pasadas por alto.

- Topología de puntos de acceso: El número de dispositivos móviles soportados concurrentemente por los puntos de acceso de la técnica anterior varía de un modelo a otro. Las corporaciones deberían saber cuántos puntos de acceso son necesarios para soportar sus usuarios inalámbricos, y los puntos de acceso deberían situarse en las ubicaciones geográficas apropiadas para maximizar la cobertura. Un buen acceso puede depender también de la línea física del emplazamiento a la vista de los puntos de acceso, lo cual podría ser un problema en ciertos entornos, tales como edificios con oficinas interiores, por ejemplo.
- Gestión de fallos y rendimiento: Como las mayoría de los componentes de hardware, los puntos de acceso tienen una probabilidad de fallar. Además, debido a ciertos límites en el número de usuarios concurrentes, es importante controlar la capacidad y el uso para que se puedan tomar medidas para proporcionar puntos de acceso adicionales según las necesidades. Los administradores deberán ser notificadas cuando las políticas son violadas, o si falla un componente. La solución de gestión debería soportar los diferentes estándares como RMON, NIB-II y MIB propietario para controlar efectivamente el estado de estos dispositivos.
- Privacidad y seguridad: Las redes inalámbricas son unas de las más fácil de piratear y las medidas de seguridad de la técnica anterior no son adecuadas para prevenir esta intrusión. Hay varias vulnerabilidades en las características de seguridad WEP proporcionados en el estándar 802.11b. El objetivo de WEP es proporcionar confidencialmente datos en redes inalámbricas al mismo nivel que en la red por cable. Sin embargo, a pesar de tener mecanismos de cifrado bien conocidos, en concreto el cifrado RC4, WEP es vulnerable a ataques tanto pasivos como activos. Estas vulnerabilidades abren una red inalámbrica a que partes maliciosas intercepten y alteran las transmisiones inalámbricas.
- Protección contra virus: Las soluciones de antivirus para corporaciones de la técnica anterior pueden proteger servidores, ordenadores de sobremesa, y ordenadores portátiles, pero la técnica anterior no ha proporcionado una solución que proteja un servidor de corporación contra virus que infectan la corporación usando dispositivos móviles como portadores. Los virus pueden incluso atacarse ellos mismos en puntos de acceso y espiar las transmisiones confidenciales.
- Gestión de corporación para administradores móviles: los administradores de red deberían tener la capacidad de gestionar la corporación a través de los dispositivos móviles. Los administradores deberían tener acceso a todas las herramientas de gestión apropiadas a través de todos sus dispositivos móviles para poder ser más eficientes mientras se desplazan.

La presente solicitud reconoce que es deseable gestionar las infraestructuras por cable e inalámbricas de manera unificada o integrada, De este modo, las compañías pueden aislar más fácilmente los problemas de fallos y rendimiento, los cuales pueden afectar adversamente a la calidad del servicio. Las soluciones de gestión tanto con soporte por cable como inalámbricas pueden proporcionar análisis sofisticados de la causa raíz y gestión de nivel de servicio extremo a extremo.

Consideraciones de gestión de dispositivos móviles

Como la parte móvil de los dispositivos inalámbricos de corporación como ordenadores portátiles, PDA, y otros dispositivos inalámbricos deberían ser gestionados y asegurados con control efectivo sin restringir la libertad del usuario de aprovechar los beneficios de ser móvil. Importantes consideraciones relativas a la gestión de dispositivos móviles incluyen:

- Detección de dispositivos: El administrador de corporación debería saber que dispositivos móviles están siendo utilizado en la red. Según la presente solicitud, hacer un seguimiento y mantener un inventario de todos los dispositivos aprobados puede prevenir el acceso no autorizado a la red inalámbrica.
- Suministro de software: Las herramientas administrativas deberían asegurar que todos los dispositivos móviles utilizan las versiones correctas de las aplicaciones corporativas. Por ejemplo, las últimas firmas de virus deberían actualizarse en los dispositivos móviles para mantener la seguridad. Cuando un dispositivo es sustituido o replicado, el administrador debería tener una manera de transferir fácilmente el software corporativo autorizado al dispositivo móvil del usuario para mantener la continuidad de corporación.
- Gestión de recursos: Los dispositivos móviles que se suponen son de uso corporativo deberían estar protegidos contra aplicaciones y datos no autorizados. Los administradores deberían mantener un inventario de software y hardware de cada dispositivo móvil e imponer las políticas apropiadas.
- Seguridad de dispositivos: Los dispositivos móviles incluyen características sofisticadas de seguridad de manera que si son pierden, extravían o son robados, se pueden localizar ye inhabilitar fácilmente antes de que la información confidencial caiga en malas manos.

- Identificación y seguimiento de dispositivos: Muchos dispositivos móviles no tienen nombres o identificadores únicos, haciendo que sea difícil para los administradores seguir y dar cuenta de todos los dispositivos inalámbricos en uso. Muchos empleados pueden estar usando dispositivos que no están soportado por la corporación y podrían convertirse en una responsabilidad de seguridad. Por lo tanto los dispositivos móviles aprobados deberían ampliarse para incluir la capacidad de soportar un único identificador.

- Protección contra virus: Los ordenadores portátiles y algunos dispositivos móviles basados en Windows son susceptibles de virus que funcionan sobre PC y requieren protección antivirus. Aunque no se haya informado actualmente de virus importantes para la mayoría de los dispositivos móviles es posible que nuevos virus se puedan propagar infectando específicamente y destruyendo archivos e información en dispositivos móviles. No solo se debería proteger el dispositivo contra ataque de virus, sino que tampoco debería convertirse en un soporte para virus que permanece durmiente en el dispositivo inalámbrico e infecta el PC complementario durante la sincronización u otras máquinas en la LAN.
- Preservación de datos: La información en los ordenadores portátiles inalámbricos y otros dispositivos móviles debería ser sometida a una copia de seguridad regularmente. En caso de pérdida de datos, la restauración de los datos no debería ser complicada.

La presente solicitud reconoce que los sistemas inalámbricos no funcionan independientemente de la infraestructura de cable, están integrados en la infraestructura IT. Por lo tanto la gestión de la infraestructura inalámbrica debería ser llevada a cabo en el contexto de la infraestructura de corporación global. Las soluciones de la técnica anterior diseñadas específicamente para y limitada a redes inalámbricas no integran efectivamente funciones de gestión de dispositivos inalámbricos con control del resto de la corporación para identificar rápidamente y resolver problemas. Las soluciones de gestión inalámbrica deberían ser integradas, exhaustivas y fiables. Tales soluciones exhaustivas permiten que los administradores de red gestionen y aseguren su infraestructura de red inalámbrica y les permite mejorar la productividad de gestión y mantener altos niveles de servicio para aplicaciones inalámbricas.

De acuerdo con un aspecto de la presente solicitud, dispositivos tales como puntos de acceso y dispositivos móviles, en una red inalámbrica son detectados automáticamente e identificados. Tal detección e identificación automática asegura que todos los componentes en la red inalámbrica, incluyendo servidores, ordenadores portátiles, puntos de acceso inalámbricos y dispositivos móviles, por ejemplo, sean considerados. Se crea un mapa topológico de sus conexiones físicas y lógicas. Usando este mapa topológico, los administradores de red pueden detectar fácilmente las adiciones de componentes no autorizados en la red y tomar las acciones apropiadas para rectificar una situación particular.

En una realización ejemplar, una solución de gestión de red integrada puede detectar e identificar automáticamente dispositivos inalámbricos en una red. La figura 4 es un diagrama de bloques que ilustra una metodología ejemplar para detectar automáticamente puntos de acceso inalámbricos, tales como el punto de acceso inalámbrico 325, en una red tal como la red 100.

En el bloque 405, se identifica una pluralidad de puntos de acceso inalámbricos lógicos autorizados dentro de una red. Cada punto de acceso físico puede proporcionar a uno o más dispositivos inalámbricos acceso a la red. En el bloque 410, la red detecta una pluralidad de puntos de acceso inalámbricos físicos dentro de la red. En el bloque 415, cada punto de acceso inalámbrico físico es comparado con la pluralidad de puntos de acceso inalámbricos lógicos autorizados para determinar si el punto de acceso inalámbrico físico es un punto de acceso autorizado a la red. En el bloque 420, si el punto de acceso físico no está autorizado, se informa del punto de acceso no autorizado en el bloque 425 a un administrador de red u otra parte responsable de manera a tomar una acción correctiva.

La información recogida usando la metodología 400, junto con información acerca de otros dispositivos incluyendo dispositivos inalámbricos que usan los puntos de acceso físicos, se pueden usar para crear un mapa de la topología de la red. Una vez descubiertos los componentes en la infraestructura inalámbrica, el mapa resultante puede usarse para construir una topología más eficiente para mejorar el rendimiento de la red inalámbrica.

Las redes inalámbricas tienen una topología jerárquica y cada dispositivo móvil está asociado al punto de acceso que usa para conectarse a la red. A medida que los usuarios se desplazan de un punto de acceso a otro, la topología puede cambiar para reflejar este movimiento. De esta manera, los dispositivos móviles sobre la red inalámbrica pueden ser seguidos y su ubicación puede ser representada en consecuencia.

La naturaleza dinámica del soporte inalámbrico presenta algunos desafíos para gestionar fallos y el rendimiento de dispositivos en la red inalámbrica. Además del conjunto estándar de valores métricos que son comunes a todas las redes por cable, las redes inalámbricas tienen un conjunto adicional de valores métricos relacionados con el propio soporte inalámbrico que puede ser controlado. Algunos de estos valores métricos incluyen potencia de transmisión, interferencia, retransmisión, recuentos de fragmentación, recuento de fallos, y cambio en la velocidad de transmisión. Las soluciones de la presente solicitud proporcionan capacidades de control extensivas para configuraciones de dispositivos RMON-I, RMON-II y MIB-II, que son adoptadas por muchos puntos de acceso actualmente disponibles. Asimismo se pueden recoger valores métricos de MIN propietario del proveedor.

Los administradores pueden ser alertados cuando un punto de acceso se apaga o cuando las operaciones normales se interrumpen. Usando análisis de causas raíz, las aplicaciones de gestión de red pueden determinar si un componente de red ha fallado o si el propio dispositivo tiene problemas. Políticas personalizadas puede también crearse para asegurar que un componente de red inalámbrico se está llevando a cabo eficientemente.

Además de la gestión de fallos y del rendimiento, es importante gestionar el acceso a los dispositivos inalámbricos, y a la red. En una realización, los usuarios que intentan registrarse en la red inalámbrica pueden autenticarse y cualquier actividad inusual puede ser detectada. En consecuencia, se puede prevenir que los intrusos tengan acceso a información sensible. Políticas de seguridad pueden ser definidas y aplicadas y se las autoridades apropiadas pueden ser avisadas cuando se infringe una política.

La gestión de recursos de dispositivos inalámbricos es otra área importante de interés para la gestión de red inalámbrica. En una realización ejemplar, una solución de gestión de red integrada puede ser recursos de un dispositivo inalámbrico en una red. La figura 5 es un diagrama de bloques que ilustra una metodología ejemplar para gestionar los recursos de un dispositivo de red inalámbrico.

En el bloque 505, un conjunto de recursos autorizados está definido. Los recursos están asociados con un dispositivo inalámbrico en una red. Los recursos pueden incluir hardware o software, y la definición de recurso puede ser suficientemente específica para identificar una versión particular de software o un nivel particular de revisión de hardware. Cualesquiera recursos de hardware y software en el dispositivo móvil pueden ser gestionados. En los bloques 510 y 515, la aplicación de gestión de red detecta el dispositivo realmente asociados a o que residen en el dispositivo inalámbrico detectado.

En el bloque 520, el conjunto de recursos autorizados y los recursos que residen realmente en el dispositivo inalámbrico son analizados para identificar al menos un recurso marcado. Por ejemplo, un recurso marcado puede ser un componente de software desaparecido o caducado, un componente de hardware no autorizado o un componente de hardware o software dañado.

En el bloque 525, se informa de cualesquiera recursos marcados, por ejemplo) a un administrador de red. La metodología 500 permite mantener un inventario de recursos y detectar e informar de cualquier violación de política de manera que se pueda rectificar bien automáticamente o manualmente. Esto evita que el dispositivo inalámbrico esté fuera de conformidad con las políticas de red o que por el contrario sea utilizado indebidamente.

Usando la metodología 500, el software de corporación puede ser proporcionada a dispositivos móviles bien a través de una unidad incrustada o directamente sobre la red inalámbrica. Esto asegura uniformidad y que todos los usuarios móviles tengan las últimas versiones de software en sus dispositivos para una mayor productividad y un soporte simplificado.

La figura 6 es un diagrama de flujo que ilustra una metodología ejemplar 600 para mantener la seguridad de un dispositivo inalámbrico en una red. En el bloque 605 y 610, la red detecta un dispositivo y determina que el dispositivo es un dispositivo inalámbrico. En el bloque 615, la red determina que el dispositivo ha recibido recientemente datos de un ordenador que puede estar infectado con un virus informático. En el bloque 620, la red inicia la ejecución de una rutina de exploración de virus asociada al dispositivo inalámbrico.

Un antivirus de intervención moderada especialmente construido para dispositivos móviles puede ser usado para preservar la red de ataques de virus. Las exploraciones en busca de virus pueden ser llevada a cabo siempre que el dispositivo inalámbrico se sincroniza con o descarga información de un PC complementario. Evidentemente, las exploraciones bajo pedido pueden ser realizadas en cualquier momento. Los virus para PC que no afectan a los dispositivos móviles también pueden ser detectados, previniendo de este modo que el dispositivo sea un portador.

La figura 7 es un diagrama de flujo que ilustra una metodología ejemplar 700 para iniciar una copia de seguridad de datos de un dispositivo inalámbrico en una red. Se define una política de copia de seguridad para el dispositivo inalámbrico en el bloque 705. La red detecta el dispositivo inalámbrico en el bloque 710 y la política de copia de seguridad de datos es analizada para determinar que se debería hacer una copia de seguridad de los datos que residen en el dispositivo inalámbrico (715). En el bloque 720, se procesa una rutina de copia de seguridad de datos.

Lo que se ha descrito anteriormente incluye varios ejemplos. Evidentemente, no es posible describir cada combinación imaginable de componentes o metodologías para describir los sistemas, procedimientos, y soportes legibles por ordenador asociados a dispositivos inalámbricos de gestión en una corporación. Sin embargo, el experto en la técnica puede reconocer que son posibles combinaciones y permutaciones adicionales. En consecuencia, la presente solicitud está destinada a comprender tales alteraciones, modificaciones, y variaciones que forman parte del alcance de las reivindicaciones adjuntas. Asimismo, en la medida en que el término “incluye” se emplea en la descripción detallada o las reivindicaciones, tal término está destinado a ser inclusivo de manera similar al término “que comprende” ya que ese término se interpreta cuando se emplea como una palabra de transición en una reivindicación.

REIVINDICACIONES

1.- Un procedimiento para gestionar un dispositivo inalámbrico en una red, comprendiendo el procedimiento:

identificar (405) una pluralidad de puntos de acceso inalámbricos lógicos autorizados dentro de una red;
detectar (410) una pluralidad de puntos de acceso inalámbricos físicos dentro de la red;
determinar (415, 420), para cada uno de la pluralidad de puntos de acceso inalámbricos físicos, si el punto de acceso inalámbrico físico está asociado con uno de la pluralidad de puntos de acceso inalámbricos lógicos autorizados; e
informar (425) de cada punto de acceso inalámbrico físico que no está asociado con un punto de acceso inalámbrico lógico autorizado.

caracterizado porque el procedimiento incluye, además:

detectar una pluralidad de dispositivos inalámbricos, incluyendo determinar el punto de acceso inalámbrico físico asociado; y
crear un mapa topológico de la red que refleje la relación entre cada uno de la pluralidad de dispositivos inalámbricos y el punto de acceso inalámbrico físico respectivamente asociado.

2,- El procedimiento de la reivindicación 1, que comprende, además:

definir un valor métrico preferido asociado con un dispositivo inalámbrico; detectar los dispositivos inalámbricos, incluyendo determinar un valor métrico real,
y
comparar el valor métrico determinado con el valor métrico preferido para determinar si el dispositivo inalámbrico está funcionando indebidamente; e informar de si el dispositivo inalámbrico está funcionando indebidamente.

3.- El procedimiento de la reivindicación 2, en el cual el valor métrico preferido es una medición de la potencia de transmisión.

4.- El procedimiento de la reivindicación 2, en el cual el valor métrico es una medición de interferencia aceptable.

5.- El procedimiento de la reivindicación 2, en el cual el valor métrico preferido es un recuento de fragmentación.

6.- El procedimiento de la reivindicación 2, en el cual el valor métrico preferido es una velocidad de transmisión.

7.- El procedimiento de la reivindicación 2, en el cual el valor métrico preferido es un recuento de fallos.

8.- El procedimiento de la reivindicación 1, que comprende, además:

definir una política de seguridad asociada a un dispositivo inalámbrico;
detectar el dispositivo inalámbrico, incluyendo obtener información de seguridad asociada al dispositivo;
determinar que la información de seguridad viola la política de seguridad; e informar de una violación de seguridad.

9.- El procedimiento de la reivindicación 8, en el cual la política de seguridad define una combinación autorizada de identificador de usuario/contraseña, y en el cual la información de seguridad es una combinación no autorizada de identificador de usuario/contraseña.

10.- El procedimiento de la reivindicación 8, en el cual la política de seguridad define un identificador de dispositivo inalámbrico autorizado, y la información de seguridad es un identificador de dispositivo inalámbrico no autorizado.

11.- Un medio legible por ordenador que comprende instrucciones que, cuando se son ejecutadas por un ordenador apropiado, hacen que el ordenador efectúe un procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores.

12.- Un aparato para gestionar un dispositivo inalámbrico en una red, comprendiendo el aparato:

medios para identificar una pluralidad de puntos de una pluralidad de puntos de acceso inalámbricos lógicos autorizados dentro de una red;
medios para detectar una pluralidad de puntos de acceso inalámbricos físicos dentro de la red;
medios para determinar, para cada uno de la pluralidad de puntos de acceso inalámbricos físicos, si el punto de acceso inalámbrico físico está asociado con uno de la pluralidad de puntos de acceso inalámbricos lógicos autorizados; y
medios para informar de cada punto de acceso inalámbrico físico que no está asociado con un punto de acceso inalámbrico lógico autorizado.

caracterizado porque el aparato comprende, además:

medios para detectar una pluralidad de dispositivos inalámbricos, incluyendo determinar el punto de acceso inalámbrico físico asociado; y
medios para crear un mapa topológico de la red que refleje la relación entre cada uno de la pluralidad de dispositivos inalámbricos y el punto de acceso inalámbrico físico respectivamente asociado.

13.- El aparato de la reivindicación 12, que comprende, además:

medios para definir un valor métrico asociado con un dispositivo inalámbrico;
medios para detectar loa dispositivos inalámbricos, incluyendo determinar un valor métrico real; y
medios para comparar el valor métrico determinado con el valor métrico preferido para determinar si el dispositivo inalámbrico está funcionando indebidamente; y
medios para informar de si el dispositivo inalámbrico está funcionando indebidamente.

14.- El aparato de la reivindicación 13, en el cual el valor métrico preferido es una medición de la potencia de transmisión, una medición de interferencia aceptable, un recuento de fragmentación, una velocidad de transmisión o un recuento de fallos.

15.- El aparato de la reivindicación 12, que comprende, además:

medios para definir una política de seguridad asociada a un dispositivo inalámbrico;
medios para detectar el dispositivo inalámbrico, incluyendo obtener información de seguridad asociada al dispositivo;
medios para determinar que la información de seguridad viola la política de seguridad; y
medios para informar de una violación de seguridad.

16.- El aparato de la reivindicación 15, en el cual la política de seguridad define una combinación autorizada de identificador de usuario/contraseña, y en el cual la información de seguridad es una combinación no autorizada de identificador de usuario/contraseña.

17.- El aparato de la reivindicación 15, en el cual la política de seguridad define un identificador de dispositivo inalámbrico autorizado, y la información de seguridad es un identificador de dispositivo inalámbrico no autorizado.

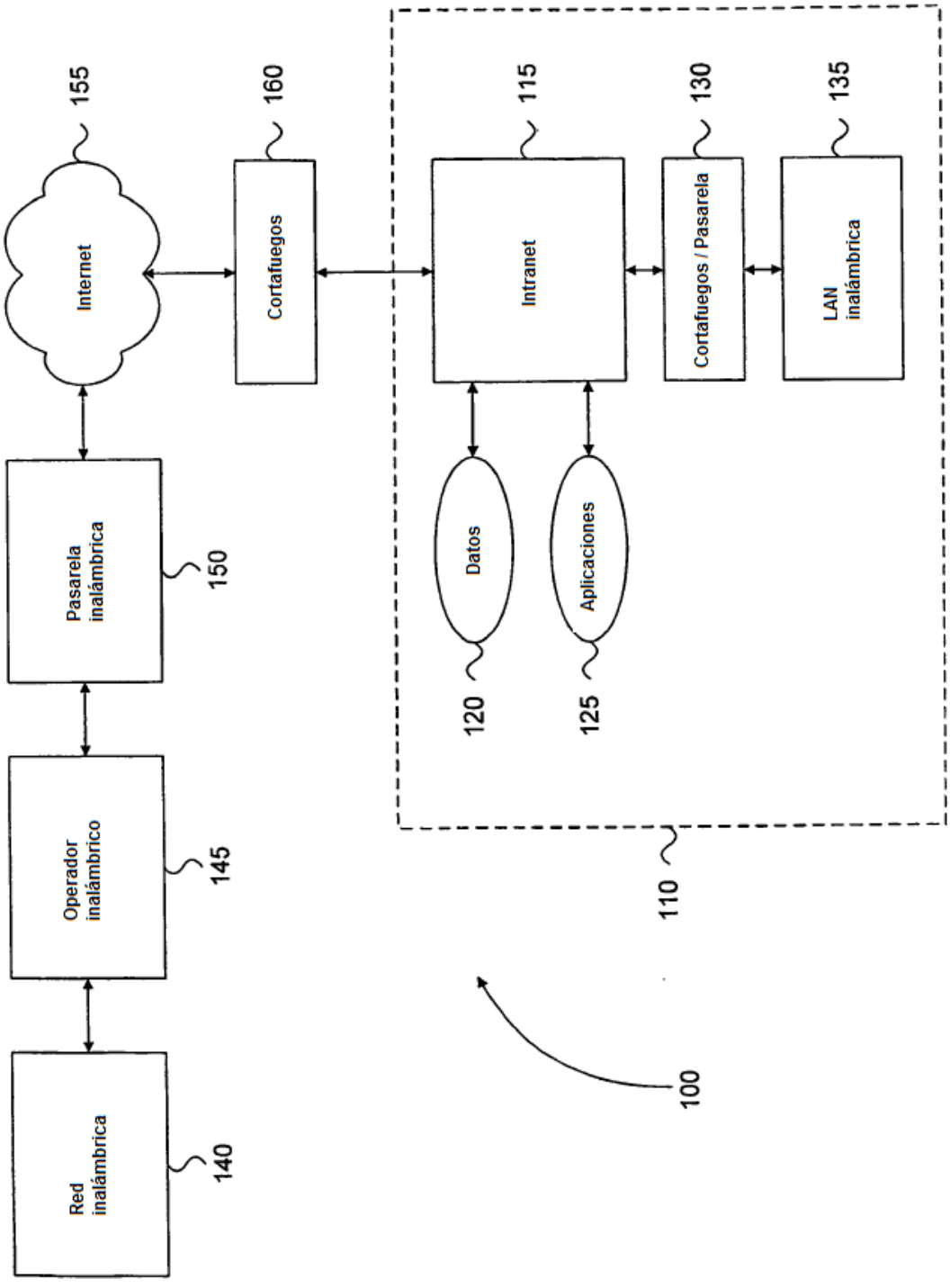
155
160
115
130
135
Internet
Cortafuegos
Intranet
Cortafuegos / Pasarela
LAN inalámbrica
Pasarela inalámbrica
150
Datos
Aplicaciones
120
125
Operador inalámbrico
145
110
Red inalámbrica
140
100

Figura 1

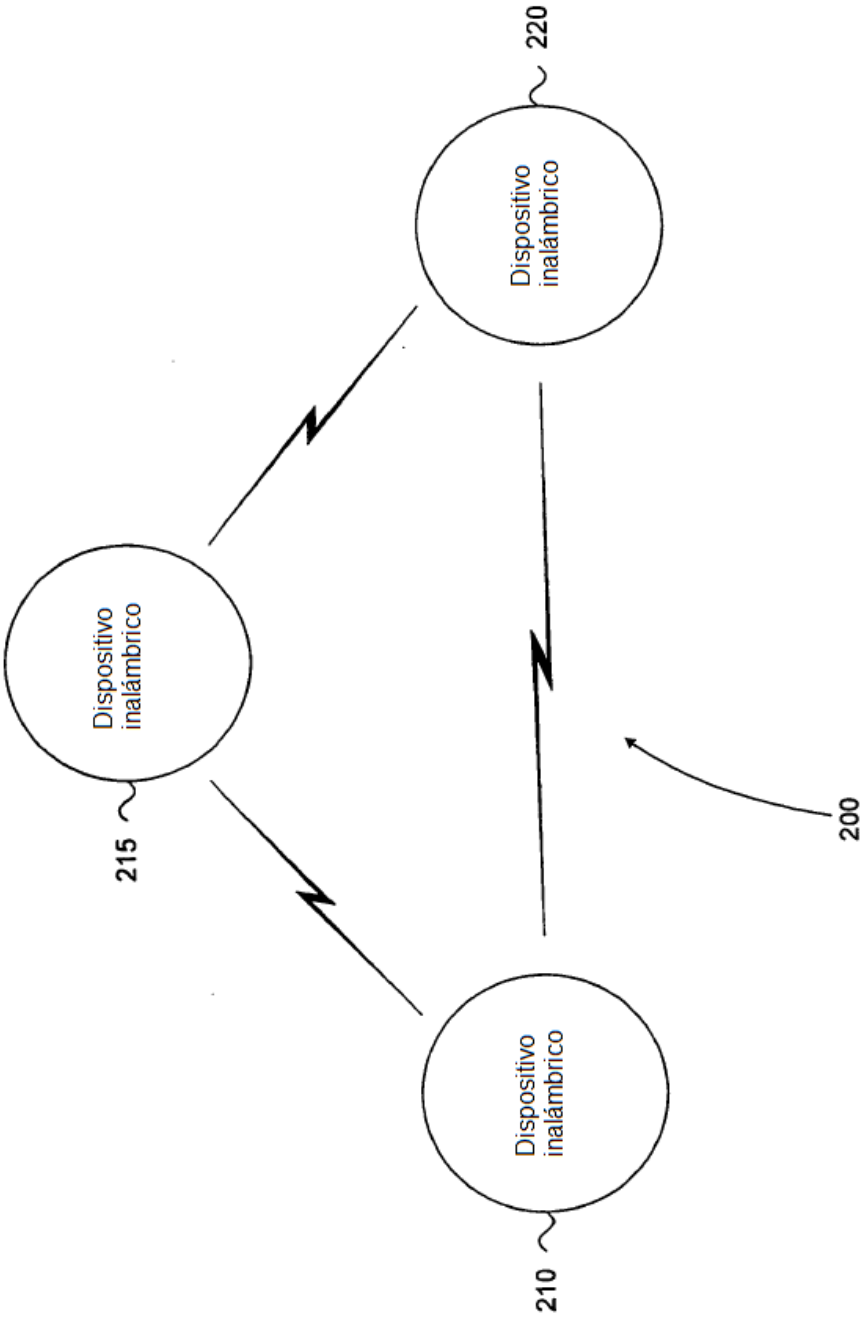
220
Dispositivo inalámbrico
Dispositivo inalámbrico
215
Dispositivo inalámbrico
210
200

Figura 2

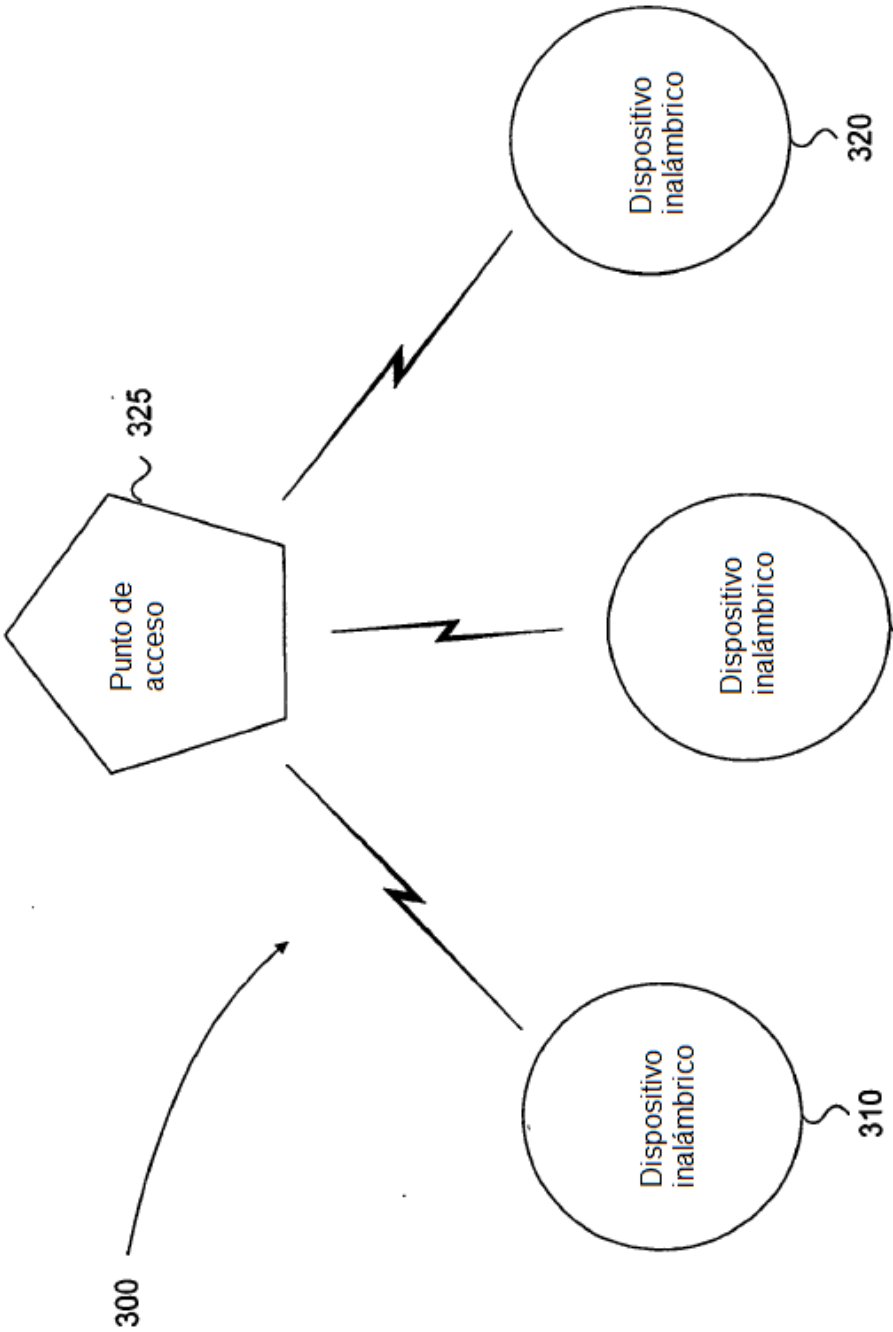
300
Punto de acceso
325
Dispositivo inalámbrico
310
Dispositivo inalámbrico
315
Dispositivo inalámbrico
320

Figura 3

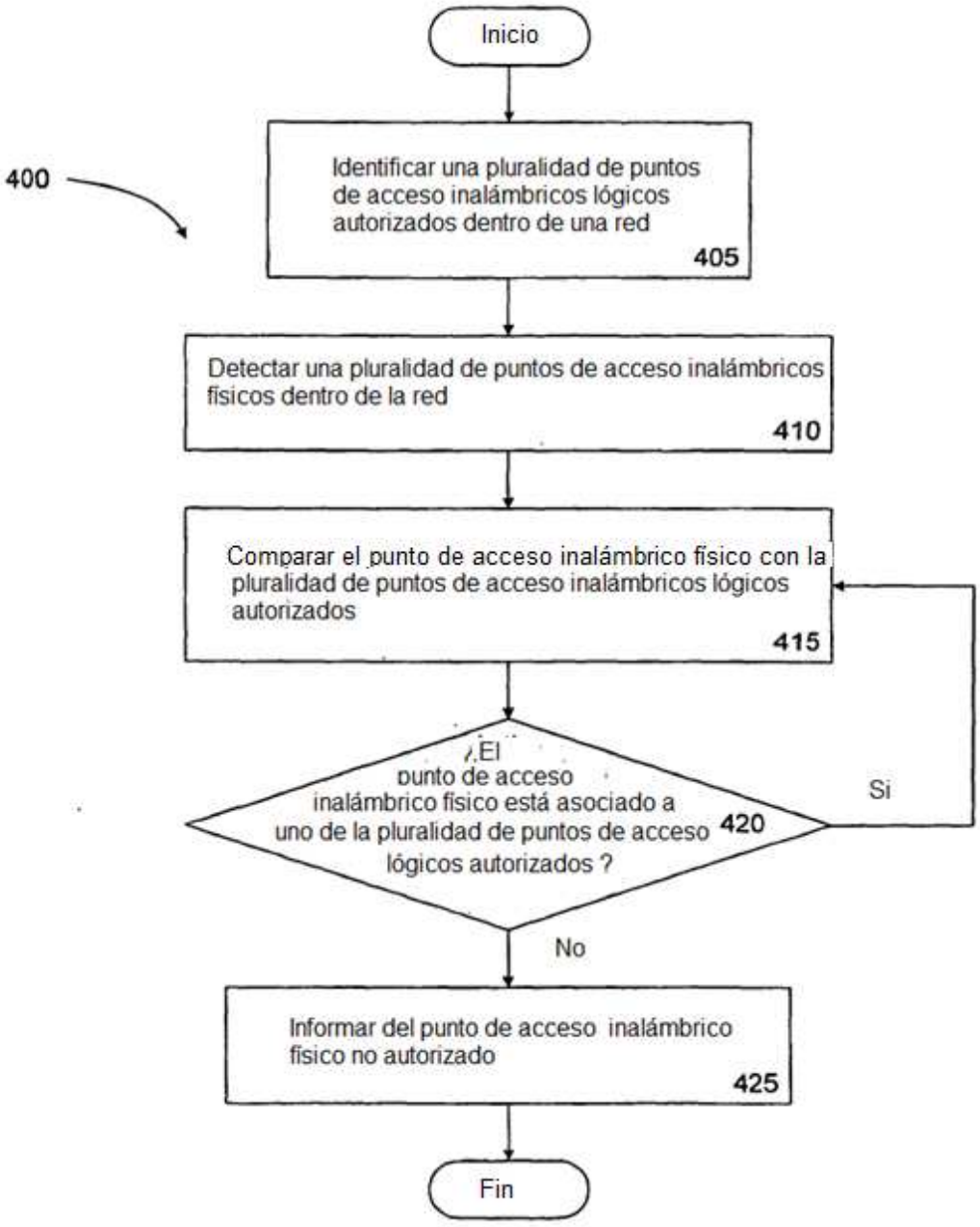
Inicio
400
Identificar una pluralidad de puntos de acceso inalámbricos lógicos autorizados dentro de una red
405
Detectar una pluralidad de puntos de acceso inalámbricos físicos dentro de la red
410
Comparar el punto de acceso inalámbrico físico con la pluralidad de puntos de acceso inalámbricos lógicos autorizados
415
¿El punto de acceso inalámbrico físico está asociado a uno de la pluralidad de puntos de acceso lógicos autorizados ?
420
Si
No
Informar del punto de acceso inalámbrico físico no autorizado
425
Fin

Figura 4

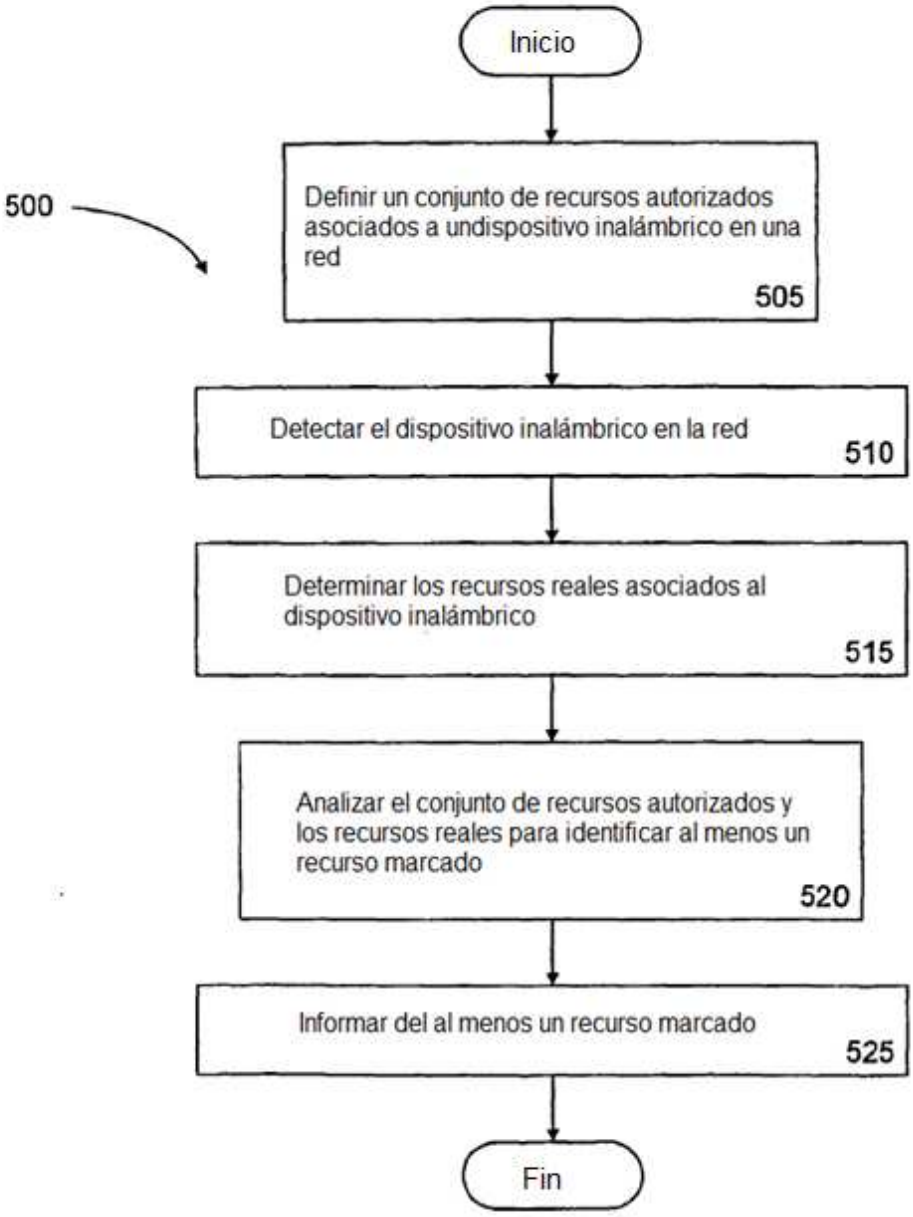
Inicio
500
Definir un conjunto de recursos autorizados asociados a undispositivo inalámbrico en una red
505
Detectar el dispositivo inalámbrico en la red
510
Determinar los recursos reales asociados al dispositivo inalámbrico
515
Analizar el conjunto de recursos autorizados y los recursos reales para identificar al menos un recurso marcado
520
Informar del al menos un recurso marcado
525
Fin

Figura 5

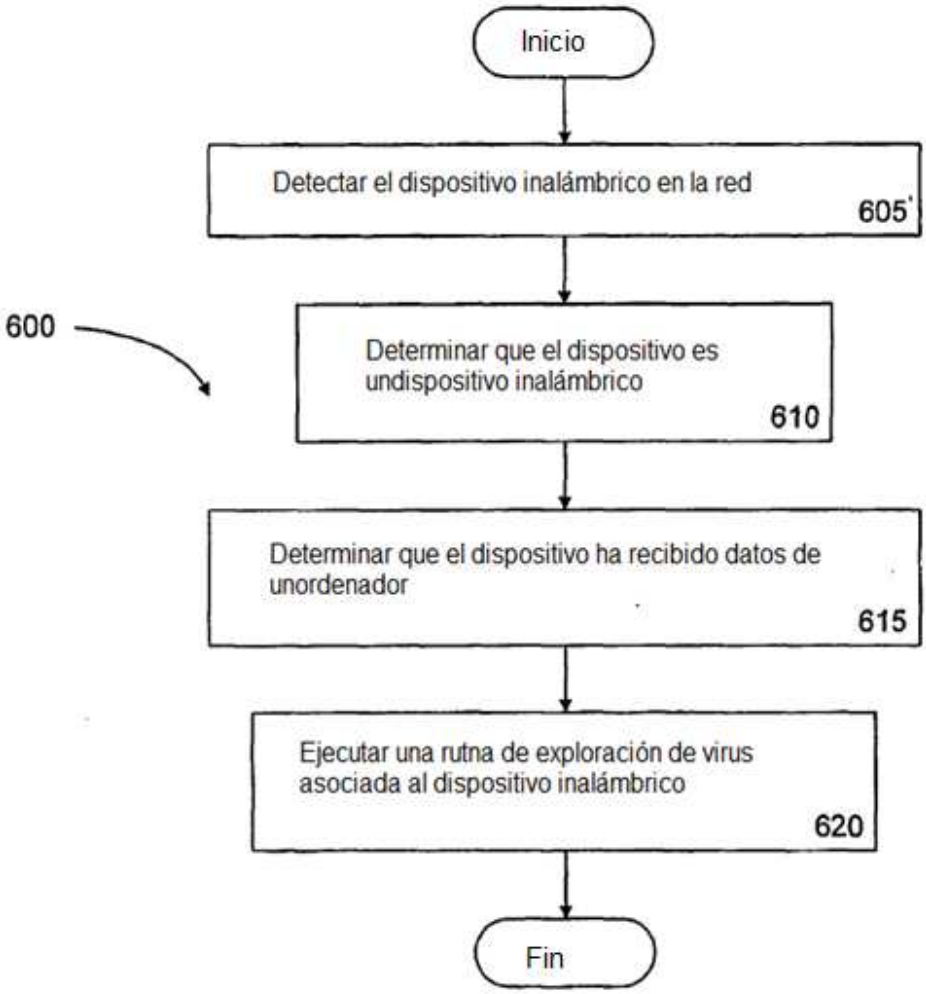
Inicio
Detectar el dispositivo inalámbrico en la red
605
600
Determinar que el dispositivo es undispositivo inalámbrico
610
Determinar que el dispositivo ha recibido datos de unordenador
615
Ejecutar una rutna de exploración de virus asociada al dispositivo inalámbrico
620
Fin

Figura 6

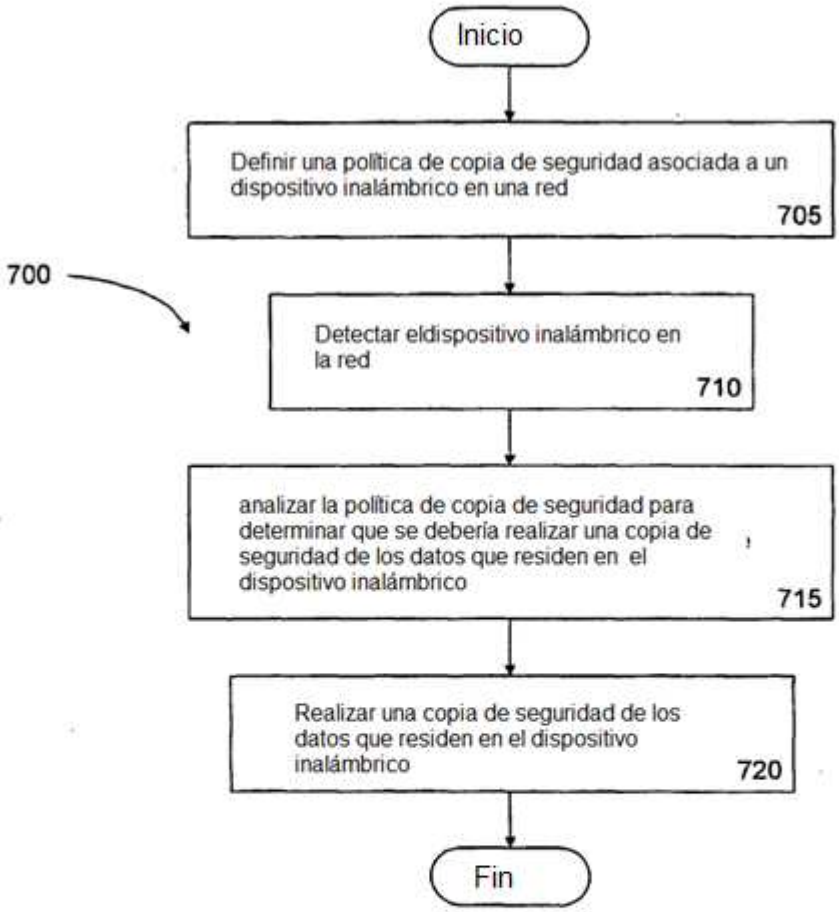
Inicio
Definir una política de copia de seguridad asociada a un dispositivo inalámbrico en una red
705
700
Detectar eldispositivo inalámbrico en la red
710
analizar la política de copia de seguridad para determinar que se debería realizar una copia de seguridad de los datos que residen en el dispositivo inalámbrico
715
Realizar una copia de seguridad de los datos que residen en el dispositivo inalámbrico
720
Fin

Figura 7