(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 389 651**

(51) Int. CI.:

H04W 48/16 (2009.01)
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04025545 .7**
(96) Fecha de presentación: **27.10.2004**
(97) Número de publicación de la solicitud: **1538780**
(97) Fecha de publicación de la solicitud: **08.06.2005**

(54) Título: **Detección automática del tipo de red inalámbrica**

(30) Prioridad:
05.12.2003 US 729209

(45) Fecha de publicación de la mención BOPI:
30.10.2012

(45) Fecha de la publicación del folleto de la patente:
30.10.2012

(73) Titular/es:
MICROSOFT CORPORATION (100.0%)
ONE MICROSOFT WAY
REDMOND, WA 98052, US

(72) Inventor/es:
KRANTZ, ANTON W.;
PALEKAR, ASHWIN;
DUPLESSIS, JEAN-PIERRE;
ALAM, MOHAMMAD SHABBIR;
LYNDERSAY, SEAN O. y
MOORE, TIMOTHY M.

(74) Agente/Representante:
CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Detección automática del tipo de red inalámbrica

Campo técnico

La presente invención versa en general sobre la comunicación en redes inalámbricas y, más en particular, sobre un sistema y un procedimiento que facilitan la detección automática del tipo de una red inalámbrica.

Antecedentes de la invención

Los dispositivos de ordenador que llevan a cabo comunicaciones de red por enlaces inalámbricos se están volviendo crecientemente populares. Convencionalmente, cuando un usuario entra en el alcance de una red inalámbrica, el dispositivo cliente (por ejemplo, un sistema de ordenador) es capaz de discernir dos informaciones sobre esa red sin conectarse con ella (por ejemplo, a partir de la baliza de la red inalámbrica): (1) el identificador del conjunto de servicio (SSID) de la red (por ejemplo, esencialmente, su nombre); y (2) si la red cifra los datos o no. Si la red emplea cifrado, se requiere una clave de cifrado. La clave de cifrado puede ser introducida manualmente por el usuario y/o ser enviada según el protocolo 802.1x.

Con la información que el dispositivo cliente puede recuperar de la baliza de red inalámbrica, generalmente el dispositivo cliente puede determinar si la red es de tipo sin cifrado, cifrado o, con la adición de un elemento de información de acceso protegido de fidelidad inalámbrica (WPA), cifrado usando una clave WPA compartida de antemano o cifrado usando WPA. Si está sin cifrar, entonces un usuario solo tiene que reconocer que la red es insegura y que desea usarla a pesar de esa información. Sin embargo, si está cifrada y no usa WPA, entonces requiere que el usuario introduzca una clave WEP, o bien es una red habilitada para 802.1x que distribuye la clave WEP automáticamente (requiriendo que el ordenador cliente habilite la autenticación 802.1x para completar la conexión).

Dado que el ordenador cliente no puede saber si la red cifrada sin WPA requiere que el usuario introduzca una clave WEP o si es una red habilitada para 802.1x que no soporta WPA, típicamente solicita que el usuario introduzca información. En la vasta mayoría de los casos, el usuario no está en condiciones, desde la perspectiva de un conocimiento técnica, de responder a tal solicitud.

Además, el documento US 2003 / 163558 A1 describe una técnica para que un operador monitorice los servicios de una red de acceso disponibles para un dispositivo final, comunicándose el dispositivo final en un entorno de redes heterogéneas. Se describe que diferentes redes de acceso están disponibles para el dispositivo final con base en una ubicación del dispositivo final y en el momento en el que la red está siendo objeto de acceso. Un usuario del dispositivo final puede desear acceder a una red particular dependiendo de las redes de acceso disponibles. Para determinar qué redes de acceso están disponibles, un operario da la instrucción al dispositivo final para que determine redes de acceso disponibles situadas dentro del entorno de redes heterogéneas. La información de las redes de acceso es recogida desde al menos un nodo dentro de la red heterogénea y es puesta a disposición del operario. Después, la red de acceso puede ser proporcionada al dispositivo final según la información recogida. Se describe que la determinación puede usarse para seleccionar una red de acceso disponible para el usuario con base, por ejemplo, en la normativa de contrato de abonados. Los resultados también pueden ser usados para llevar a cabo hiperconmutaciones, es decir, una transferencia sustancialmente sin fisuras entre dos tipos de redes de acceso, tales como de una red celular a una LAN inalámbrica. Además, el documento US 2003 / 204748 describe una técnica para la identificación del protocolo particular de seguridad para acceder a cada red que se encuentre un usuario de un dispositivo portátil. Si se requiere un protocolo de seguridad para una red y el usuario tiene la clave apropiada de seguridad, el sistema está configurado, además, para identificar esa clave. El sistema está configurado para determinar si una red dentro del alcance del dispositivo requiere cifrado y, en tal caso, a qué nivel. Si se requiere cifrado, los sistemas acceden a un perfil de red para determinar si el usuario posee una clave para el uso en la red particular. Se describe que un receptor recibe transmisiones de transmisores en las inmediaciones del receptor. Un detector de red está configurado para detectar transmisiones de redes recién encontradas, por ejemplo detectando nuevas señales piloto de una red. Se describe adicionalmente que el detector está configurado para proporcionar a un controlador un identificador, nominalmente el SSID, de la red. Además, también se describe que el detector está configurado para proporcionar una indicación de si la red es segura. En el paradigma de una red 802.11b, la indicación de seguridad la proporciona la bandera de privacidad equivalente a la cableada (WEP).

Por lo tanto, es el objeto de la presente invención proporcionar procedimientos y sistemas mejoradas para la gestión de la comunicación con redes inalámbricas.

Este problema objetivo es resuelto por la materia de las reivindicaciones independientes.

Las realizaciones preferentes son el objeto de las reivindicaciones dependientes.

Lo que sigue presenta un resumen simplificado de la invención para proporcionar una comprensión básica de algunos aspectos de la invención. Este resumen no es un una visión general amplia de la invención. no se propone

identificar elementos clave/críticos de la invención ni delinear el alcance de la invención. Su único propósito es presentar algunos conceptos de la invención de forma simplificada como preludio de la descripción más detallada que se presenta después.

La presente invención proporciona un sistema y un procedimiento que facilitan la detección automática del tipo de una red inalámbrica. Según un aspecto de la presente invención, el o los clientes de la red inalámbrica pueden detectar automáticamente el "tipo" de una red sin requerir indicaciones del usuario. El este contexto, el "tipo" se refiere al procedimiento de autenticación y cifrado que requiere la red (por ejemplo, redes no cifradas que no requieren autenticación alguna, redes cifradas que requieren que el usuario introduzca una clave WEP, redes cifradas que soportan autenticación 802.1x, redes con acceso de fidelidad inalámbrica (WPA) que requieren que el usuario introduzca una clave WPA compartida de antemano, redes habilitadas para 802.1x que sí soportan WPA y/o redes que soportan servicios de dotación inalámbrica). Así, el sistema emplea una técnica para determinar de forma eficiente y segura a cuáles tipos de red está intentando conectarse el usuario, permitiendo con ello que el sistema operativo presente al usuario una interfaz apropiada de usuario. Por ejemplo, el sistema puede proporcionar una manera de distinguir si la red inalámbrica requiere una autenticación (1) de clave WP o (2) 802.1x.

Según otro aspecto de la presente invención, se proporciona un sistema de detección de redes inalámbricas que tiene un componente de conexión y un componente de detección. El componente de conexión facilita la conexión de un sistema cliente con al menos una de una pluralidad de redes inalámbricas. El componente de detección identifica el tipo de una red inalámbrica disponible.

En un ejemplo, la identificación por parte del componente de detección puede estar basada, al menos en parte, en la recepción de un elemento específico de información procedente de una baliza de red inalámbrica. En otro ejemplo, el componente de detección sondea iterativamente la baliza de la red inalámbrica en conexión con la identificación del tipo de la red inalámbrica.

Por ejemplo, el componente de detección puede primero intentar conectarse con la red inalámbrica como si fuese una red que soporta servicios de dotación inalámbrica (WPS). Esperando ciertos tipos de fallo(s) en la secuencia de autenticación, el componente de detección puede determinar si la red requiere que el usuario introduzca una clave WEP.

Si no se observan los fallos, el componente de detección puede esperar un periodo de tiempo mayor (por ejemplo, hasta treinta segundos) una sección particular de la secuencia de autenticación (por ejemplo, protocolo de autenticación extensible protegido – tipo-longitud-valor (PEAP-TLV)) que identifique una red WPS. En ausencia de esta sección de la secuencia, el componente de detección puede identificar ante el componente de conexión a la red inalámbrica como una red habilitada para 802.1x. Si el componente de detección detecta la sección particular de la secuencia de autenticación, el componente de detección puede identificar ante el componente de conexión a la red como una red que soporta WPS.

En consecuencia, no se pide que el usuario determine el tipo de red. Esto puede llevar, por ejemplo, a usuarios que tengan más éxito en su uso de redes inalámbricas y a reducir más la frustración de los usuarios con la o las redes inalámbricas.

Para el logro de los fines precedentes y relacionados, en el presente documento se describen ciertos aspectos ilustrativos de la invención en conexión con la siguiente descripción y con los dibujos adjuntos. Sin embargo, estos aspectos son indicativos únicamente de algunas de las diversas maneras en las que pueden emplearse los principios de la invención, y se pretende que la presente invención incluya la totalidad de tales aspectos y sus equivalentes. Otras ventajas y características novedosas de la invención pueden hacerse evidentes a partir de la siguiente descripción detallada de la invención cuando se la considera en unión de los dibujos.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de bloques de un sistema de detección de redes inalámbricas según un aspecto de la presente invención.
La Fig. 2 es un diagrama de bloques de tipos ejemplares de redes inalámbricas según un aspecto de la presente invención.
La Fig. 3 es un diagrama de flujo de un procedimiento que facilita la detección de redes inalámbricas según un aspecto de la presente invención.
La Fig. 4 es un diagrama de flujo de un procedimiento que facilita la detección de redes inalámbricas según un aspecto de la presente invención.
La Fig. 5 es un diagrama de flujo que ilustra adicionalmente el procedimiento de la Fig. 4.
La Fig. 6 ilustra un entorno operativo ejemplar en el que la presente invención puede funcionar.

Descripción detallada de la invención

Ahora se describe la presente invención con referencia a los dibujos, en los que se usan números de referencia semejantes para referirse a elementos semejantes de principio a fin. En la siguiente descripción, con fines

explicativos, se definen numerosos detalles específicos para proporcionar una comprensión cabal de la presente invención. sin embargo, puede ser evidente que la presente invención puede ser puesta en práctica sin estos detalles específicos. En otros casos, estructuras y dispositivos bien conocidos son mostrados en forma de diagrama de bloques para facilitar la descripción de la presente invención.

Tal como se usan en la presente solicitud, los términos “componente”, “controlador”, “modelo”, “sistema” y similares están pensados para referirse a una entidad relacionada con los ordenadores, ya sea soporte físico, una combinación de soporte físico y soporte lógico, soporte lógico o soporte lógico en ejecución. Por ejemplo, un componente puede ser, sin limitación, un proceso que se ejecute en un procesador, un procesador, un objeto, un ejecutable, un hilo de ejecución, un programa y/o un ordenador. A título de ilustración, tanto una aplicación que se ejecute en un servidor como el servidor pueden ser un componente. Uno o más componentes pueden residir dentro de un proceso y/o un hilo de ejecución, y un componente puede estar localizado en un ordenador y/o estar distribuido entre dos o más ordenadores. Además, estos componentes pueden ejecutarse desde diversos medios legibles por ordenador que tengan diversas estructuras de datos almacenadas en los mismos. Los componentes pueden comunicarse por medio de procesos locales y/o remotos, tales como según una señal que tenga uno o más paquetes de datos (por ejemplo, datos procedentes de un componente que interactúa con otro componente en un sistema local, un sistema distribuido y/o en una red como Internet con otros sistemas a través de la señal). Los componentes de ordenador pueden estar almacenados, por ejemplo, en medios legibles por ordenador que incluyen, sin limitación, un ASIC (circuito integrado para aplicaciones específicas), un CD (disco compacto), un DVD (disco de vídeo digital), una ROM (memoria de solo lectura), disquete, disco duro, una EEPROM (memoria de solo lectura programable borrable eléctricamente) y una tarjeta de memoria según la presente invención.

Con referencia a la Fig. 1, se ilustra un sistema 100 de detección de redes inalámbricas según un aspecto de la presente invención. El sistema 100 puede facilitar la detección automática de un tipo de red inalámbrica por parte de un cliente (por ejemplo, sin requerir indicaciones de un usuario).

El “tipo” de una red inalámbrica se refiere generalmente a la clase de autenticación y cifrado que requiere la red. En un ejemplo, las redes inalámbricas pueden dividirse en seis tipos:

(1) Redes no cifradas (por ejemplo, abiertas), que generalmente no requieren autenticación alguna.
(2) Redes cifradas con privacidad equivalente a la cableada (WEP), en las que el usuario precisa introducir una clave WEP.
(3) Redes cifradas de acceso protegido de fidelidad inalámbrica (WPA), en las que el usuario precisa introducir una clave WPA compartida de antemano (WPAPSK)
(4) Redes habilitadas para 802.1x que no soportan WPA.
(5) Redes habilitadas para 802.1x que sí soportan WPA.
(6) Redes habilitadas con soporte de servicios de dotación inalámbrica (WPS) que soportan WPA o no.

El conjunto de estándares IEEE 802.11 define dos tipos de redes: las redes cifradas (por ejemplo, las redes WEP) y las redes no cifradas. Debido a las debilidades bien conocidas del protocolo WEP, la industria inalámbrica implementó el soporte para el estándar IEEE 802.1x como mecanismo para abordar las deficiencias clave en el protocolo WEP, siendo ellas la autenticación del usuario, la gestión de la clave de cifrado y la distribución de la clave de cifrado. Para las redes cifradas con WEP, el usuario precisa proporcionar una clave de cifrado, y para las redes habilitadas para 802.1x la clave es proporcionada automáticamente si el usuario tiene una credencial válida (por ejemplo, tal como un certificado digital o un nombre de usuario y una contraseña). Para las redes 802.11 que están cifradas, esto presenta un problema de utilización, ya que en la actualidad no es posible determinar a priori si el usuario precisa introducir una clave WEP o si la red soporta 802.1x, en cuyo caso no tiene que introducirla.

Para abordar las debilidades subyacentes al algoritmo WEP, que se ha demostrado que es criptográficamente débil, se introdujo una mejora de seguridad en el conjunto de estándares 802.11, denominado acceso protegido de fidelidad inalámbrica (WPA). El WPA también aborda algunos de los problemas de utilización del estándar 802.11 original especificando un elemento de información que los puntos de acceso habilitados para WPA incluyen en la trama de su baliza. Este elemento de información describe, entre otros, si la red requiere que el usuario introduzca la clave de cifrado, denominado modo de clave WPA compartida de antemano (WPA-PSK), o si la clave es proporcionada automáticamente en virtud de la credencial del usuario, denominado “modo WPA”.

Privacidad equivalente a la cableada

La WEP es definida por el estándar IEEE 802.11 y está pensada para proporcionar un nivel de confidencialidad de los datos que es equivalente a una red cableada. Debido a la naturaleza de las redes LAN inalámbricas, implementar una infraestructura de seguridad que monitorice el acceso físico a la red puede resultar difícil. A diferencia de una red cableada, en la que se requiere la conexión física, es concebible que cualquiera dentro del alcance de un punto de acceso (AP) inalámbrico pueda enviar y recibir tramas, así como estar a la escucha de otras tramas que se envíen. Esto hace que la intercepción y el espionaje remoto de tramas de LAN inalámbricas resulten muy fáciles.

La WEP proporciona servicios de confidencialidad de datos mediante el cifrado de los datos enviados entre nodos inalámbricos. Se indica el cifrado WP para una trama 802.11 poniendo una bandera WEP en la cabecera MAC de la trama 802.11. La WEP proporciona integridad de datos para errores aleatorios incluyendo un valor de comprobación de la integridad (ICV) en la porción cifrada de la trama inalámbrica.

La siguiente tabla ilustra las dos claves compartidas que la WEP define:

TABLA 1

Tipo de clave	Descripción
Clave de multidifusión/global	Clave de cifrado que contribuye a proteger el tráfico de multidifusión y radiodifusión desde un AP inalámbrico a todos sus clientes inalámbricos conectados.
Clave de sesión de unidifusión	Clave de cifrado que contribuye a proteger el tráfico de unidifusión entre un cliente inalámbrico y un AP inalámbrico y el tráfico de multidifusión y radiodifusión enviado por un cliente inalámbrico al AP inalámbrico.

El cifrado WEP emplea el cifrador RC4 de flujo simétrico con claves de cifrado de 40 bits y 104 bits.

Acceso protegido de fidelidad inalámbrica

El WPA es un estándar de fidelidad inalámbrica diseñado para mejorar las características de seguridad la WEP. A diferencia de la WEP, en el WPA se requiere la autenticación 802.1x. Con el WPA, se requiere la regeneración de clave tanto de la clave de cifrado de unidifusión como de la global. Para la clave de cifrado de unidifusión, el protocolo de integridad de clave temporal (TKIP) cambia la clave de cada trama, y el cambio se sincroniza entre el cliente inalámbrico y el punto de acceso (AP) inalámbrico. Para la clave de cifrado global, el WPA incluye un sistema para que el AP inalámbrico anuncie la clave cambiada a los clientes inalámbricos conectados.

El TKIP sustituye a la WEP con un algoritmo de cifrado que es más fuerte que el algoritmo WEP. El TKIP también permite la verificación de la configuración de seguridad después de que se determinan las claves de cifrado; el cambio sincronizado de la clave de cifrado de unidifusión para cada trama; y la determinación de una clave inicial única de cifrado de unidifusión para cada autenticación de clave compartida de antemano.

El WPA emplea, además, un procedimiento denominado “Michael”, que especifica un algoritmo que calcula un código de integridad de mensajes (MIC) de 8 bytes. El MIC se sitúa entre la porción de datos de la trama IEEE 802.11 y el valor de comprobación de la integridad (ICV) de 4 bytes. El campo MIC se cifra junto con los datos de la trama y el ICV.

El WPA es un estándar provisional que será sustituido con el estándar 802.11i de IEEE tras su finalización.

Redes que soportan servicios de dotación inalámbrica (WPS)

Los WPS permiten que los proveedores y/o las empresas de redes de fidelidad inalámbrica envíen información de dotación y configuración a un cliente móvil cuando se conecta a Internet o a una red empresarial, proporcionando dotación y configuración sin fisuras y automáticas del cliente con una experiencia uniforme de registro. Cuando un usuario inicia sesión en una red inalámbrica, la red reconoce al usuario, establece automáticamente la sesión y factura a la cuenta del usuario.

La seguridad de una sesión inalámbrica mejora porque la autenticación automática y el cifrado proporcionados por los WPS minimizan la probabilidad de que la sesión inalámbrica de un usuario sea forzada por puntos de acceso fraudulentos o por piratas informáticos. Con los WPS, una red puede solicitar del usuario sustancialmente cualquier tipo de información, por ejemplo, un nombre de usuario, un código de descuento y/o información demográfica.

Diferencias entre tipos ejemplares de redes inalámbricas

Pasando brevemente a la Fig. 2, se ilustra un diagrama 200 de tipos ejemplares de redes inalámbricas según un aspecto de la presente invención.

Las redes inalámbricas abarcadas por la especificación original 210 de 802.11 incluyen la cifrada 214 y la no cifrada 216. La especificación 802.1x facilitó, además, la distribución automática de la clave 222 de cifrado WEP y la autenticación 224 de 802.1x. la introducción de los WPS permite, además, que la autenticación 224 de 802.1x se subdivida en una o más redes 242 que soportan WPS y una o más redes 244 que no soportan WPS.

Alternativamente, la introducción de la especificación WPA permitió una red inalámbrica que soportaba la especificación 802.11 y que, además, abarcaba la especificación 230 de WPA. Esta red o estas redes 234 están cifradas y pueden subdividirse en WPA 236 (por ejemplo, redes habilitadas para 802.1x que soportan WPA) y WPA PSK 238. Con la introducción de los WPS, el nodo 236 de WPA puede ser subdividido adicionalmente en una o más redes 252 que soportar WPS y una o más redes 254 que no soportan WPS.

El sistema 100 de detección de redes inalámbricas

Volviendo a la Fig. 1, el sistema 100 de detección de redes inalámbricas incluye un componente 110 de conexión y un componente 120 de detección. El componente de conexión facilita la conexión de un sistema cliente 130 con al menos uno de una pluralidad de tipos de redes inalámbricas. El componente 120 de detección puede sondear iterativamente una baliza 140 de red inalámbrica disponible en conexión con la identificación del tipo de la red inalámbrica. Por ejemplo, el sistema 100 puede emplear una técnica de sondeo para determinar el tipo de red de una red "nueva" la primera vez que el usuario intente conectarse con ella. Además y/o alternativamente, el sistema 100 puede emplear un elemento de información procedente de la baliza 140 de la red inalámbrica para facilitar la determinación del tipo de red.

Convencionalmente, tal como se ha expuesto previamente, cuando un usuario está dentro del alcance de una red inalámbrica, el ordenador cliente es capaz de discernir dos informaciones sobre la red sin conectarse con ella (por ejemplo, a partir de la baliza de la red inalámbrica): (1) el SSID de la red (por ejemplo, esencialmente, su nombre); y (2) si la red cifra los datos o no. Si la red emplea cifrado, se requiere una clave de cifrado. La clave de cifrado puede ser introducida manualmente por el usuario y/o a través del protocolo 802.1x. Así, para cada uno de los tipos de red, la información que el ordenador cliente requiere del usuario puede ser diferente.

Sin embargo, con la información que el ordenador puede recuperar de la baliza de red, el ordenador solo puede determinar sin la red es (a) no cifrada (tipo nº 1) o (b) cifrada (tipo nº 2 o nº 4) o, con la adición del elemento de información de WPA, cifrada usando WPA-PSK (tipo nº 3) o cifrada usando WPA (tipo nº 5).

Si está sin cifrar (por ejemplo, el tipo nº 1), el usuario puede reconocer que la red es insegura y que desea usarla a pesar de esa información. Sin embargo, si está cifrada y no usa WPA, entonces es o bien del tipo nº 2 o del nº 4. Si es del tipo nº 2, el usuario tendría que introducir una clave WEP, y si es del tipo nº 4 el usuario no tendría que introducir una clave WEP, pero es preciso que el ordenador cliente habilite la autenticación 802.1x para completar la conexión. Dado que el ordenador cliente no puede saber si la red es la nº 2 o la nº 4, esencialmente tiene que preguntar al usuario. En la vasta mayoría de los casos, el usuario no está en posición (desde una perspectiva del conocimiento técnico) de responder tal pregunta. La introducción de la o las redes WPS ha vuelto la situación aún más complicada (por ejemplo, tres tipos diferentes de redes cifradas).

El sistema 100 de detección de redes inalámbricas determina con eficiencia y seguridad a cuál de una pluralidad de tipos de red está intentando conectarse el usuario para presentar al usuario una interfaz de usuario (UI) apropiada. Tal como se ha hecho notar previamente, para cada uno de los tipos de red, la información que el ordenador cliente precisa del usuario puede ser diferente. Así, el sistema 100 puede proporcionar una manera de distinguir si la red inalámbrica requiere (1) una clave WEP introducida manualmente o (2) autenticación 802.1 sin una indicación significativa del usuario.

En un ejemplo, el sistema 100 emplea un elemento de información (IE) procedente de la baliza 140 de la red inalámbrica para facilitar la determinación del tipo de red. El concepto general de un IE forma parte del estándar 802.11. Según un aspecto de la presente invención, puede usarse un IE específico, por ejemplo, dos bits, para proporcionar información para distinguir entre los tipos de red (por ejemplo, tres). La siguiente tabla ilustra la estructura y el diseño de un IE ejemplar:

TABLA 2

Nombre	Valor	Tamaño (octetos)	Descripción
ID del elemento	0xDD	1	
Longitud	11	1	
OUI	0x00:50:f2	3	
Tipo de OUI	5	1	
WPS soportado	Verdadero/Falso	1	Indica si la red soporta servicios de dotación inalámbrica
802.1X requerido	Verdadero/Falso	1	Para redes WEP (no WPA), indica si se requiere 802.1X

En este ejemplo, la baliza 140 de la red inalámbrica proporciona el IE al componente 120 de detección. Con base, al menos en parte, en el IE, el componente 120 de detección identifica el tipo de red inalámbrica.

En otro ejemplo, el sistema 100 emplea una técnica de sondeo para determinar el tipo de cifrado de una red, llevada a cabo, por ejemplo, la primera vez que el usuario intenta conectarse a ella. Por ejemplo, el componente 120 de detección puede intentar primero conectarse a la red inalámbrica como si fuese una red WPS. Las redes WPS son un subconjunto de las redes 802.1x (por ejemplo, del tipo nº 4 o el tipo nº 5) y pueden o no soportar WPA. Esperando ciertos tipos de fallos en la secuencia de autenticación, el componente 120 de detección puede determinar si la red es del tipo nº 2 (por ejemplo, una clave WEP introducida manualmente). Por ejemplo, el sondeo puede mitigar el impacto en el usuario al reconocer un tipo común de red (por ejemplo, una clave WEP introducida manualmente).

Si no se observan los fallos, el componente 120 de detección puede esperar un periodo de tiempo mayor (por ejemplo, hasta treinta segundos) una sección particular de la secuencia de autenticación (por ejemplo, protocolo de autenticación extensible protegido – tipo-longitud-valor (PEAP-TLV)) que identifique una red WPS. En ausencia de esta sección de la secuencia, el componente 120 de detección puede identificar ante el componente 110 de conexión a la red inalámbrica como del tipo nº 4 o del tipo nº 5. Si el componente 120 de detección detecta la sección particular de la secuencia de autenticación, el componente 120 de detección puede identificar ante el componente 110 de conexión a la red como una red que soporta WPS.

En consecuencia, no se pide que el usuario determine el tipo de red. Esto puede llevar, por ejemplo, a usuarios que tengan más éxito en su uso de redes inalámbricas y a reducir más la frustración de los usuarios con la o las redes inalámbricas.

Debe apreciarse que el sistema 100 de detección de la red inalámbrica, el componente 110 de conexión, el componente 120 de detección, el sistema cliente 130 y/o la baliza 140 de la red inalámbrica pueden ser componentes de ordenador, según se define ese término en el presente documento.

Pasando brevemente a las Figuras 3-5, se ilustran metodologías que pueden ser implementadas según la presente invención. Aunque, en aras de la simplicidad de la explicación, las metodologías son mostradas y descritas como una serie de bloques, debe entenderse y apreciarse que la presente invención no está limitada por el orden de los bloques, ya que algunos bloques, según la presente invención, pueden darse en órdenes diferentes y/o concurrentemente con otros bloques con respecto a lo mostrado y descrito en el presente documento. Además, pueden no requerirse todos los bloques ilustrados para implementar las metodologías según la presente invención.

La invención puede ser descrita en el contexto general de instrucciones ejecutables por ordenador, tal como módulos de programa, ejecutados por uno o más componentes. En general, los módulos de programa incluyen rutinas, programas, objetos, estructuras de datos, etc. que llevan a cabo tareas particulares o implementan tipos particulares de datos abstractos. Típicamente, la funcionalidad de los módulos de programa puede combinarse o distribuirse según se desee en diversas realizaciones.

Con referencia a la Fig. 3, se ilustra un procedimiento que facilita la detección 300 de redes inalámbricas según un aspecto de la presente invención. En 310, se intenta la conexión con una red inalámbrica como una red WPS. En 320, se efectúa una determinación en cuanto a si la tentativa tuvo éxito. Si la determinación de 320 es NO, en 330, la red inalámbrica es identificada como que requiere una clave WEP y no ocurre ningún procesamiento adicional.

Si la determinación en 320 es SÍ, en 340, se espera hasta un periodo de tiempo umbral (por ejemplo, 30 segundos) la recepción de una sección particular de información de autenticación que identifique una red WPS (por ejemplo, secuencia PEAP - TLV). En 350, se efectúa una determinación en cuanto a si se ha recibido la sección particular de información de autenticación. Si la determinación en 350 es NO, en 360, la red es identificada como del tipo nº 4 o del tipo nº 5 y no ocurre ningún procesamiento adicional. Si la determinación en 350 es SÍ, en 370, la red es identificada como que soporta WPS y no ocurre ningún procesamiento adicional.

A continuación, con referencia a las Figuras 4 y 5, se ilustra un procedimiento que facilita la detección 400 de redes inalámbricas según un aspecto de la presente invención. En 404, se inicia el proceso de conexión. En 408, se efectúa una determinación en cuanto a si la red inalámbrica está cifrada (por ejemplo, con base, al menos en parte, en información recibida de la baliza de la red inalámbrica). Si la determinación en 408 es NO, en 412, la red es identificada como no cifrada. En 416, puede pedirse confirmación de un usuario para que se conecte a una red insegura y no ocurre ningún procesamiento adicional.

Si la determinación en 408 es SÍ, en 420, es efectúa una determinación en cuanto a si la red es WPA (por ejemplo, con base, al menos en parte, en información recibida de la baliza de la red inalámbrica). Si la determinación en 420 es SÍ, en 422, se efectúa una determinación en cuanto a si la red es WPA PSK (por ejemplo, con base, al menos en parte, en información recibida de la baliza de la red inalámbrica). Si la determinación en 422 es SÍ, en 424, la red es identificada como WPA PSK. En 428 puede pedirse que un usuario introduzca una clave WPA compartida de antemano y no ocurre ningún procesamiento adicional. Si la determinación en 422 es NO, el procesamiento continúa en 432.

Si la determinación en 420 es NO, en 432, se efectúa una determinación en cuanto a si la red soporta 802.1x. por ejemplo, tal como se ha expuesto previamente, la determinación puede efectuarse empleando una técnica de sondeo y/o un elemento de información recibido de la baliza de la red inalámbrica. Si la determinación en 432 es NO, en 436, la red identificada como de un tipo WEP manual. En 440 puede pedirse a un usuario que introduzca una clave WEP y no ocurre ningún procesamiento adicional.

Si la determinación en 432 es SÍ, en 444, se efectúa una determinación en cuanto a si la red soporta WPS. De nuevo, la determinación puede efectuarse empleando una técnica de sondeo y/o un elemento de información recibido de la baliza de la red inalámbrica. Si la determinación en 444 es SÍ, en 448, la red es identificada como con soporte de WPS. En 452, puede cargarse la información WPS y continuar la conexión, y no ocurre ningún procesamiento adicional.

Si la determinación en 444 es NO, en 456, la red es identificada como una red 802.1x. En 460, puede continuar la conexión a la red inalámbrica usando un tipo de autenticación 802.1x por defecto y no ocurre ningún procesamiento adicional.

Para proporcionar un contexto adicional para diversos aspectos de la presente invención, la Fig. 6 y la siguiente exposición están pensadas para proporcionar una breve descripción general de un entorno operativo 610 adecuado en el que pueden ser implementados diversos aspectos de la presente invención. Aunque se describe la invención en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutadas por uno o más ordenadores u otros dispositivos, los expertos en la técnica reconocer que la invención también puede ser implementada en combinación con otros módulos de programa y/o como una combinación de soporte físico y soporte lógico. Sin embargo, en general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc. que llevan a cabo tareas particulares o implementadas tipos particulares de datos. El entorno operativo 610 es solo un ejemplo de un entorno operativo adecuado y no se pretende sugerir ninguna limitación en cuanto al alcance del uso o la funcionalidad de la invención. Otros sistemas, entornos y/o configuraciones bien conocidos de ordenadores que pueden ser adecuados para su uso con la invención incluyen, sin limitación, ordenadores personales, dispositivos de mano o portátiles, sistemas multiprocesador, sistemas basados en microprocesadores, electrónica programable de consumo, PC de red, miniordenadores, ordenadores centrales, entornos informáticos distribuidos que incluyen los anteriores sistemas o dispositivos, y similares.

Con referencia a la Fig. 6, un entorno ejemplar 610 para implementar diversos aspectos de la invención incluye un ordenador 612. El ordenador 612 incluye una unidad 614 de proceso, una memoria 616 del sistema y un bus 618 del sistema. El bus 618 del sistema acopla los componentes del sistema, incluyendo, sin limitación, la memoria 616 del sistema a la unidad 614 de proceso. La unidad 614 de proceso puede ser cualquiera de diversos procesadores disponibles. También pueden emplearse microprocesadores duales y arquitecturas multiprocesador como unidad 614 de proceso.

El bus 618 del sistema puede ser cualquiera de varios tipos de estructuras de bus, incluyendo el bus de memoria o controlador de memoria, un bus de periféricos o bus externo, y/o un bus local que use cualquier variedad de arquitecturas de bus disponibles, incluyendo, sin limitación, una Arquitectura Industrial Normalizada (ISA) de bus de 8 bits, Arquitectura Microcanal (MSA), ISA Extendida (EISA), Electrónica de Unidades Inteligentes (IDE), Bus Local VESA (VLB), Interconexión de Componentes Periféricos (PCI), Bus Universal Serie (USB), Puerto Avanzado de Gráficos (AGP), bus de la Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales (PCMCIA) y la Interfaz para Sistemas de Ordenadores Pequeños (SCSI).

La memoria 616 del sistema incluye memoria volátil 620 y memoria no volátil 622. El sistema básico de entrada/salida (BIOS), que contiene las rutinas básicas para transferir información entre elementos dentro del ordenador 612, tal como durante el arranque, está almacenado en la memoria no volátil 622. A título de ilustración, y no de limitación, la memoria no volátil 622 puede incluir memoria de solo lectura (ROM), ROM programable (PROM), ROM programable eléctricamente (EPROM), ROM borrable eléctricamente (EEPROM) o memoria flash. La memoria volátil 620 incluye la memoria de acceso aleatorio (RAM), que actúa como memoria intermedia externa. A título de ilustración y no de limitación, la RAM está disponible en muchas formas, tal como la RAM síncrona (SRAM), la RAM dinámica (DRAM), la DRAM síncrona (SDRAM), la SDRAM de doble tasa de transferencia de datos (DDR SDRAM), la SDRAM mejorada (ESDRAM), la DRAM de enlace síncrono (SLDRAM) y la RAM directa Rambus (DRRAM).

El ordenador 612 también incluye medios de almacenamiento de ordenador extraíbles/no extraíbles volátiles/no volátiles. La Fig. 6 ilustra, por ejemplo, un almacenamiento 624 en disco. El almacenamiento 624 en disco incluye, sin limitación, dispositivos como una unidad de disco magnético, una unidad de disquete, una unidad de cinta, una unidad Jaz, una unidad Zip, una unidad LS-100, una tarjeta de memoria flash o una tarjeta de memoria. Además, el almacenamiento 624 en disco puede incluir medios de almacenamiento por separado o en combinación con otros medios de almacenamiento, incluyendo, sin limitación, una unidad de disco óptico, tal como un dispositivo ROM de discos compactos (CD-ROM), una unidad de CD grabable (unidad CD-R), una unidad de CD reescribible (unidad CD-RW) o una unidad ROM de disco versátil digital (DVD-ROM). Para facilitar la conexión de los dispositivos 624 de almacenamiento en disco con el bus 618 del sistema, se usa típicamente una interfaz extraíble o no extraíble, tal como la interfaz 626.

Ha de apreciarse que la Fig. 6 describe un soporte lógico que actúa como intermediario entre los usuarios y los recursos básicos del ordenador descritos en el entorno operativo adecuado 610. Tal soporte lógico incluye un sistema operativo 628. El sistema operativo 628, que puede estar almacenado en el almacenamiento 624 en disco, actúa para controlar y asignar recursos del sistema 612 de ordenador. Las aplicaciones 6230 del sistema se aprovechan de la gestión de recursos por parte del sistema operativo 628 mediante módulos 632 de programa y datos 634 de programa almacenados ya sea en la memoria 616 del sistema o en el almacenamiento 624 en disco. Ha de apreciarse que la presente invención puede ser implementada con diversos sistemas operativos o combinaciones de sistemas operativos.

Un usuario introduce instrucciones o información en el ordenador 612 a través de uno o más dispositivos 636 de entrada. Los dispositivos 636 de entrada incluyen, sin limitación, un dispositivo de puntero, tal como un ratón, una

bola de mando, un lápiz táctil, una almohadilla táctil, un teclado, un micrófono, una palanca de juego, un mando de juego, una antena parabólica, un escáner, una tarjeta sintonizadora de TV, una cámara digital, una videocámara digital, una cámara web y similares. Estos y otros dispositivos de entrada se conectan a la unidad 614 de proceso a través del bus 618 del sistema por medio de uno o más puertos 638 de interfaz. El o los puertos 638 de interfaz incluye, por ejemplo, un puerto serie, un puerto paralelo, un puerto de juegos y un bus serie universal (USB). El o los dispositivos 640 de salida usan algunos de los mismos tipos de puertos que el o los dispositivos 636 de entrada. Así, por ejemplo, puede usarse un puerto USB para proporcionar una entrada al ordenador 612 y para dar salida de información desde el ordenador 612 a un dispositivo 640 de salida. Se proporciona el adaptador 642 de salida para ilustrar que hay algunos dispositivos 640 de salida como monitores, altavoces e impresoras, entre otros dispositivos 6240 de salida que requieren adaptadores especiales. Los adaptadores especiales 642 incluye, a título de ilustración y no de limitación, tarjetas de vídeo y audio que proporcionan un medio de conexión entre el dispositivo 640 de salida y el bus 618 del sistema. Debería hacerse notar que otros dispositivos y/o sistemas proporcionan capacidades tanto de entrada como de salida, tal como uno o más ordenadores remotos 644.

El ordenador 612 puede operar en un entorno de red usando conexiones lógicas con uno o más ordenadores remotos, tales como el o los ordenadores remotos 644. El o los ordenadores remotos 644 pueden ser un ordenador personal, un servidor, un dispositivo de encaminamiento, un PC de red, una estación de trabajo, un aparato basado en microprocesadores, un dispositivo del mismo nivel u otro nodo común de red y similares, y típicamente incluyen muchos o la totalidad de los elementos descritos en cuanto al ordenador 612. En aras de la brevedad, solo se ilustra un dispositivo 646 de memoria con el o los ordenadores remotos 644. El o los ordenadores remotos 644 están conectados de forma lógica con el ordenador 612 a través de una interfaz 648 de red y luego conectados físicamente a través de la conexión 650 de comunicaciones. La interfaz 648 de red abarca redes de comunicaciones tales como redes de área local (LAN) y redes de área amplia (WAN). Las tecnologías LAN incluyen la Interfaz de Datos Distribuidos por Fibra (FDDI), la Interfaz de Datos Distribuidos por Cobre (CDDI), Ethernet/IEEE 802.3, Token Ring/IEEE 802.5 y similares. Las tecnologías WAN incluyen, sin limitación, enlaces punto a punto, redes conmutadas por circuitos, como las Redes Digitales de Servicios Integrados (RDSI) y variaciones de las mismas, redes conmutadas por paquetes y Líneas Digitales de Abonado (DSL).

Una o más conexiones 650 de comunicaciones se refieren a soporte físico/soporte lógico empleados para conectar la interfaz 648 de red con el bus 618. Aunque, para la claridad ilustrativa, se muestra la conexión 650 de comunicaciones dentro del ordenador 612, también puede ser externa al ordenador 612. El soporte físico/soporte lógico necesario para la conexión con la interfaz 648 de red incluye, solo con fines ejemplares, tecnologías internas y externas tales como módems, incluyendo módems regulares de tipo telefónico, módems de cable y módems DSL, adaptadores RDSI y tarjetas Ethernet.

Lo que se ha descrito en lo que antecede incluye ejemplos de la presente invención. Por supuesto, no es posible describir todas las combinaciones concebibles de componentes o metodologías con fines de describir la presente invención, pero una persona con un dominio normal de la técnica puede reconocer que son posibles muchas combinaciones y permutaciones adicionales de la presente invención. En consecuencia, se pretende que la presente invención abarque todas las alteraciones, las modificaciones y las variaciones de ese tipo que estén dentro del alcance de las reivindicaciones adjuntas. Además, en la media en que se usa el término “incluye”, ya sea en la descripción detallada o en las reivindicaciones, se pretende que tal término sea inclusivo, de manera similar a la expresión “que comprende”, según se interpreta “que comprende” cuando se emplea como expresión de transición en una reivindicación.

REIVINDICACIONES

1. Un sistema implementado por ordenador para facilitar la detección automática de un tipo de red inalámbrica sin requerir indicaciones del usuario, refiriéndose el tipo al procedimiento de autenticación y cifrado que requiere la red, comprendiendo el sistema:

un componente (110) de conexión que puede conectar un dispositivo con una pluralidad de redes inalámbricas (210-250); y
un componente (120) de detección que identifica automáticamente un tipo de cifrado de una red inalámbrica disponible (140), en el que la identificación del tipo de cifrado se basa en la detección de un fallo de una porción de una secuencia de autenticación de la red inalámbrica disponible o en la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación de la red inalámbrica disponible, en el que la identificación del tipo de cifrado incluye:

que el componente de detección intente (310) una secuencia de autenticación 802.1x con la red inalámbrica y determine (330) que la red inalámbrica, como una red (222) de privacidad equivalente a una cableada, requiere una clave de privacidad equivalente a una cableada cuando ocurren un fallo de una porción de la secuencia de autenticación 802.1x o la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación 802.1x;
que el componente de detección, en respuesta a la tentativa de una secuencia de autenticación 802.1x, identifique (432) la red inalámbrica como una red 802.1x (224) cuando no ocurren el fallo de una porción de la secuencia de autenticación 802.1x ni la superación de un umbral de tiempo sin haber detectado la porción esperada de la secuencia de autenticación 802.1x;
que el componente de detección, en respuesta a la identificación de la red inalámbrica como una red 802.1x, intente una secuencia de servicios de dotación inalámbrica y determine (444) que la red inalámbrica no soporta servicios (244) de dotación inalámbrica cuando ocurren un fallo de una porción de la secuencia de autenticación de servicios de dotación inalámbrica o la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación de servicios de dotación inalámbrica; y
que el componente de detección, en respuesta a la tentativa de una secuencia de servicios de dotación inalámbrica, identifique (370) la red inalámbrica como una red (242) de servicios de dotación inalámbrica con soporte de 802.1x cuando no ocurren el fallo de una porción de la secuencia de autenticación de servicios de dotación inalámbrica ni la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación de servicios de dotación inalámbrica.

2. El sistema de la reivindicación 1, estando basada la identificación por parte del componente de detección (120), al menos en parte, en la recepción de un elemento de información procedente de una baliza (140) de red inalámbrica.

3. El sistema de la reivindicación 1, comprendiendo la red inalámbrica, al menos, una de una red no cifrada, una red de privacidad equivalente a una cableada (WEP) que requiera una clave WEP (222), una red cifrada con acceso protegido de fidelidad inalámbrica (WPA) que requiere una clave WPA (238) compartida de antemano, una red (224) habilitada para 802.1x que no soporta WPA , una red (232) habilitada para 802.1x que sí soporta WPA y una red (252) con soporte habilitado de servicios de dotación inalámbrica (WPS).

4. El sistema de la reivindicación 1, estando basada la identificación por parte del componente de detección, al menos en parte, en el sondeo iterativo de la red disponible (140).

5. El sistema de la reivindicación 4 en el que el componente (120) de detección intenta conectarse con la red inalámbrica (120) como una red (252) con soporte de servicios de dotación inalámbrica, determinando el componente de detección es una red de clave compartida de antemano si se determina un fallo en una secuencia de autenticación procedente de una baliza (140) de red inalámbrica.

6. El sistema de la reivindicación 5, determinando el componente (120) de detección que la red (140) es una red (236) de acceso protegido de fidelidad inalámbrica (WPA) si se determina un fallo en una sección específica de la secuencia de autenticación que identifica una red (252) con soporte de servicios de dotación inalámbrica.

7. El sistema de la reivindicación 6, comprendiendo la sección particular de la secuencia de autenticación, una secuencia de tipo-longitud-valor.

8. El sistema de la reivindicación 6, determinando el componente (120) de detección que la red es una red (252) con soporte de servicios de dotación inalámbrica si se recibe la sección particular de la secuencia de autenticación que identifica la red con soporte de servicios de dotación inalámbrica procedente de la baliza (140) de red inalámbrica.

9. El sistema de la reivindicación 1 en el que el componente (120) de detección envía al menos uno de un mensaje de conexión, un mensaje de inicio de EAPOL 802.1x, un mensaje de identidad 802.1x.

10. El sistema de la reivindicación 1 en el que el componente (120) de detección recibe al menos uno de un mensaje asociado, un mensaje de solicitud de identidad 802.1x, un mensaje de autenticación y un mensaje de dotación procedente de la baliza (140) de red inalámbrica.

11. Un procedimiento implementado por ordenador para detectar automáticamente un tipo de red inalámbrica sin requerir indicaciones del usuario, refiriéndose el tipo al procedimiento de autenticación y cifrado que requiere la red, comprendiendo la facilitación de la detección de la red inalámbrica:

identificar automáticamente un tipo de cifrado de una red inalámbrica disponible (140), basándose la identificación del tipo de cifrado en la detección de un fallo de una porción de una secuencia de autenticación de la red inalámbrica disponible o en la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación de la red inalámbrica disponible, incluyendo la identificación:

intentar (310) una secuencia de autenticación 802.1x con la red inalámbrica y determinar (330) que la red inalámbrica, como una red (222) de privacidad equivalente a una cableada, requiere una clave de privacidad equivalente a una cableada cuando ocurren un fallo de una porción de la secuencia de autenticación 802.1x o la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación 802.1x;
identificar (432), en respuesta al intento de la secuencia de autenticación 802.1x, la red inalámbrica como una red 802.1x (224) cuando no ocurren el fallo de una porción de la secuencia de autenticación 802.1x ni la superación de un umbral de tiempo sin haber detectado la porción esperada de la secuencia de autenticación 802.1x;
intentar, en respuesta a la identificación de la red inalámbrica como una red 802.1x, una secuencia de servicios de dotación inalámbrica y determinar (444) que la red inalámbrica no soporta servicios (244) de dotación inalámbrica cuando ocurren un fallo de una porción de la secuencia de autenticación de servicios de dotación inalámbrica o la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación de servicios de dotación inalámbrica; e
identificar (370), en respuesta a la tentativa de una secuencia de servicios de dotación inalámbrica, la red inalámbrica como una red (242) de servicios de dotación inalámbrica con soporte de 802.1x cuando no ocurren el fallo de una porción de la secuencia de autenticación de servicios de dotación inalámbrica ni la superación de un umbral de tiempo sin haber detectado una porción esperada de la secuencia de autenticación de servicios de dotación inalámbrica.

12. Un medio legible por ordenador que tiene almacenado en él mismo instrucciones ejecutables por ordenador que, cuando son ejecutadas en un ordenador, están configuradas para llevar a cabo las etapas del procedimiento de la reivindicación 11.

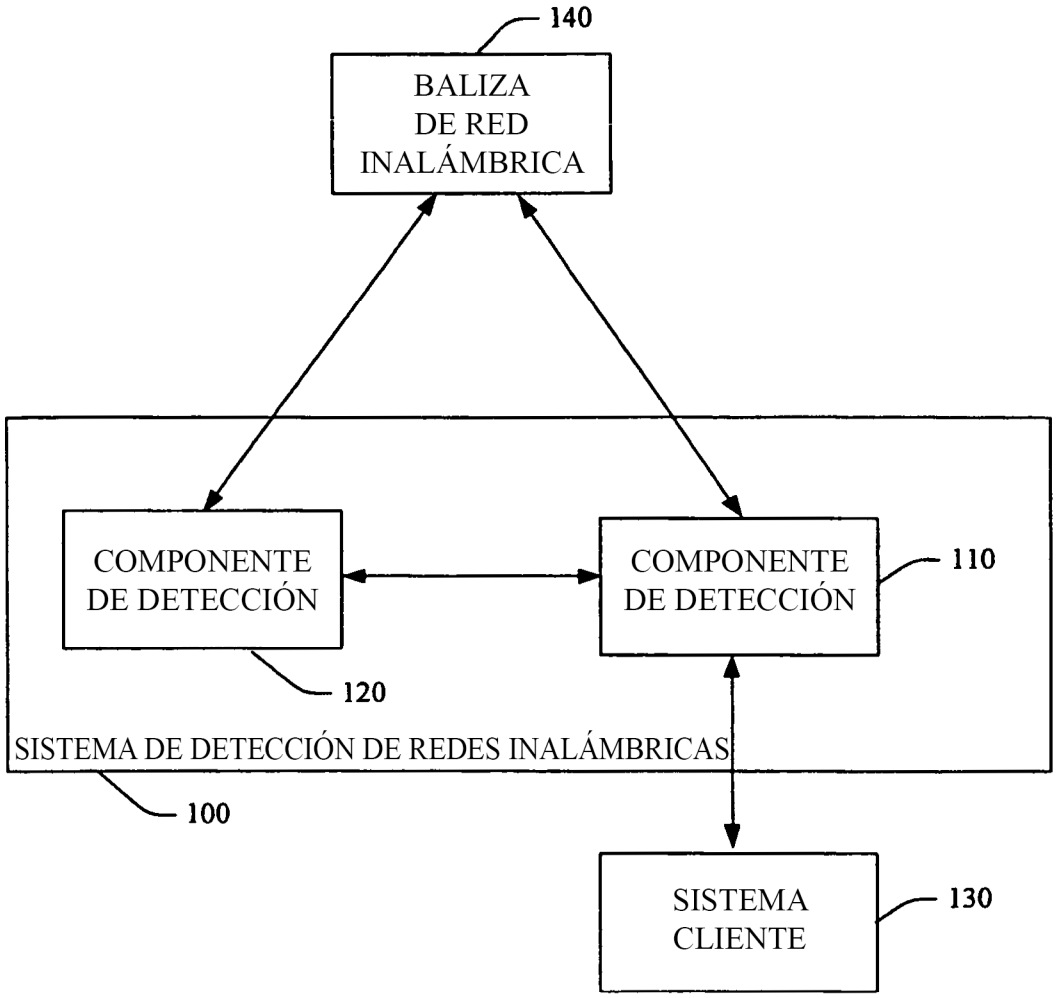
140
BALIZA
DE RED
INALÁMBRICA
COMPONENTE
DE DETECCIÓN
120
COMPONENTE
DE DETECCIÓN
110
SISTEMA DE DETECCIÓN DE REDES INALÁMBRICAS
100
SISTEMA
CLIENTE
130

FIG. 1

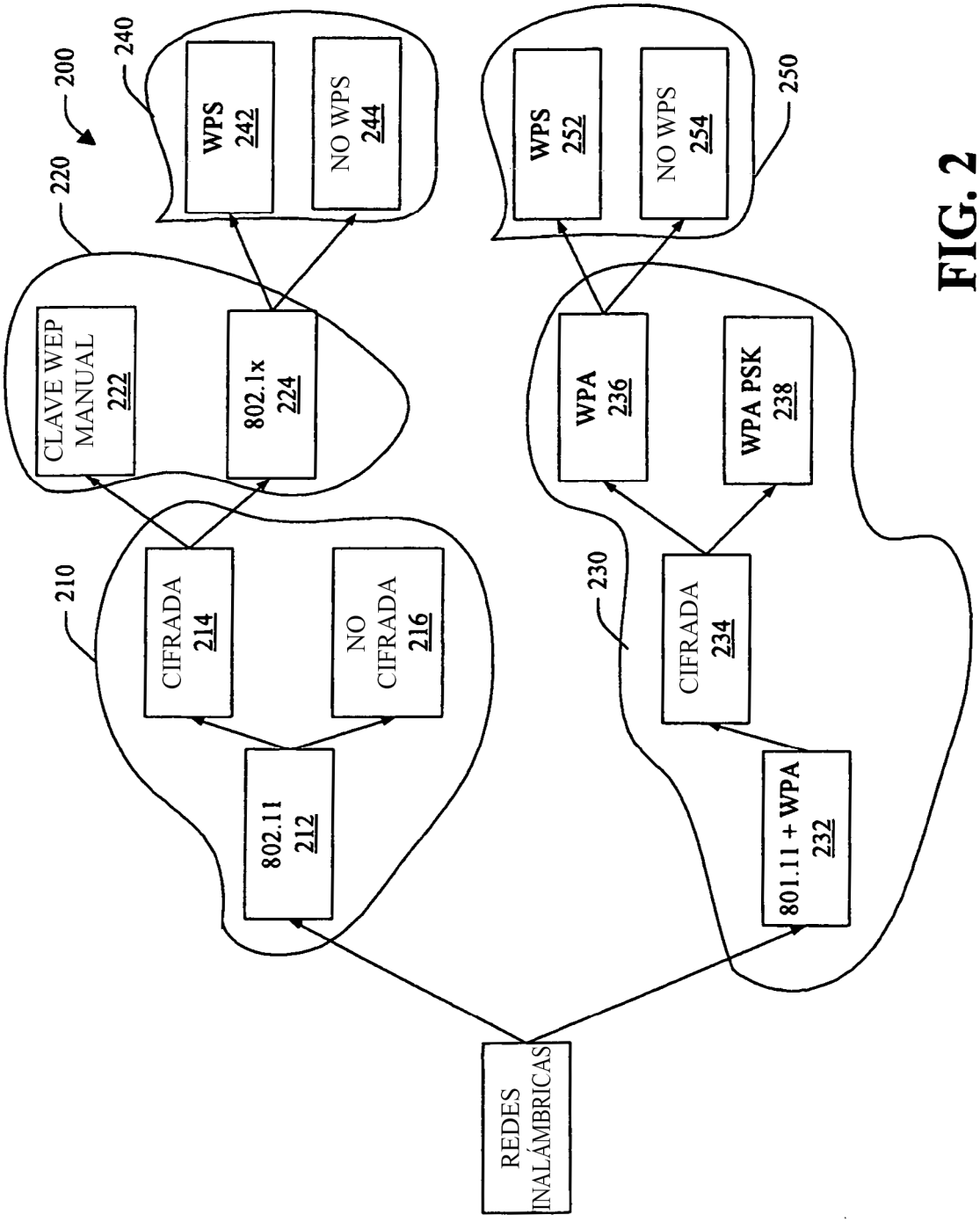
200
210
CIFRADA 214
NO CIFRADA 216
802.11 212
220
CLAVE WEP MANUAL 222
802.1x 224
240
WPS 242
NO WPS 244
230
CIFRADA 234
801.11 + WPA 232
WPA 236
WPA PSK 238
250
WPS 252
NO WPS 254
REDES INALÁMBRICAS

FIG. 2

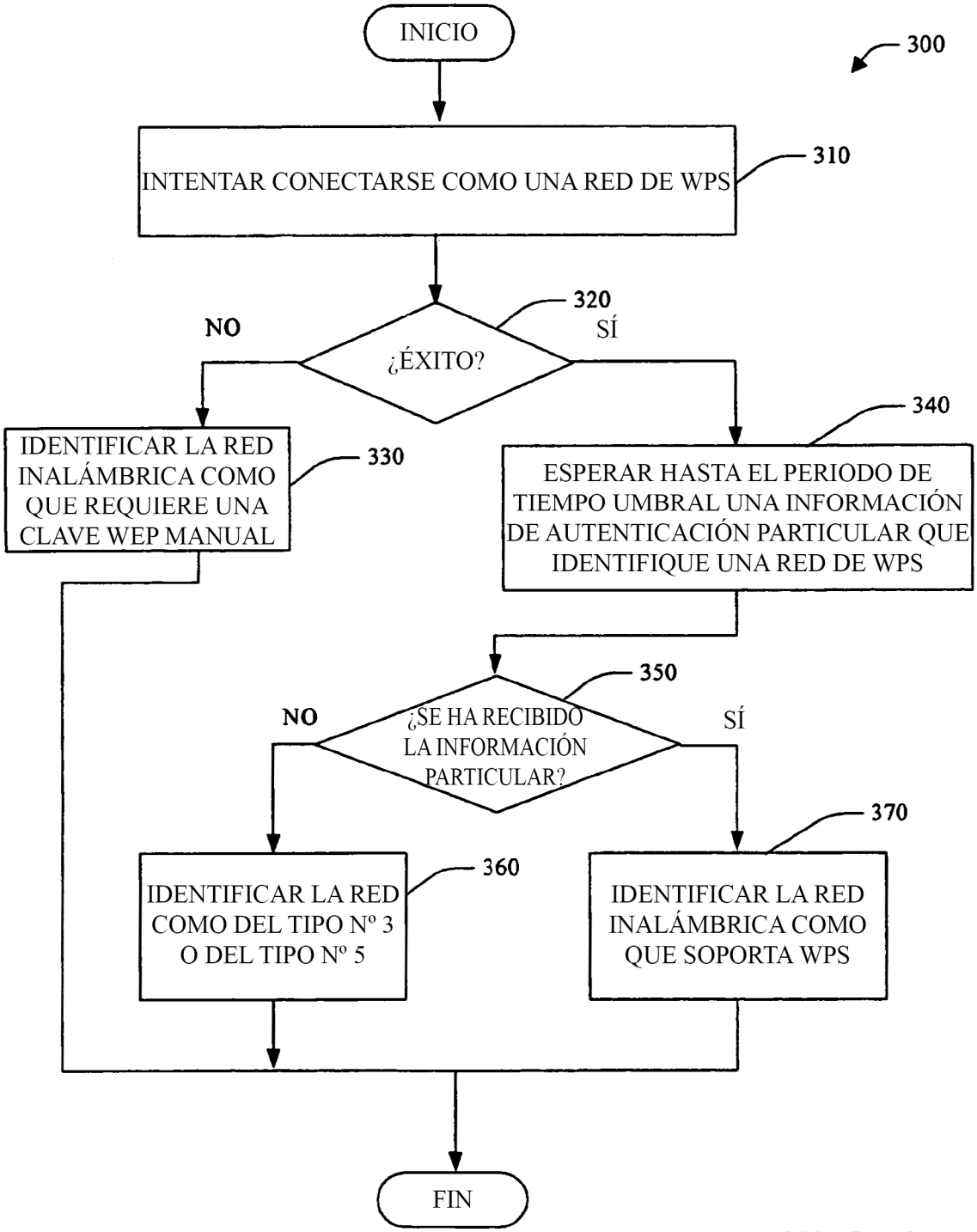
INICIO
300
INTENTAR CONECTARSE COMO UNA RED DE WPS
310
¿ÉXITO?
320
NO
SÍ
IDENTIFICAR LA RED INALÁMBRICA COMO QUE REQUIERE UNA CLAVE WEP MANUAL
330
ESPERAR HASTA EL PERIODO DE TIEMPO UMBRAL UNA INFORMACIÓN DE AUTENTICACIÓN PARTICULAR QUE IDENTIFIQUE UNA RED DE WPS
340
¿SE HA RECIBIDO LA INFORMACIÓN PARTICULAR?
350
NO
SÍ
IDENTIFICAR LA RED COMO DEL TIPO Nº 3 O DEL TIPO Nº 5
360
IDENTIFICAR LA RED INALÁMBRICA COMO QUE SOPORTA WPS
370
FIN

FIG. 3

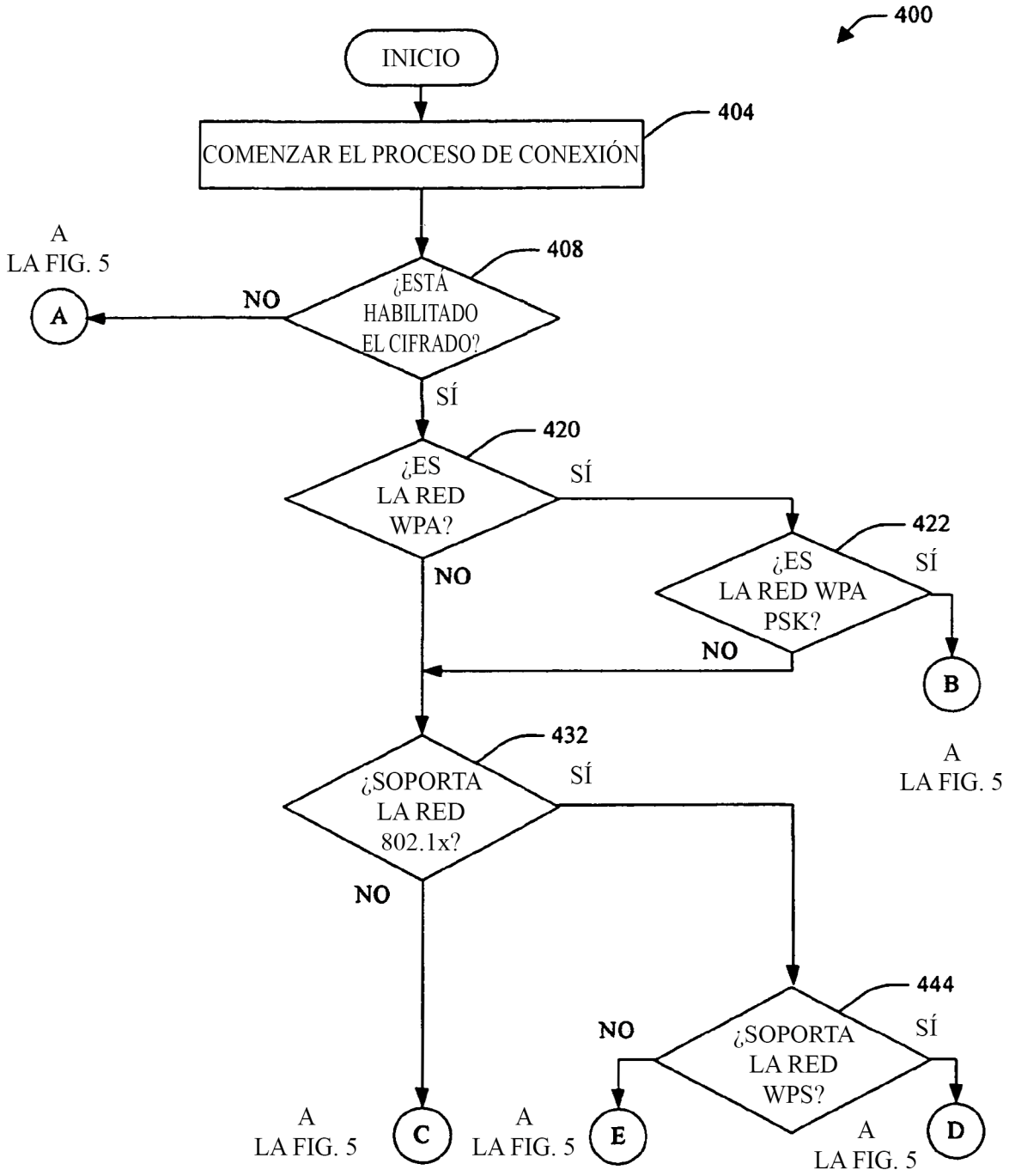
400
INICIO
404
COMENZAR EL PROCESO DE CONEXIÓN
A
LA FIG. 5
408
¿ESTÁ HABILITADO EL CIFRADO?
NO
A
SÍ
420
¿ES LA RED WPA?
SÍ
NO
422
¿ES LA RED WPA PSK?
SÍ
NO
B
A
LA FIG. 5
432
¿SOPORTA LA RED 802.1x?
SÍ
NO
444
¿SOPORTA LA RED WPS?
NO
SÍ
A
LA FIG. 5
C
A
LA FIG. 5
E
A
LA FIG. 5
D

FIG. 4

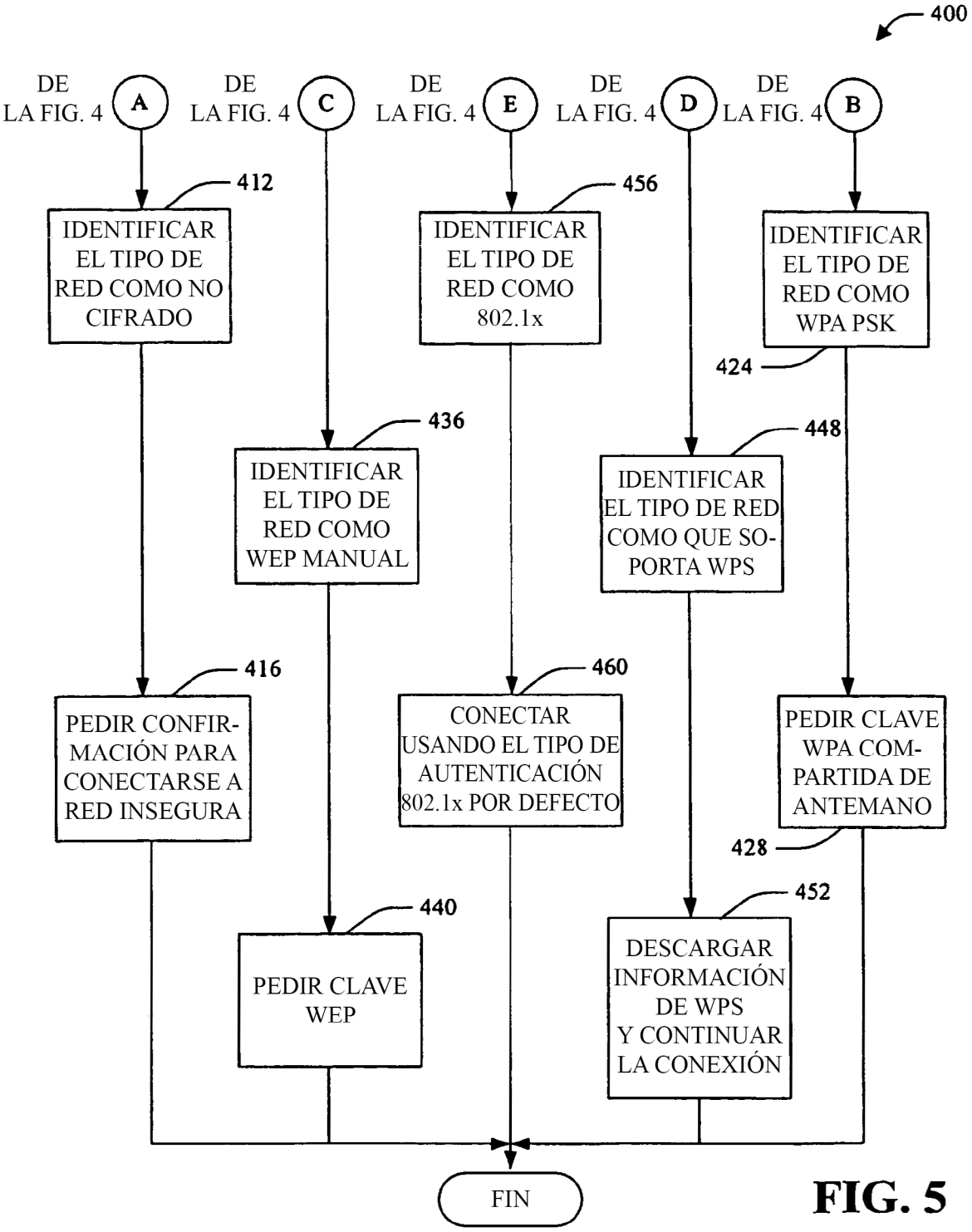
400
DE LA FIG. 4 A
DE LA FIG. 4 C
DE LA FIG. 4 E
DE LA FIG. 4 D
DE LA FIG. 4 B
412
IDENTIFICAR EL TIPO DE RED COMO NO CIFRADO
456
IDENTIFICAR EL TIPO DE RED COMO 802.1x
IDENTIFICAR EL TIPO DE RED COMO WPA PSK
424
436
IDENTIFICAR EL TIPO DE RED COMO WEP MANUAL
448
IDENTIFICAR EL TIPO DE RED COMO QUE SOPORTA WPS
416
PEDIR CONFIRMACIÓN PARA CONECTARSE A RED INSEGURA
460
CONECTAR USANDO EL TIPO DE AUTENTICACIÓN 802.1x POR DEFECTO
PEDIR CLAVE WPA COMPARTIDA DE ANTEMANO
428
440
PEDIR CLAVE WEP
452
DESCARGAR INFORMACIÓN DE WPS Y CONTINUAR LA CONEXIÓN
FIN

FIG. 5

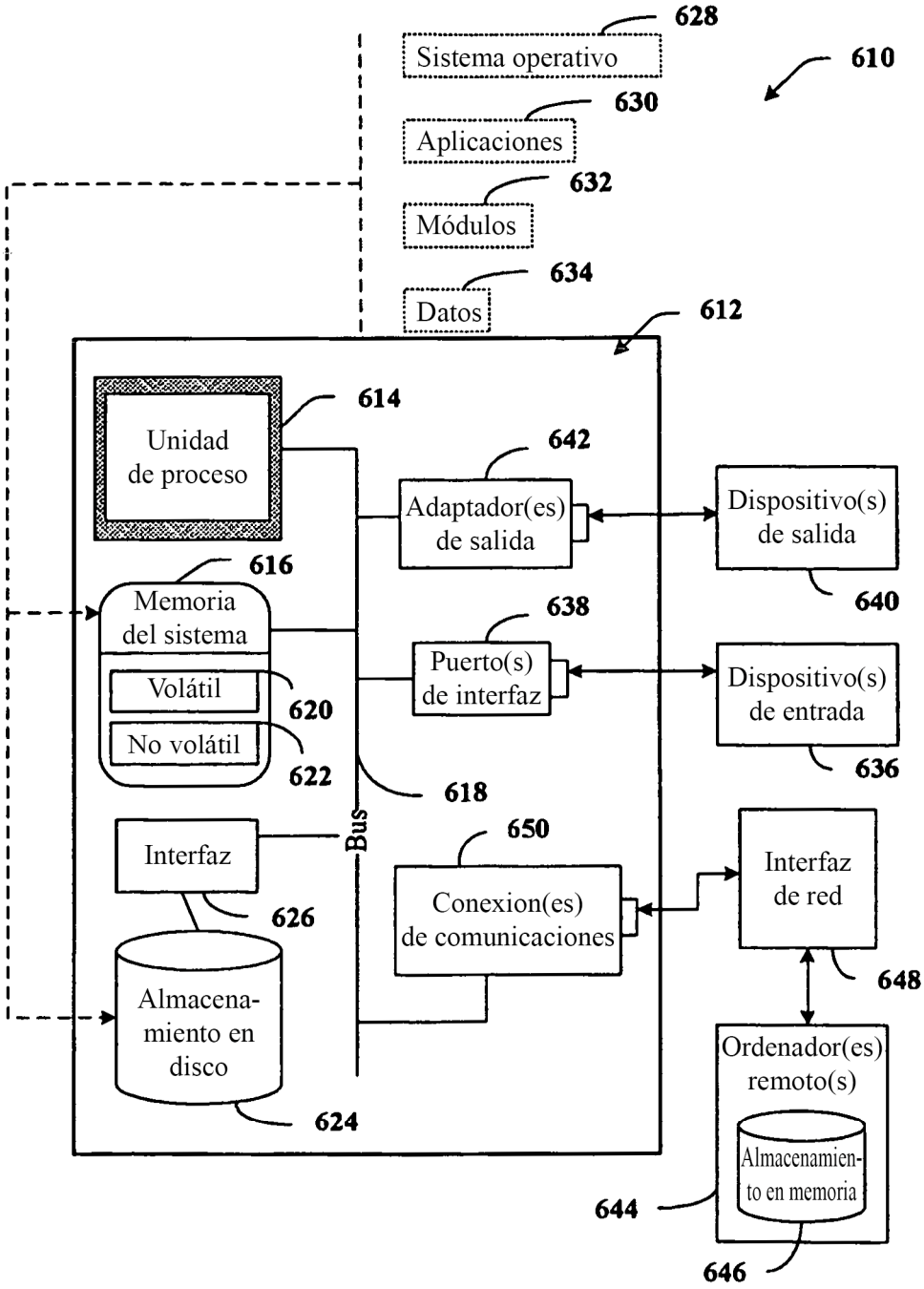
628
Sistema operativo
610
630
Aplicaciones
632
Módulos
634
Datos
612
614
Unidad de proceso
642
Adaptador(es) de salida
Dispositivo(s) de salida
640
616
Memoria del sistema
638
Puerto(s) de interfaz
Dispositivo(s) de entrada
636
Volátil
620
No volátil
622
618
Bus
650
Interfaz
Conexion(es) de comunicaciones
Interfaz de red
626
648
Almacena-miento en disco
Ordenador(es) remoto(s)
Almacenamien-to en memoria
644
624
646

FIG. 6