(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 685 919**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 88/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.08.2010 E 10173409 (3)**

(97) Fecha y número de publicación de la concesión europea: **13.06.2018 EP 2291017**

(54) Título: **Procedimiento para conexión de red**

(30) Prioridad:

27.08.2009 TW 098128899

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.10.2018

(73) Titular/es:

ARCADYAN TECHNOLOGY CORP. (100.0%)
4F, No. 9 Park Avenue II Science-Based Industrial Park
Hsinchu , TW

(72) Inventor/es:

TSAI, WEI-CHIN

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para conexión de red

Campo técnico

La presente invención se refiere a un procedimiento para conexión de red. Más particularmente, se refiere a un procedimiento para conexión de red inalámbrica.

Técnica anterior

Internet es omnipresente en la sociedad moderna. La red de área local inalámbrica (WLAN) es cada vez más frecuente debido a los beneficios de no estar equipada con cable. El estándar de comunicación WLAN original IEEE 802.11 fue lanzado en 1997, y define el control de acceso al medio (MAC) y la capa física. Bajo el estándar, la conexión entre dos equipos de comunicación puede proceder con un procedimiento ad-hoc y también puede proceder con la cooperación entre una estación base (BS) y un punto de acceso (AP). En 1999, la industria de las telecomunicaciones conforma una alianza Wi-Fi, para resolver los problemas relacionados con la compatibilidad de los productos y dispositivos estándar 802.11.

Mediante la presente tecnología, con el fin de llevar a cabo la conexión bajo el estándar de comunicación de red inalámbrica, tradicionalmente un usuario tiene que crear manualmente un título red inalámbrica, es decir, el identificador de conjunto de servicio (SSID), y luego entra un conjunto de seguridad clave en los puntos de acceso y los extremos del cliente, respectivamente, a fin de evitar un agrietamiento de inicio de sesión no admisible en la red inalámbrica. El usuario debe conocer los conocimientos básicos sobre el dispositivo Wi-Fi y ser capaz de establecer los parámetros con respecto a una demanda para realizar todo el procedimiento. Por lo tanto, no es fácil para un usuario utilizarlo. Para garantizar la seguridad de la red inalámbrica y hacer que la conexión a Internet sea más conveniente para el usuario, Wi-Fi Alliance ha desarrollado un nuevo esquema de certificación conocido como "configuración protegida de Wi-Fi (WPS)" en 2007. Al utilizar la WPS, sin conocer el SSID y las claves de seguridad o contraseñas de inicio de sesión, los usuarios pueden establecer las claves de seguridad del SSID, el acceso protegido de Wi-Fi (WPA) para el AP y dispositivos cliente capaces de usar la WPS en Internet. En la actualidad, la WPS tiene dos formas comunes de configurar una red inalámbrica, es decir, el "procedimiento de configuración de entrada del PIN" y el "procedimiento de configuración de botón pulsador (PBC)".

El procedimiento de configuración de entrada del PIN significa introducir un conjunto de número de secuencia para establecer una conexión. El procedimiento de configuración de botón pulsador (PBC) significa establecer una conexión presionando el botón en línea, y el botón del mismo podría ser un botón virtual creado por software o un botón real dispuesto en un dispositivo de hardware. Cuando se selecciona un procedimiento específico para establecer una conexión en una estación base inalámbrica, el extremo del cliente solo necesita seleccionar la misma manera para establecer la conexión.

Los procedimientos para crear una conexión del procedimiento de configuración de entrada del PIN y el procedimiento de PBC son casi los mismos. Pero dado que el procedimiento de configuración de entrada del PIN procede ingresando directamente los datos PIN de una tarjeta de interfaz de red inalámbrica y la estación base ha restringido el alcance de transmisión del cliente, por lo tanto, la velocidad de establecer una conexión es por consiguiente más rápida. Por el contrario, el procedimiento de PBC procede presionando el botón de conexión del cliente para establecer una conexión dentro de un tiempo específico solo después de presionar el botón de conexión en la estación base. Por lo tanto, el cliente buscará primero para averiguar si hay una estación base que soporta la WPS en el rango de comunicación inalámbrica, y al mismo tiempo la función de PBC de la estación base debe iniciarse para que coincida con la conexión. Por el contrario, la velocidad de establecer una conexión a través del procedimiento de PBC es más lenta que mediante el procedimiento de configuración de entrada del PIN, por lo que no es conveniente.

Además, cuando se utiliza el procedimiento de PBC para sistema de distribución inalámbrico (WDS), es necesario establecer las direcciones MAC de otros en los puntos de acceso respectivos para una conexión entre los puntos de acceso debido a las restricciones de la arquitectura del sistema y necesario tienen el mismo SSID y mecanismo de seguridad, lo que hace que el usuario necesite establecer parámetros a través de una red Ethernet y hacer que la conexión sea más lenta. Por lo tanto, también es un inconveniente para el uso.

Parte introductoria modificada de la descripción

Algunas de las referencias se proporcionan adicionalmente de la siguiente manera.

En "Fabricación, usabilidad y seguridad a bajo coste: Un análisis del emparejamiento simple de Bluetooth y la configuración protegida de Wi-Fi "(XP019085841), Cynthia Kuo et al., se presenta que el emparejamiento simple de Bluetooth y la configuración protegida de Wi-Fi especifican mecanismos para intercambiar credenciales de autenticación en redes inalámbricas. Tanto el emparejamiento simple como la configuración protegida admiten múltiples mecanismos de configuración, lo que aumenta los riesgos de seguridad y perjudica la experiencia del usuario. Para mejorar la seguridad y usabilidad de estas especificaciones, Cynthia Kuo et al. sugieren definir una

línea de base común para las características de hardware y una experiencia de usuario consistente e interoperable en todos los dispositivos.

En el documento KR 2009 0030629 A, se presenta un sistema de comunicación inalámbrico. El sistema de comunicación inalámbrica comprende: un punto de acceso que entrega al exterior un mensaje de baliza, que contiene un dato que significa establecimiento automático por solicitud de un usuario, y opera un ajuste de acceso a través de un intercambio de un mensaje según un repetidor que responde y un protocolo de WPS; y otro punto de acceso que recibe el mensaje de baliza que contiene un dato que significa el ajuste automático desde el punto de acceso, y que opera el ajuste de acceso a través de un intercambio de un mensaje según el punto de acceso y el protocolo de WPS. De acuerdo con la presente invención, existe la ventaja de que un administrador no necesita verificar una dirección Mac y otros datos de acceso del punto de acceso o del repetidor, ya que la configuración entre el punto de acceso y el repetidor, o entre dos puntos de acceso es hecho automáticamente

En el documento "Windows Connect Now-NET" (XP002460510), se presenta que la tecnología de Microsoft® Windows® Connect Now permite una configuración sencilla y segura de las redes inalámbricas y aprovisionamiento de hardware inalámbrico. Windows Connect Now-NET (WCN-NET) es la implementación de Microsoft del protocolo de configuración simple Wi-Fi, un nuevo estándar en Wi-Fi Alliance. WCN-NET admite la configuración de dispositivos en redes inalámbricas fuera de banda y dentro de banda. Windows Connect Now-NET en Microsoft Windows Vista™ se comunica con puntos de acceso (AP) y estaciones inalámbricas mediante UPnP, se autentica con un número de identificación personal (PIN) y proporciona configuraciones inalámbricas basadas en la selección del usuario. Esta especificación define los detalles de implementación de WCN-NET para dispositivos que se conectan con sistemas que ejecutan el sistema operativo Windows Vista. WCN-NET es un componente del conjunto de tecnologías Microsoft Windows Rally™.

En el documento "Autenticación de desafío-respuesta de canal auxiliar unidireccional" (XP 031274989), Nilsson DK et al., presentan un enfoque para la autenticación de los valores públicos intercambiados entre dos dispositivos previamente desconocidos en las proximidades. Nilsson DK et al. sugieren el uso de un esquema de desafío-respuesta de canal auxiliar unidireccional, donde la respuesta y el desafío de un dispositivo se transmiten a través de un canal auxiliar. Se supone que un atacante de la red no puede acceder al canal auxiliar y, por lo tanto, se evitan los ataques del intermediario ya que el atacante no puede aprender la respuesta y el desafío. Además, se evita el espionaje pasivo ya que no se utilizan secretos compartidos. Nilsson DK et al. diseñan un protocolo de respuesta-desafío de canal auxiliar unidireccional para Bluetooth y demostrar que es sustancialmente más eficiente y logra un nivel igual o mayor de seguridad mientras se mantiene el nivel de usabilidad y conveniencia para el usuario en comparación con el protocolo Bluetooth original. El documento estándar 3GPP "Proyecto de asociación de tercera generación; servicio de grupo de especificaciones técnicas y aspectos del sistema; seguridad 3G; seguridad de interfuncionamiento de red de área local inalámbrica (WLAN)", TS 33.234, V8.1.0, especifica la arquitectura de seguridad; el modelo de confianza y los requisitos de seguridad para el interfuncionamiento del sistema 3GPP y las redes de acceso WLAN.

Por lo tanto, sería útil para inventar un procedimiento para la conexión a la red para eludir todas las cuestiones antes mencionadas. Para cumplir con esta necesidad, los inventores han propuesto un "procedimiento de conexión de red" para la invención. El resumen de la presente invención se describe a continuación.

La invención se define en las reivindicaciones independientes adjuntas. La idea original de la invención es usar una etiqueta de identificación específica en el procedimiento de conexión, cuya etiqueta nunca se utiliza en las definiciones actuales de WPS. Al usar la etiqueta de identificación específica, no solo hace que la conexión a la red sea mucho más fácil y conveniente, sino que también es consciente de la seguridad e incluso no entra en conflicto con la arquitectura del sistema existente.

De acuerdo con el primer aspecto de la presente invención, se proporciona un procedimiento para una conexión de red entre un terminal de cliente y un punto de acceso (AP) acoplado a un registrador. El procedimiento incluye las etapas de: (A) enviar un primer mensaje con una etiqueta de identificación específica desde el terminal del cliente al registrador a través del AP; (B) enviar un segundo mensaje con una etiqueta de pregunta del registrador al terminal del cliente; (C) enviar un tercer mensaje con una etiqueta de respuesta desde el terminal del cliente al registrador; (D) determinar si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí en el registrador; y (E) si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí, enviar una configuración WiFi privada del registrador al terminal del cliente para conectar el terminal del cliente al AP.

Preferentemente, se proporciona el procedimiento, en el que la etapa (A) comprende además una etapa (A1) de enviar una solicitud de sondeo desde el terminal de cliente al AP después de que el terminal de cliente confirma que el AP envía una baliza.

Preferentemente, se proporciona el procedimiento, en el que la etiqueta de pregunta y la etiqueta de respuesta están codificadas por un procedimiento de codificación seleccionado de un grupo que consiste en un cifrado Rivest 2 (RC2), un cifrado Rivest 4 (RC4), un cifrado Rivest 5 (RC5), un cifrado Rivest 6 (RC6) y un estándar de encriptación avanzado (AES).

Preferentemente, se proporciona el procedimiento, en el que el primer mensaje incluye además un identificador de conjunto de servicio (SSID) y una dirección de control de acceso de medio (MAC) del terminal de cliente y el segundo mensaje incluye además un SSID y una dirección de MAC del registrador.

Preferentemente, se proporciona el procedimiento, en el que la etapa (E) incluye además una etapa (E1) de establecer un sistema de distribución inalámbrico (WDS) de acuerdo con el primer mensaje y el segundo mensaje si la etiqueta de pregunta y la etiqueta de repuesta coinciden entre sí.

Preferentemente, se proporciona el procedimiento, en el que la etapa (E) incluye además una etapa (E1) de dejar un procedimiento de configuración Wi-Fi protegida (WPS) si un resultado de la etapa (E) es negativo.

Preferentemente, el procedimiento incluye además una etapa (F) de procesamiento de un procedimiento de configuración de botón (PCB).

Preferentemente, se proporciona el procedimiento, en el que el primer, el segundo y el tercer mensaje son mensajes de registrador y la etiqueta de identificación específica incluye un SSID específico.

De acuerdo con el segundo aspecto de la presente invención, se proporciona un procedimiento para una conexión de red entre un primer punto de acceso (AP) y un segundo punto de acceso (AP) acoplado a un registrador. El procedimiento incluye las etapas de: (A) enviar una etiqueta de identificación específica desde el primer AP al registrador a través del segundo AP; (B) enviar una etiqueta de pregunta del registrador al primer AP; (C) enviar una etiqueta de respuesta desde el primer AP al registrador; (D) determinar si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí en el registrador; y (E) conectar el primer AP y el segundo AP si la etiqueta de pregunta y la etiqueta de respuesta coinciden.

Preferentemente, se proporciona el procedimiento, en el que la etapa (A) comprende además una etapa (A1) de la transformación del primer AP en un terminal de cliente por la etiqueta de identificación específica.

Preferentemente, se proporciona el procedimiento, en el que la etiqueta de identificación específica se incluye en un primer mensaje y se envía desde el primer AP al registrador a través del segundo AP en la etapa (A), la etiqueta cuestión está incluido en un segundo mensaje y enviado desde el registrador al primer AP en la etapa (B), y la etiqueta de respuesta se incluye en un tercer mensaje y se envía desde el primer AP al registrador en la etapa (C). Además, el primer mensaje podría incluir un identificador de conjunto de servicios (SSID) y una dirección de control de acceso a medios (MAC) del primer AP, el segundo mensaje podría incluir además un SSID y una dirección MAC del registrador, y el primero, el segundo y el tercer mensaje podrían ser mensajes de registro.

Preferentemente, se proporciona el procedimiento, en el que la etapa (E) incluye además una etapa (E0) de establecer un sistema de distribución inalámbrico (WDS) de acuerdo con el primer mensaje y el segundo mensaje con el fin de conectar el primer AP al segundo AP. Además, la etapa (E) podría incluir una etapa (E1) de envío de una configuración WiFi-privada desde el registrador al primer AP para conectar el primer AP al segundo AP si la etiqueta de pregunta y la etiqueta de respuesta coinciden. Si la etiqueta de pregunta y la etiqueta de respuesta no coinciden, se interrumpirá el procedimiento de configuración protegida Wi-Fi (WPS).

Preferentemente, el procedimiento incluye además una etapa (F) de procesamiento de un procedimiento de configuración de botón (PCB).

De acuerdo con el tercer aspecto de la presente invención, se proporciona un procedimiento para conectar un primer nodo y un segundo nodo. El procedimiento incluye las etapas de: (A) enviar una etiqueta de identificación específica desde el primer nodo al segundo nodo; (B) enviar una etiqueta de pregunta desde el segundo nodo al primer nodo; (C) enviar una etiqueta de respuesta del primer nodo al segundo nodo; y (D) conectar el primer nodo al segundo nodo si la etiqueta de pregunta y la etiqueta de respuesta están satisfechas con una regla específica.

Preferentemente, se proporciona el procedimiento, en el que el primer nodo es uno de un primer punto de acceso y un primer terminal de cliente, el segundo nodo es uno de un segundo punto de acceso y un segundo terminal de cliente, el segundo nodo incluye además un registrador para determinar si la etiqueta de pregunta y la etiqueta de respuesta están satisfechas con la regla específica, y la etiqueta de pregunta y la etiqueta de respuesta están codificadas por un procedimiento de codificación seleccionado de un grupo que consiste en un cifrado Rivest 2 (RC2), un cifrado Rivest 4 (RC4), un cifrado Rivest 5 (RC5), un cifrado Rivest 6 (RC6) y un estándar de encriptación avanzado (AES).

Preferentemente, el procedimiento incluye además las etapas de: (D0) determinar si la etiqueta de pregunta y la etiqueta de respuesta coinciden; y (D1) conectar el primer nodo y el segundo nodo si la determinación de la etapa (D0) es positiva.

Breve descripción de las figuras en los dibujos

Las anteriores y otras características y ventajas de la presente invención se entenderán más claramente a través de las siguientes descripciones con referencia a los dibujos:

La figura 1 es un diagrama que muestra el primer sistema de comunicación;
La figura 2 es un diagrama de flujo que muestra la primera realización preferida de la presente invención;
La figura 3 es un diagrama que muestra el segundo sistema de comunicación;
La figura 4 es un diagrama de flujo que muestra la segunda realización preferida de la presente invención;
La figura 5 es un diagrama que muestra el tercer sistema de comunicación; y
La figura 6 es un diagrama de flujo que muestra la tercera realización preferida de la presente invención.

Mejor modo de llevar a cabo la invención

La presente invención se describirá más específicamente a continuación con referencia a las siguientes realizaciones. Debe observarse que las siguientes descripciones de las realizaciones preferidas de esta invención se presentan en la presente memoria únicamente para el aspecto de ilustración y descripción; no pretenden ser exhaustivas o limitarse a lo que se describe.

Refiérase a la figura 1 que es un diagrama que muestra el primer sistema de comunicación. El sistema de comunicación 100 incluye un terminal 101 de cliente, un AP 102 y un registrador 103 que se conecta al AP 102. Diríjase además a la figura 2, que es un diagrama de flujo que muestra la primera realización preferida de la presente invención. La primera realización preferida de la invención es un primer procedimiento 200 para una conexión de red bajo el marco WPS (configuración protegida Wi-Fi).

En primer lugar, cuando un usuario pulsa un botón de PBC virtual o real (etapa 201) en el terminal 101 de cliente, el terminal 101 de cliente buscará una baliza emitida desde el AP 102 (etapa 202) con el elemento de información de los servicios de aprovisionamiento inalámbrico (WPS IE). Cuando el terminal 101 de cliente confirma la baliza, el terminal 101 de cliente enviará una solicitud de sondeo con WPS IE al AP 102 y el AP 102 responderá una respuesta de sonda con WPS IE (etapa 203). A continuación, el terminal 101 de cliente ingresa al procedimiento de autenticación y enlace e inicia EAP sobre LAN (EAPOL). El terminal 101 de cliente envía un primer mensaje de registro (M1) que incluye una etiqueta de identificación específica, un identificador de conjunto de servicios (SSID) y una dirección MAC al AP 102 (etapa 204) y luego el AP 102 transferirá M1 a un registrador 103 (etapa 205). El registrador 103 responde a un segundo mensaje de registro (M2) que incluye una etiqueta de pregunta, un identificador de conjunto de servicios (SSID) y una dirección MAC al terminal 101 de cliente (etapa 206). Entonces, el terminal 101 de cliente responde a un tercer mensaje de registro (M3) que incluye una etiqueta de respuesta al registrador 103 (etapa 207). Finalmente, el registrador 103 determina si la etiqueta de respuesta y la etiqueta de pregunta coinciden entre sí (etapa 208). Si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí, el registrador 103 envía una configuración de WiFi privada al terminal 101 de cliente, de modo que el terminal 101 de cliente se conectará al AP 102 después de que el terminal 101 de cliente reciba la configuración WiFi-privada (etapa 209A). Se observa que el mensaje de registro puede ser cualquier tipo de mensaje. Además, el terminal 101 de cliente podría enviar mensajes directamente al registrador 103.

En la realización anterior, la etiqueta de identificación específica es la etiqueta que nunca ha sido utilizado en las definiciones de WPS actuales de modo que pudiera evitar los conflictos con la arquitectura del sistema existente e incluso mejorar la seguridad para mantener el secreto. Además, en algunas máquinas de red, el AP 102 tendría al menos un conjunto de configuración de conexión para el valor predeterminado (es decir, al menos un conjunto de SSID y claves de seguridad) para satisfacer las demandas especiales. Sin embargo, para que cualquier terminal 101 de cliente no pueda conectarse al AP 102 para otros conjuntos de configuración de conexión, el diseño de la etiqueta de identificación específica de la realización preferida podría informar al AP 102 para conectarse a un SSID específico y, por lo tanto, el AP 102 enviaría los datos específicos al terminal del cliente 101 a través del WPS.

En este caso, por ejemplo, la etiqueta de identificación de M1 se puede establecer como "1110 1 56 (HEX)", la etiqueta cuestión de M2 se puede establecer como "R = (RND(x) % 0x10000), Qv = RC4 (R), Q = 1110 8 Qv", y la etiqueta de respuesta de M3 podría establecerse como "Obtener la etiqueta Q' es 1110 8 Qt, A1 = RC4 (Qt), Av = RC4 (A1 + 0x0718), A = 1110 8 Av". Después de recibir M3, el registrador 103 puede analizar la etiqueta de respuesta para verificar, la etiqueta "Obtener la etiqueta A' es 1110 8 At, A2 = RC4 (At), A3 = RC4 (Qv + 0x0718)". Si A2 = A3, la etiqueta de respuesta y la etiqueta de pregunta coinciden entre sí y el terminal 101 de cliente se verifica y se autentica de modo que se envíe la configuración WiFi-privada. Si A2 y A3 no coinciden o no están apareadas, el procedimiento de WPS cesará (etapa 209B). Se observa que la etiqueta de identificación específica podría incluir un SSID específico para informar al AP 102 que se conecte para el SSID específico. Además, podría haber dos SSID para un terminal 101 de cliente, y un SSID está incluido en M3 y el otro está incluido en la etiqueta de especificación.

La etiqueta de pregunta y la etiqueta de respuesta podría ser codificada por un cifrado Rivest 2 (RC2), un cifrado Rivest 4 (RC4), un cifrado Rivest 5 (RC5), un cifrado Rivest 6 (RC6), un estándar de cifrado avanzado (AES) u otros procedimientos de codificación.

Refiérase a la figura 3 que es un diagrama que muestra el segundo sistema de comunicación. El sistema de comunicación 300 incluye un primer AP 301, un segundo AP 302 y un registrador 303 que se conecta al segundo AP 302. Consulte la figura 4, que es un diagrama de flujo que muestra la segunda realización preferida de la presente invención. La segunda realización preferida de la invención es un segundo procedimiento 400 para una conexión de

red entre los dos AP bajo el marco WDS (sistema de distribución inalámbrico). Dado que una técnica anterior necesita configurar los dos AP (301 y 302) para la asociación (es decir, establecer el MAC del primer AP 301 en el segundo AP 302 y establecer el MAC del segundo AP 302 en el primer AP 301), una red Ethernet debe ser configurada por un usuario que conozca la dirección MAC, el SSID y la clave de seguridad. Por lo tanto, el primer AP 301 podría transformarse en un terminal de cliente y las etapas similares a la primera realización podrían realizarse para conectar el primer AP 301 y el segundo AP 302.

En primer lugar, cuando un usuario pulsa un botón PBC virtual o real (etapa 401) en el primer AP 301, el primer AP 301 buscará una señal emitida desde el segundo AP 302 (etapa 402) con elemento de información de servicios de aprovisionamiento inalámbrico (WPS IE). Cuando el primer AP 301 confirma la baliza, el primer AP 301 enviará una solicitud de la sonda con WPS IE al segundo AP 302 y el segundo AP 302 responderá una respuesta de la sonda con WPS IE (etapa 403). A continuación, el primer AP 301 ingresa al procedimiento de autenticación y asociación e inicia EAP a través de LAN (EAPOL). El primer AP 301 envía un primer mensaje de registro (M1) que incluye una etiqueta de identificación específica, un Identificador de conjunto de servicios (SSID) y una dirección MAC al segundo AP 302 (etapa 404) y luego el segundo AP 302 transferirá el M1 al registrador 303 (etapa 405). El registrador 303 responde a un segundo mensaje de registro (M2) que incluye una etiqueta de pregunta, un identificador de conjunto de servicios (SSID) y una dirección MAC al primer AP 301 (etapa 406). Entonces, el primer AP 301 responde a un tercer mensaje de registro (M3) que incluye una etiqueta de respuesta al registrador 303 (etapa 407). Finalmente, el registrador 303 determina si la etiqueta de respuesta y la etiqueta de pregunta coinciden entre sí (etapa 408). Si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí, el registrador 303 establece una lista de sistema de distribución inalámbrica (WDS) según M1 y M2 (incluidos los SSID y las direcciones MAC del primer y segundo AP 301 y 302) para conectar el primer AP 301 al segundo AP 302 (etapa 409A). Se observa que el mensaje de registro puede ser cualquier tipo de mensaje. Además, el primer AP 301 podría enviar mensajes directamente al registrador 303. Para el otro ejemplo, el M1 con la etiqueta de identificación específica podría incluir además un SSID y una dirección MAC del primer AP 301, el M2 con la etiqueta de pregunta podría incluir además un SSID y una dirección MAC del segundo AP 302 o el registrador 303, y estos mensajes son mensajes de registro.

En la realización anterior, la etiqueta de identificación específica tampoco es usada en las definiciones de las WPS en la actualidad de manera que pudiera evitar los conflictos con la arquitectura del sistema existente e incluso mejorar la seguridad para mantener el secreto. La diferencia entre la primera y la segunda realizaciones preferidas es que la etiqueta de identificación específica del M1 emitido por el primer AP 301 podría establecerse en "1110 1 42 (HEX)". La etiqueta de identificación específica podría usarse para disfrazar la identidad real del primer AP 301 como un terminal de cliente virtual (es decir, transformar el primer AP 301 en el terminal de cliente virtual) para conectarse al segundo AP 302. La etiqueta de pregunta de M2 podría establecerse en "R = (RND (x) % 0x10000), Qv = RC4 (R), Q = "1110 8 Qv", y la etiqueta de respuesta de M3 podría establecerse en "Obtener Q" la etiqueta es 1110 8 Qt, A1 = RC4 (Qt), Av = RC4 (A1 + 0x1223), A = 1110 8 AV". Después de recibir M3, el registrador 303 puede analizar la etiqueta de respuesta para verificar, la etiqueta "Obtener la etiqueta A' es 1110 8 At, A2 = RC4 (At), A3 = RC4 (Qv + 0x1223)". Si A2 = A3, la etiqueta de respuesta y la etiqueta de pregunta coinciden entre sí y el terminal de cliente virtual es auténtico, de modo que el WDS para el otro podría ser configurado por el M1 y M2 (direcciones MAC de cada uno) cuando el proceso WPS finaliza Si A2 ≠ A3, el proceso WPS se rompería (etapa 409B). Se observa que la etiqueta de identificación específica podría incluir un SSID específico.

Se observa que la misma etiqueta se utiliza en la primera y la segunda formas de realización preferidas pero los procedimientos de codificación y decodificación de los mismos son diferentes (es decir, Av = RC4 (A1 + 0x0718) y Av = RC4 (A1 + 0x1223)) a fin de lograr los efectos de la distinción y la seguridad. La etiqueta de pregunta y la etiqueta de respuesta en la segunda realización preferida también podrían codificarse mediante un cifrado Rivest 2 (RC2), un cifrado Rivest 4 (RC4), un cifrado Rivest 5 (RC5), un cifrado Rivest 6 (RC6), un estándar de encriptación avanzado (AES) u otros procedimientos de codificación. Además, después de que el primer AP 301 se transforma en el terminal de cliente virtual y gana el SSID y la dirección MAC del segundo AP 302 del M2, el terminal de cliente virtual podría transformarse de nuevo en el primer AP 301 en cualquier etapa del segundo realización para conectar el segundo AP 302.

Refiérase a la figura 5 que es un diagrama que muestra el tercer sistema de comunicación. El sistema de comunicación 500 incluye un primer nodo 501 y un segundo nodo 502. El segundo nodo 502 incluye además un registrador 5021. Consulte la figura 6 que es un diagrama de flujo que muestra la tercera realización preferida de la presente invención. La tercera realización preferida de la invención es un segundo procedimiento 600 para una conexión de red.

En primer lugar, el primer nodo 501 envía una etiqueta de identificación específica al segundo nodo 502 (etapa 601) y luego el segundo nodo 502 envía una etiqueta de pregunta al primer nodo 501 (etapa 602). Entonces, el primer nodo 501 envía una etiqueta de respuesta al segundo 502 (etapa 603). Finalmente, se determina si la etiqueta de pregunta y la etiqueta de respuesta se satisfacen con una regla específica (etapa 604). Si la etiqueta de pregunta y la etiqueta de respuesta se satisfacen con la regla específica, el primer nodo 501 se conecta al segundo nodo 502 (etapa 605A). Si la etiqueta de pregunta y la etiqueta de respuesta no son satisfechas con la regla específica, el primer nodo 501 no se puede conectar al segundo nodo 502 (etapa 605B). Se observa que el primer nodo 501 podría ser un AP o un terminal de cliente y el segundo nodo 502 podría ser un AP o un terminal de cliente. La regla

anterior podría realizarse basándose en si el primer nodo 501 y el segundo nodo 502 coinciden o no. Las etiquetas podrían incluirse respectivamente en diferentes mensajes. La etiqueta de identificación específica podría incluir un SSID específico y el mensaje que incluye la etiqueta de identificación específica podría tener un SSID normal en lugar del SSID específico. Para el otro ejemplo, el mensaje con la etiqueta de identificación específica podría incluir además un SSID y una dirección MAC del primer nodo 501, el mensaje con la etiqueta de pregunta podría incluir además un SSID y una dirección MAC del segundo nodo 502, y estos los mensajes son mensajes de registro. Además, el registrador 5021 podría configurarse fuera del segundo nodo 502.

En base a la realización anterior, se podría usar una etiqueta de identificación específica en el proceso de conexión. No solo hace que la conexión de red sea más fácil y conveniente, sino que también mejora la seguridad, e incluso no tiene conflictos con la arquitectura de sistema existente.

REIVINDICACIONES

1. Un procedimiento (600) para conectar un primer nodo (501) y un punto (102) de acceso AP, cuando, bajo el marco de configuración de Wi-Fi protegido, se presiona un botón de configuración de botón virtual o real, que comprende las etapas de:

(A) enviar (601) una etiqueta de identificación específica, un identificador de conjunto de servicios (SSID) y una dirección MAC desde el primer nodo (501) al punto (102) de acceso AP y desde el punto (102) de acceso AP a un registrador (103), en el que la etiqueta de identificación específica incluye un identificador de conjunto de servicios específico (SSID) para informar al punto (102) de acceso (AP) que se conecte para el SSID específico, y la etiqueta de identificación específica nunca se utiliza en definiciones actuales e configuración protegida Wi-Fi (WPS);
(B) enviar (602) una etiqueta de pregunta, un identificador de conjunto de servicios (SSID) y una dirección MAC desde el registrador (103) al primer nodo (501);
(C) enviar (603) una etiqueta de respuesta desde el primer nodo (501) al registrador (103); y
(D) conectando (604) el primer nodo (501) al punto (102) de acceso AP si la etiqueta de pregunta y la etiqueta de respuesta se satisfacen con una regla específica, donde la regla específica incluye determinar si la etiqueta de pregunta y la etiqueta de respuesta son coincidentes mediante el registrador (103).

2. El procedimiento (600) según la reivindicación 1, **caracterizado porque** el primer nodo (501) es uno de entre un primer punto de acceso y un primer terminal de cliente, el segundo nodo (502) es uno de un segundo punto de acceso y un segundo cliente terminal, el segundo nodo (502) comprende además un registrador (5021) para determinar si la etiqueta de pregunta y la etiqueta de respuesta se satisfacen con la regla específica, y la etiqueta de pregunta y la etiqueta de respuesta se codifican mediante un procedimiento de codificación seleccionado de una grupo compuesto por un cifrado Rivest 2 (RC2), un cifrado Rivest 4 (RC4), un cifrado Rivest 5 (RC5), un cifrado Rivest 6 (RC6) y un estándar de encriptación avanzada (AES).

3. El procedimiento (600) según las reivindicaciones 1 o 2, **caracterizado** además **porque** comprende las etapas de:

(D0) determinar (604) si la etiqueta de pregunta y la etiqueta de respuesta coinciden; y
(D1) conectar (605A) el primer nodo (501) y el segundo nodo (502) si la determinación de la etapa (D0) es positiva.

4. El procedimiento (600) según la reivindicación 1, **caracterizado porque** el primer nodo (501) es un terminal (101) de cliente y el segundo nodo (502) es el AP (102) acoplado al registrador (103), y el procedimiento (600) se **caracteriza** además **por** las etapas de:

(A1) enviar (204 y 205) un primer mensaje que tiene la etiqueta de identificación específica desde el terminal (101) de cliente al registrador a través del AP (102);
(B1) enviar (206) un segundo mensaje que tiene la etiqueta de pregunta del registrador (103) al terminal de cliente (102);
(C1) enviar (207) un tercer mensaje que tiene la etiqueta de respuesta desde el terminal (101) de cliente al registrador (103);
(D0) determinar (208) si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí en el registrador (103); y
(D1) si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí, enviando (209A) una configuración WiFi-privada del registrador (103) al terminal (101) de cliente para conectar el terminal (101) de cliente al AP (102).

5. El procedimiento (600) según la reivindicación 4, **caracterizado porque** la etapa (A1) comprende además una etapa (A11) de envío (203) de una solicitud de sonda desde el terminal (101) de cliente al AP (102) después de que el terminal (101) de cliente confirma que el AP (102) envía una baliza.

6. El procedimiento (600) según las reivindicaciones 4 o 5, **caracterizado porque** el primer mensaje comprende además el identificador de conjunto de servicios (SSID) y una dirección de control de acceso a medios (MAC) del terminal cliente, y el segundo mensaje comprende además un SSID y una dirección MAC del registrador (103).

7. El procedimiento (600) según una cualquiera de las reivindicaciones 4 a 6, **caracterizado porque** la etapa (D1) comprende además una etapa (D11) de establecer un sistema de distribución inalámbrica (WDS) según el primer mensaje y el segundo mensaje si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí, o cesan (209B) el procedimiento de configuración protegida de Wi-Fi (WPS) si el resultado de la etapa (D1) es negativo.

8. El procedimiento (600) según una cualquiera de las reivindicaciones 4 a 7, **caracterizado porque** el primer, el segundo y el tercer mensaje son mensajes de registro y la etiqueta de identificación específica incluye un SSID específico.

9. El procedimiento (600) según la reivindicación 1, **caracterizado porque** el primer nodo (501) es un primer punto (301) de acceso (AP) y el segundo nodo (502) es un segundo punto (302) de acceso (AP) acoplado a un registrador

(303), y el procedimiento (600) se **caracteriza** además **por** las etapas de:

(A1) enviar (404 y 405) una etiqueta de identificación específica desde el primer AP (301) al registrador (303) a través del segundo AP (302);
(B1) enviar (406) una etiqueta de pregunta del registrador (303) al primer AP (301);
(C1) enviar (407) una etiqueta de respuesta del primer AP (301) al registrador (303);
(D0) determinar (408) si la etiqueta de pregunta y la etiqueta de respuesta coinciden entre sí en el registrador (303); y
(D1) conectando (409A) el primer AP (301) y el segundo AP (302) si la etiqueta de pregunta y la etiqueta de respuesta coinciden.

10. El procedimiento (600) según la reivindicación 9, **caracterizado porque** la etapa (A1) comprende además una etapa (A11) de transformación del primer AP (301) en un terminal (101) de cliente mediante la etiqueta de identificación específica.

11. El procedimiento (600) según las reivindicaciones 9 o 10, **caracterizado porque** la etiqueta de identificación específica se incluye en un primer mensaje y se envía desde el primer AP (301) al registrador (303) a través del segundo AP (302) en la etapa (A1), la etiqueta de pregunta se incluye en un segundo mensaje y se envía desde el registrador (303) al primer AP (301) en la etapa (B1), y la etiqueta de respuesta se incluye en un tercer mensaje y se envía desde el primer AP (301) al registrador (303) en la etapa (C1).

12. El procedimiento (600) según la reivindicación 11, **caracterizado porque** el primer mensaje comprende además un identificador de conjunto de servicios (SSID) y una dirección de control de acceso a medios (MAC) del primer AP, el segundo mensaje comprende además un SSID y una dirección MAC del registrador, y el primero, el segundo y el tercer mensaje son mensajes de registro.

13. El procedimiento (600) según una cualquiera de las reivindicaciones 9 a 12, **caracterizado porque** la etapa (D1) comprende además una etapa (D10) de configuración (409A) de un sistema de distribución inalámbrica (WDS) según el primer mensaje y el segundo mensaje para conectar el primer AP (301) al segundo AP (302).

14. El procedimiento (600) según una cualquiera de las reivindicaciones 9 a 13, **caracterizado porque** la etapa (D1) comprende además una etapa (D11) de envío de una configuración WiFi privada desde el registrador (303) al primer AP (301) para conectar el primer AP (301) con el segundo AP (302) si la etiqueta de pregunta y la etiqueta de respuesta coinciden, o para cesar (409B) un procedimiento de configuración protegida Wi-Fi (WPS) si la etiqueta de pregunta y la etiqueta de respuesta están desparejas.

15. El procedimiento (600) según una cualquiera de las reivindicaciones 1 a 14, **caracterizado** además **porque** comprende una etapa (E) de procesamiento de un procedimiento de configuración de botón pulsador (PCB).

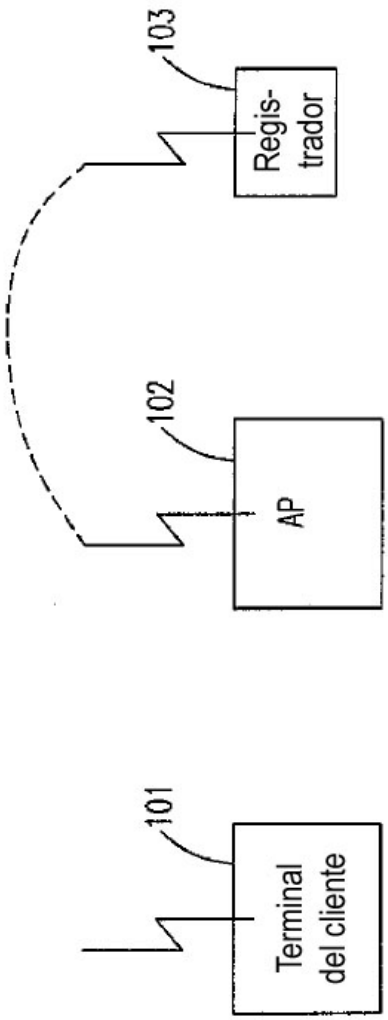

Fig. 1

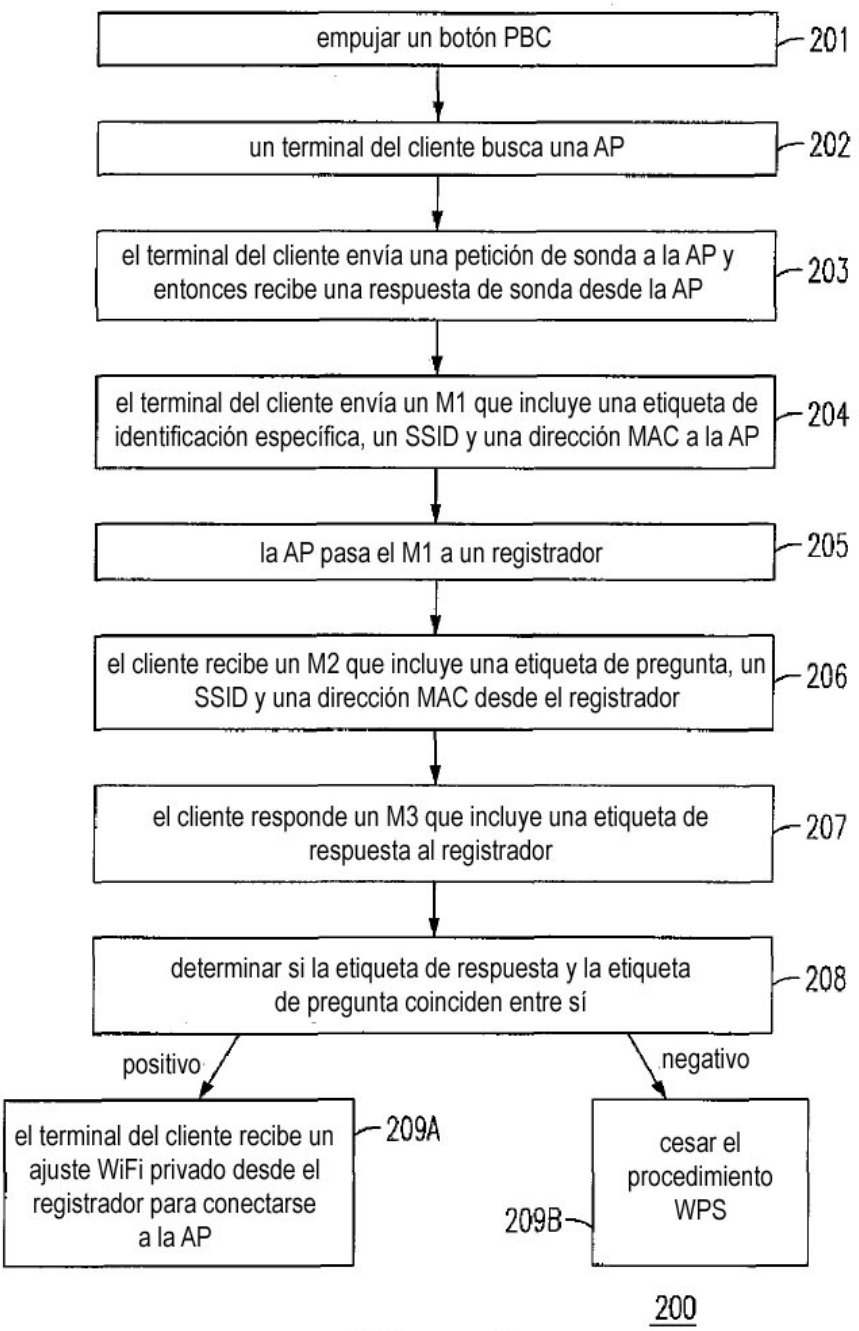
empujar un botón PBC
201
un terminal del cliente busca una AP
202
el terminal del cliente envía una petición de sonda a la AP y entonces recibe una respuesta de sonda desde la AP
203
el terminal del cliente envía un M1 que incluye una etiqueta de identificación específica, un SSID y una dirección MAC a la AP
204
la AP pasa el M1 a un registrador
205
el cliente recibe un M2 que incluye una etiqueta de pregunta, un SSID y una dirección MAC desde el registrador
206
el cliente responde un M3 que incluye una etiqueta de respuesta al registrador
207
determinar si la etiqueta de respuesta y la etiqueta de pregunta coinciden entre sí
208
positivo
negativo
el terminal del cliente recibe un ajuste WiFi privado desde el registrador para conectarse a la AP
209A
cesar el procedimiento WPS
209B
200

Fig. 2

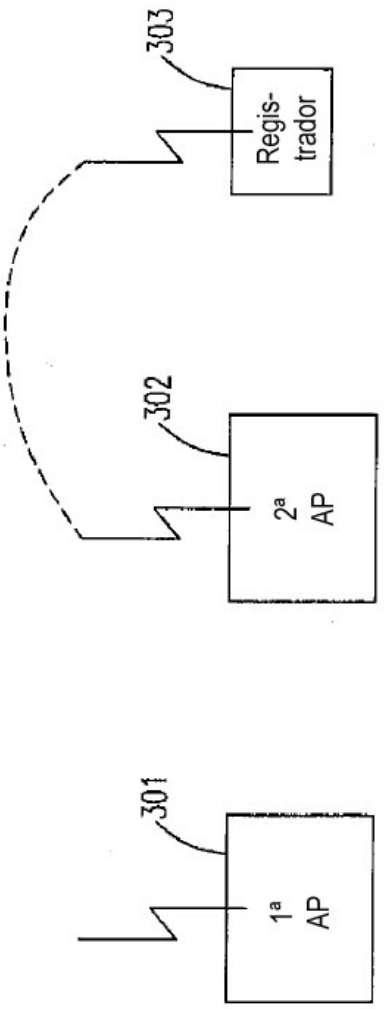

Fig. 3

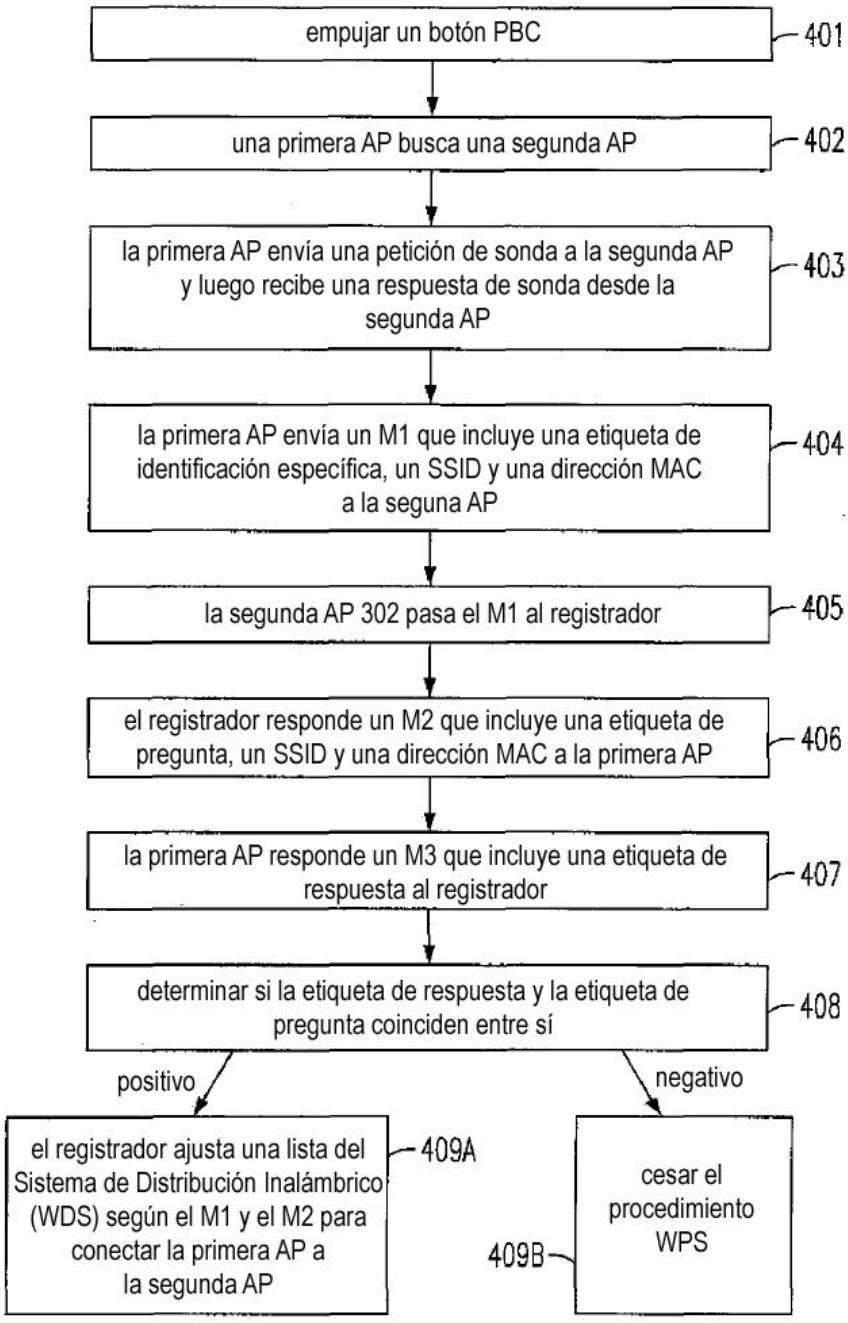
empujar un botón PBC
401
una primera AP busca una segunda AP
402
la primera AP envía una petición de sonda a la segunda AP y luego recibe una respuesta de sonda desde la segunda AP
403
la primera AP envía un M1 que incluye una etiqueta de identificación específica, un SSID y una dirección MAC a la seguna AP
404
la segunda AP 302 pasa el M1 al registrador
405
el registrador responde un M2 que incluye una etiqueta de pregunta, un SSID y una dirección MAC a la primera AP
406
la primera AP responde un M3 que incluye una etiqueta de respuesta al registrador
407
determinar si la etiqueta de respuesta y la etiqueta de pregunta coinciden entre sí
408
positivo
negativo
el registrador ajusta una lista del Sistema de Distribución Inalámbrico (WDS) según el M1 y el M2 para conectar la primera AP a la segunda AP
409A
cesar el procedimiento WPS
409B
400

Fig. 4

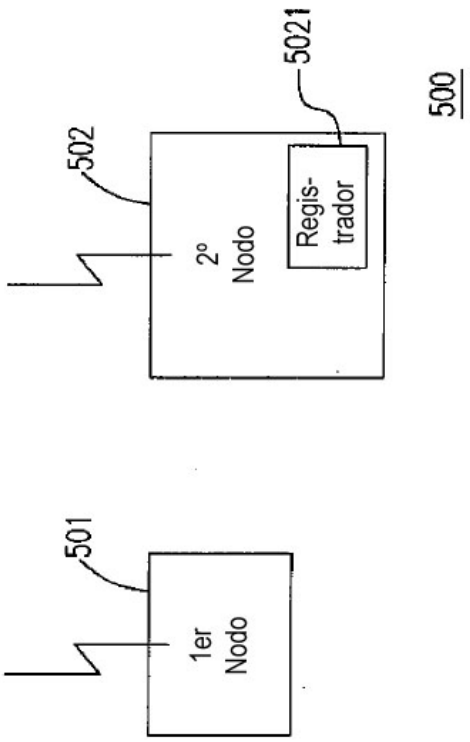

Fig. 5

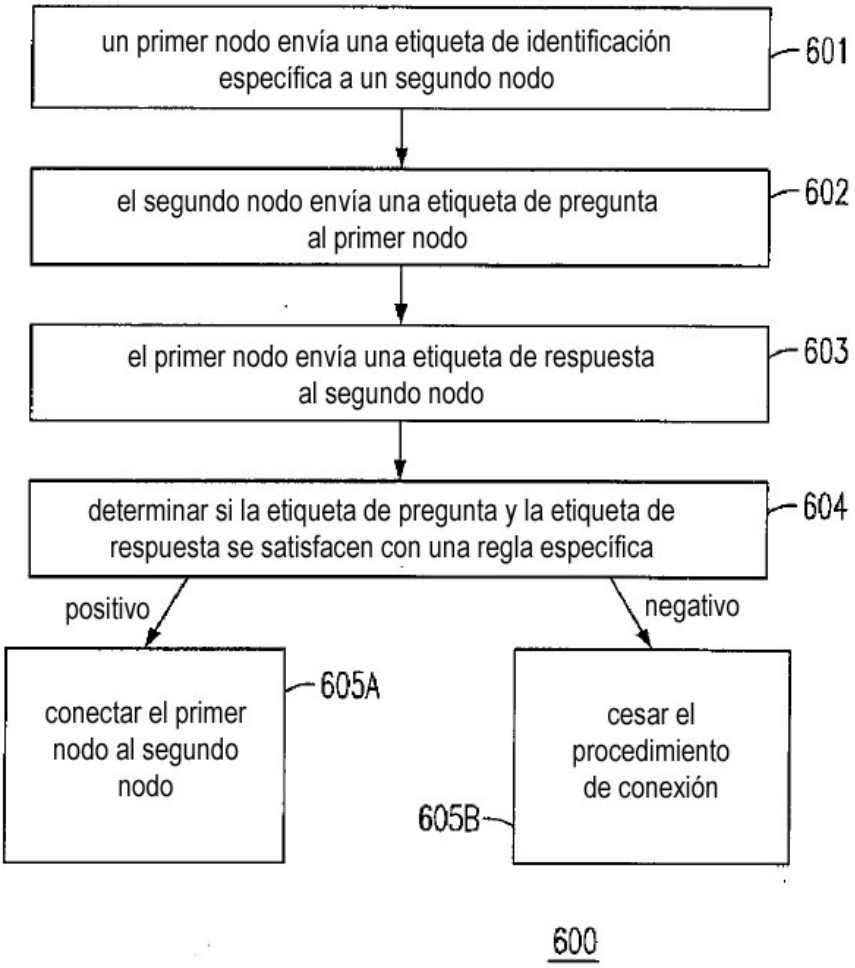
un primer nodo envía una etiqueta de identificación específica a un segundo nodo
601
el segundo nodo envía una etiqueta de pregunta al primer nodo
602
el primer nodo envía una etiqueta de respuesta al segundo nodo
603
determinar si la etiqueta de pregunta y la etiqueta de respuesta se satisfacen con una regla específica
604
positivo
negativo
conectar el primer nodo al segundo nodo
605A
cesar el procedimiento de conexión
605B
600

Fig. 6