(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 025 859**

(51) Int. Cl.:

H04W 76/10 (2008.01)
H04W 8/00 (2009.01)
H04W 84/12 (2009.01)
H04W 84/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.09.2009 E 22194308 (7)**

(97) Fecha y número de publicación de la concesión europea: **09.04.2025 EP 4149200**

(54) Título: **Aparato de comunicación, procedimiento de control del aparato de comunicación, programa informático y medio de almacenamiento**

(30) Prioridad:

06.10.2008 JP 2008259997

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.06.2025

(73) Titular/es:

CANON KABUSHIKI KAISHA (100.00%)
30-2, Shimomaruko 3-chome, Ohta-ku
Tokyo 146-8501, JP

(72) Inventor/es:

GOTO, FUMIHIDE y
SAKAI, TATSUHIKO

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Aparato de comunicación, procedimiento de control del aparato de comunicación, programa informático y medio de almacenamiento

SECTOR TÉCNICO

La presente invención se refiere a un aparato de comunicación, a un procedimiento y a un programa informático.

ESTADO DE LA TÉCNICA ANTERIOR

En las comunicaciones inalámbricas representadas por LAN inalámbricas que cumplen con la serie de estándares IEEE 802.11, existen muchos elementos de configuración que tienen que ser configurados antes de la utilización. Por ejemplo, dichos elementos de configuración incluyen parámetros de la comunicación necesarios para realizar comunicaciones inalámbricas, tales como un SSID como identificador de red, un procedimiento de cifrado, una clave de cifrado, un procedimiento de autenticación y una clave de autenticación, y es muy problemático para el usuario introducir manualmente estos parámetros.

Por ello, diversos fabricantes han propuesto procedimientos de configuración automática que permiten al usuario configurar fácilmente los parámetros de la comunicación en los aparatos inalámbricos. Con estos procedimientos de configuración automática, un aparato proporciona los parámetros de la comunicación a otro aparato utilizando procedimientos y mensajes, que están determinados de antemano, entre los aparatos a conectar, configurando, por lo tanto, automáticamente, los parámetros de la comunicación.

La Patente de la técnica anterior WO2008/093817 A1 da a conocer un aparato de comunicación configurado para buscar otra red tras la creación de una red, para participar en otra red de acuerdo con una función, en el procesamiento de la configuración de parámetros de comunicación, de un aparato de comunicación existente en otra red, y para ejecutar el procesamiento de la configuración de parámetros de comunicación. Después de que el aparato de comunicación decide recibir los parámetros de comunicación desde otro aparato de comunicación, el aparato de comunicación determina un estado de activación de una función de suministro de un aparato proveedor de los parámetros de la comunicación, y solicita al aparato proveedor que proporcione los parámetros de la comunicación según la determinación. La Patente japonesa abierta a inspección pública 2006-311139 (denominada referencia de patente 1 en lo sucesivo) da a conocer un ejemplo de procesamiento de configuración automática de los parámetros de la comunicación en una comunicación en un modo ad hoc de LAN inalámbrica (denominada comunicación ad hoc en lo sucesivo). El documento Wi-Fi CERTIFIED for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks, http://www.wi-fi.org/wp/wifi-protected-setup (en lo sucesivo, denominado referencia 1 no de patente) da a conocer la "Configuración protegida de Wi-Fi" (abreviada como WPS (Wi-Fi Protected Setup) en lo sucesivo) como la especificación estándar de la industria del procesamiento de configuración automática de los parámetros de la comunicación entre un punto de acceso (estación base) y una estación (estación terminal). Asimismo, el documento Wi-Fi Protected Access Enhanced Security Implementation Based on IEEE P802.11i standard (en lo sucesivo, denominado referencia 2 no de patente) da a conocer el "Acceso protegido de Wi-Fi" (en lo sucesivo, abreviado como WPA) como la especificación estándar de la industria de un procedimiento de cifrado, clave de cifrado, procedimiento de autenticación, clave de autenticación y similares en el procesamiento de la conexión de comunicación inalámbrica.

Con la WPS, puesto que las funciones de un aparato para proporcionar los parámetros de la comunicación (en lo sucesivo, denominado un aparato proveedor) y un aparato que recibe los parámetros de la comunicación (en lo sucesivo, denominado un aparato receptor) se determinan de antemano, la dirección de transferencia de los parámetros de la comunicación también se determina de manera única.

Sin embargo, cuando las funciones del aparato proveedor y del aparato receptor no se determinan de antemano, la dirección de transferencia de los parámetros de la comunicación no se puede determinar de manera única. En este caso, cuando el usuario selecciona un aparato para ser utilizado como un aparato proveedor y otro para ser utilizado como un aparato receptor, la operatividad del usuario se ve afectada.

Además, cuando se seleccionan una pluralidad de aparatos como aparatos proveedores, el aparato receptor no puede discriminar un aparato proveedor desde el que se van a recibir los parámetros de la comunicación.

Los problemas mencionados anteriormente también pueden ocurrir cuando se añade un nuevo aparato a una red ya construida entre una pluralidad de aparatos. En este caso, es deseable que un aparato que ya es un participante de la red sirva como aparato proveedor, y un nuevo aparato como posible participante reciba los parámetros de la comunicación de la red. Sin embargo, puesto que las funciones del aparato proveedor y del aparato receptor no están determinadas de antemano, no se pueden configurar parámetros de la comunicación apropiados en el nuevo aparato como posible participante.

Los problemas mencionados anteriormente también pueden ocurrir no solo en los parámetros de la comunicación de las comunicaciones inalámbricas sino también en los de las comunicaciones por cable que requieren configuraciones en las comunicaciones entre aparatos.

CARACTERÍSTICAS DE LA INVENCIÓN

La presente invención está definida por las reivindicaciones independientes. Las realizaciones ventajosas son el objeto de las reivindicaciones dependientes. Una realización de la presente invención da a conocer un aparato de comunicación que puede configurar parámetros de la comunicación apropiados sin perjudicar la operatividad del usuario, incluso cuando las funciones no están determinadas de antemano en el procesamiento de configuración automática de los parámetros de la comunicación, y un procedimiento de control del mismo.

Según un aspecto de la presente invención, tal como se reivindica, se da a conocer un aparato de comunicación que se puede conectar a una red de comunicación, que comprende: un medio de notificación, configurado para notificar la presencia de

el aparato de comunicación, utilizando un canal de comunicación asignado al aparato de comunicación entre los canales de comunicación disponibles para una comunicación inalámbrica, en el que en un primer período durante el cual el medio de notificación notifica la presencia del aparato de comunicación, el aparato de comunicación es capaz de recibir una señal de búsqueda de otro aparato de comunicación y de enviar a dicho otro aparato de comunicación una señal de respuesta de búsqueda en respuesta a dicha señal de búsqueda;
un medio de búsqueda, configurado para buscar otro aparato de comunicación mediante la transmisión de una señal de búsqueda utilizando un canal de búsqueda, en el que el canal de búsqueda es uno de los canales de comunicación disponibles para una comunicación inalámbrica;
un medio de control, configurado para controlar la realización del procesamiento por el medio de notificación durante el primer período, y para realizar el procesamiento por el medio de búsqueda para buscar otro aparato de comunicación después del primer período; en el que el medio de control está configurado para establecer el canal de búsqueda en un segundo canal de comunicación y controlar el medio de búsqueda para buscar otro aparato de comunicación utilizando el segundo canal de comunicación tras ejecutar una búsqueda de otro aparato de comunicación utilizando un primer canal de comunicación; en el que el canal de búsqueda utilizado para una búsqueda por el medio de búsqueda es cambiado intermitentemente, y el medio de control está configurado para controlar el medio de notificación de modo que la duración del primer período sea igual a la duración del intervalo de baliza o una duración aleatoria mayor que la del intervalo de baliza; y un medio proveedor, configurado para proporcionar información predeterminada, identificable por un usuario, para indicar el éxito de un procesamiento compartido para compartir un parámetro de comunicación con un aparato de comunicación asociado descubierto.

Según otro aspecto de la presente invención, no reivindicado, se da a conocer un aparato de comunicación que se puede conectar a una red de comunicación, que comprende:

un medio de notificación, para notificar la presencia del aparato de comunicación utilizando un canal de comunicación predeterminado de entre los canales de comunicación disponibles en la red de comunicación, en respuesta a una instrucción de inicio de procesamiento de configuración automática de los parámetros de la comunicación;
un medio de búsqueda, para buscar un aparato de comunicación asociado que funciona como un aparato proveedor que proporciona los parámetros de la comunicación utilizando el canal de comunicación predeterminado;
un medio de configuración, para ejecutar el procesamiento de configuración automática de los parámetros de la comunicación con el aparato de comunicación asociado encontrado por el medio de búsqueda; y
un medio de restauración, para restaurar el canal de comunicación a un canal de comunicación antes del inicio del procesamiento de configuración automática de los parámetros de la comunicación después de completar el procesamiento de la configuración automática de los parámetros de la comunicación.

Según otro aspecto de la presente invención, se da a conocer un procedimiento para controlar un aparato de comunicación que se puede conectar a una red de comunicación, que comprende:

una etapa de notificación, para notificar la presencia del aparato de comunicación utilizando un canal de comunicación asignado al aparato de comunicación, de entre los canales de comunicación disponibles para una comunicación inalámbrica, en el que, en un primer período durante el cual la etapa de notificación notifica la presencia del aparato de comunicación, el aparato de comunicación es capaz de recibir una señal de búsqueda de otro aparato de comunicación, y de enviar a dicho otro aparato de comunicación una señal de respuesta de búsqueda en respuesta a dicha señal de búsqueda; una etapa de búsqueda, para buscar otro aparato de comunicación mediante la transmisión de una señal de búsqueda utilizando un canal de

búsqueda, en el que el canal de búsqueda es uno de los canales de comunicación disponibles para una comunicación inalámbrica; una etapa de control, para controlar que la etapa de notificación se realice durante el primer período y la etapa de búsqueda se realice después del primer período, en el que la etapa de control controla la etapa de búsqueda para establecer el canal de búsqueda en un segundo canal de comunicación y buscar otro aparato de comunicación utilizando el segundo canal de comunicación tras ejecutar una búsqueda de otro aparato de comunicación utilizando un primer canal de comunicación, y en el que el canal de búsqueda utilizado para una búsqueda en la etapa de búsqueda es cambiado intermitentemente, y la etapa de control controla la etapa de notificación de modo que la longitud del primer período sea la duración del intervalo de baliza o una duración aleatoria mayor que la del intervalo de baliza; y una etapa de suministro para proporcionar información predeterminada identificable por un usuario para indicar el éxito de un procesamiento compartido para compartir un parámetro de comunicación con un aparato de comunicación asociado descubierto.

Según otro aspecto de la presente invención, no reivindicado, se da a conocer un procedimiento para controlar un aparato de comunicación que se puede conectar a una red de comunicación, que comprende:

una etapa de notificación, para notificar la presencia del aparato de comunicación utilizando un canal de comunicación predeterminado de entre los canales de comunicación disponibles en la red de comunicación en respuesta a una instrucción de inicio del procesamiento de configuración automática de los parámetros de la comunicación;
una etapa de búsqueda, para buscar un aparato de comunicación asociado que funcione como un aparato proveedor que proporcione los parámetros de la comunicación utilizando el canal de comunicación predeterminado;
una etapa de configuración de ejecución del procesamiento de configuración automática de los parámetros de la comunicación con el aparato de comunicación asociado encontrado en la etapa de búsqueda; y
una etapa de restauración, para restaurar el canal de comunicación a un canal de comunicación antes del inicio del procesamiento de configuración automática de los parámetros de la comunicación después de completar el procesamiento de configuración automática de los parámetros de la comunicación.

Otras características de la presente invención resultarán evidentes a partir de la siguiente descripción de las realizaciones a modo de ejemplo haciendo referencia a los dibujos adjuntos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama de bloques que muestra la disposición de un aparato de comunicación, según una realización de la presente invención;
la figura 2 es un diagrama de bloques que muestra funciones de software en el aparato, según la realización de la presente invención;
la figura 3 es un diagrama que muestra la primera disposición de la red, según la realización de la presente invención;
la figura 4 es un diagrama de secuencia que muestra las operaciones de los aparatos A y B, según la realización de la presente invención;
la figura 5 es un diagrama que muestra la segunda disposición de la red, según la realización de la presente invención;
la figura 6 es un diagrama de flujo que muestra la operación de procesamiento de notificaciones de un aparato proveedor, según la realización de la presente invención;
la figura 7 es un diagrama de flujo que muestra una operación de respuesta de proxy, según la realización de la presente invención;
la figura 8 es un diagrama de flujo que muestra una operación de configuración automática de los parámetros de la comunicación, según la realización de la presente invención;
la figura 9 es un diagrama de secuencia que muestra las operaciones de los aparatos A, B y C, según la realización de la presente invención;
la figura 10 es una tabla de procedimientos de autenticación y cifrado soportados;
la figura 11 es una tabla de comparación de claves poseídas y secuencias de intercambio de claves en algoritmos de intercambio de claves;
la figura 12 es un diagrama de secuencia (n.º 1) del procesamiento de intercambio de claves;
la figura 13 es un diagrama de secuencia (n.º 2) del procesamiento de intercambio de claves;
la figura 14 es un diagrama de secuencia (n.º 3) del procesamiento de intercambio de claves;
la figura 15 es un diagrama de secuencia (n.º 4) del procesamiento de intercambio de claves;
la figura 16 es un diagrama de flujo que muestra un algoritmo de selección de algoritmo de intercambio de claves;
la figura 17 es un diagrama de flujo que muestra una operación de procesamiento de descubrimiento del aparato proveedor, según la primera realización de la presente invención;
la figura 18 es un diagrama de flujo que muestra una operación de procesamiento de descubrimiento del aparato proveedor, según la segunda realización de la presente invención;

la figura 19 es un diagrama de temporización que muestra una operación general de procesamiento de descubrimiento de un aparato proveedor; y
la figura 20 es un diagrama de temporización que muestra una operación de procesamiento de descubrimiento de un aparato proveedor, según la presente invención.

MEJOR MODO DE REALIZACIÓN DE LA INVENCIÓN

<Primera Realización>

A continuación se describirá en detalle un aparato de comunicación según esta realización haciendo referencia a los dibujos. A continuación se describirá un ejemplo que utiliza un sistema de LAN inalámbrica compatible con la serie del estándar IEEE 802.11, pero un modo de comunicación no siempre está limitado a una LAN inalámbrica compatible con el estándar IEEE 802.11.

A continuación se describirá la disposición de hardware en un ejemplo de caso adecuado para esta realización.

La figura 1 es un diagrama de bloques que muestra un ejemplo de la disposición de un aparato de comunicación (aparato proveedor o aparato receptor) que puede ser conectado a una red de comunicación, según una realización de la presente invención. El número de referencia 101 indica un aparato completo. El número de referencia 102 indica una unidad de control que controla el aparato completo ejecutando un programa informático almacenado en una unidad de almacenamiento 103. La unidad de control 102 también ejecuta el control de la configuración de los parámetros de la comunicación con otro aparato. El número de referencia 103 indica una unidad de almacenamiento que almacena el programa informático que va a ejecutar la unidad de control 102, y diversos tipos de información, tal como los parámetros de la comunicación. Diversas operaciones que se describirán más adelante se implementan cuando la unidad de control 102 ejecuta el programa informático almacenado en la unidad de almacenamiento 103.

El número de referencia 104 indica una unidad inalámbrica utilizada para realizar comunicaciones inalámbricas. El número de referencia 105 indica una unidad de visualización que realiza diversas visualizaciones y tiene una función que puede generar información perceptible visualmente, como una pantalla LCD o de LED o puede generar información audible, como un altavoz.

El número de referencia 106 indica un botón de configuración que proporciona un activador para iniciar el procesamiento de configuración de los parámetros de la comunicación. La unidad de control 102 ejecuta el procesamiento que se describirá más adelante cuando detecta el accionamiento por parte del usuario del botón de configuración 106.

El número de referencia 107 indica una unidad de control de antena; y 108, una antena. El número de referencia 109 indica una unidad de entrada que permite al usuario realizar diversas entradas.

La figura 2 es un diagrama de bloques que muestra un ejemplo de la disposición de los bloques funcionales de software para ser ejecutados por los respectivos aparatos que se describirán más adelante en una operación de configuración de los parámetros de la comunicación que se describirá más adelante.

El número de referencia 201 indica un aparato completo. El número de referencia 202 indica un bloque funcional de la configuración automática de los parámetros de la comunicación. En esta realización, el bloque funcional 202 de la configuración automática de los parámetros de la comunicación configura automáticamente los parámetros de la comunicación requeridos para realizar comunicaciones inalámbricas, tal como un SSID como identificador de red, un procedimiento de cifrado, una clave de cifrado, un procedimiento de autenticación y una clave de autenticación.

El número de referencia 203 indica una unidad de recepción de paquetes que recibe paquetes asociados con diversas comunicaciones. La unidad 203 de recepción de paquetes recibe una baliza (señal de notificación). El número de referencia 204 indica una unidad de transmisión de paquetes que transmite paquetes asociados con diversas comunicaciones. La unidad 204 de transmisión de paquetes transmite una baliza. Cabe señalar que la baliza se agrega con diversos tipos de información (autoinformación) de un aparato de origen de transmisión.

El número de referencia 205 indica una unidad de transmisión de señales de búsqueda que controla la transmisión de una señal de búsqueda de aparato tal como una solicitud de sondeo. Cabe señalar que la solicitud de sondeo también se puede expresar como una señal de búsqueda de red utilizada para buscar una red deseada. La unidad 205 de transmisión de señales de búsqueda transmite la solicitud de sondeo. Además, la unidad 205 de transmisión de señales de búsqueda transmite una respuesta de sondeo como una señal de respuesta a la solicitud de sondeo recibida.

El número de referencia 206 indica una unidad de recepción de señales de búsqueda que controla la recepción de una señal de búsqueda de un aparato, tal como una solicitud de sondeo de otro aparato. La unidad 206 de recepción de señales de búsqueda recibe la solicitud de sondeo. Además, la unidad 206 de recepción de señales de búsqueda recibe una respuesta de sondeo. Cabe señalar que la señal de búsqueda del aparato y su señal de respuesta se suman con diversos tipos de información (autoinformación) de un aparato de origen de transmisión.

El número de referencia 207 indica una unidad de control de red que controla las conexiones de red. La unidad 207 de control de red ejecuta, por ejemplo, el procesamiento de la conexión a una red ad hoc de LAN inalámbrica.

En el bloque funcional de configuración automática de los parámetros de la comunicación, el número de referencia 208 indica una unidad de control de la configuración automática que controla diversos protocolos en el procesamiento de configuración automática de los parámetros de la comunicación.

El número de referencia 209 indica una unidad de suministro de los parámetros de la comunicación que proporciona los parámetros de la comunicación a un aparato asociado. La unidad 209 de suministro de los parámetros de la comunicación lleva a cabo el procesamiento de suministro en el procesamiento de configuración automática de los parámetros de la comunicación (que se describirá más adelante) bajo el control de la unidad 208 de control de configuración automática. El número de referencia 210 indica una unidad de recepción de los parámetros de la comunicación que recibe los parámetros de la comunicación de un aparato asociado. La unidad de recepción de los parámetros de la comunicación 210 ejecuta el procesamiento de recepción en el procesamiento de configuración automática de los parámetros de la comunicación (que se describirá más adelante) bajo el control de la unidad 208 de control de configuración automática.

La unidad 208 de control de configuración automática también determina si un período de tiempo transcurrido después del inicio del procesamiento de configuración automática de los parámetros de la comunicación supera o no un tiempo límite de ese procesamiento de configuración. Cuando se determina que el período de tiempo transcurrido supera el tiempo límite, el procesamiento de configuración se cancela bajo el control de la unidad 208 de control de configuración automática.

El número de referencia 211 indica una unidad de determinación de funciones que determina una función en el procesamiento de configuración automática de los parámetros de la comunicación. La unidad de determinación de funciones 211 ejecuta el procesamiento de determinación de funciones que se describirá más adelante.

El número de referencia 212 indica una unidad de control de notificación de configuración que controla el procesamiento asociado con las notificaciones de inicio y finalización del procesamiento de configuración automática de los parámetros de la comunicación. La unidad 212 de control de notificación de configuración ejecuta el procesamiento de transmisión/recepción de un mensaje de notificación de inicio, un mensaje de respuesta de notificación de inicio y un mensaje de notificación de finalización en un aparato proveedor que se describirá más adelante.

El número de referencia 213 indica una unidad de control de baliza que controla los tiempos de transmisión de una baliza (señal de notificación). A continuación se describirá un algoritmo de transmisión de baliza en una red ad hoc de una LAN inalámbrica del estándar IEEE 802.11.

Las balizas son transmitidas de manera autónoma distribuida en la red ad hoc entre todos los aparatos que configuran la red. Un intervalo de transmisión de baliza (ciclo de baliza) está determinado por un aparato que creó primero la red ad hoc, y las balizas son transmitidas normalmente desde aparatos arbitrarios en un intervalo de aproximadamente 100 ms. Cabe señalar que la red ad hoc se forma cuando un aparato arbitrario comienza a transmitir balizas.

Los tiempos de transmisión de balizas están controlados por un parámetro denominado ventana de contienda (un intervalo de generación de números aleatorios; en lo sucesivo abreviado como CW (Contention Window). Cuando se alcanza un tiempo de transmisión de baliza, cada aparato en la red calcula un valor aleatorio (CWrand) dentro del intervalo comprendido entre 0 y la CW. Un período de tiempo obtenido al multiplicar un intervalo constante predeterminado (tiempo de ranura) por este CWrand se configura como un período de tiempo de espera (período de tiempo de retroceso) hasta la transmisión de la baliza.

Puesto que el período de tiempo de espera hasta la transmisión de la baliza se reduce en el intervalo de tiempo, cuando el período de tiempo de espera llega a cero, se transmite una baliza. Si el aparato recibe una baliza de otro aparato antes de transmitir una baliza, el aparato aborta el procesamiento de transmisión de una baliza.

Con este control, se pueden evitar colisiones de balizas transmitidas desde los respectivos aparatos. Puesto que los respectivos aparatos en la red ad hoc seleccionan números aleatorios dentro del intervalo comprendido entre 0 y CW, un aparato, que selecciona un CWrand más pequeño, de entre los que configuran la red, transmite una baliza.

Por ejemplo, cuando se configura una CW idéntica en los aparatos respectivos como valor inicial, los aparatos respectivos tienen las mismas probabilidades de transmisión de baliza y, como resultado, el número de veces que los aparatos respectivos transmiten balizas por unidad de tiempo resulta ser casi el mismo. En otras palabras, las frecuencias de transmisión (relaciones de transmisión) de las balizas por parte de los aparatos respectivos resultan ser iguales.

Por otro lado, cuando un aparato en la red configura la CW en un valor más pequeño que el valor inicial, la probabilidad de que este aparato transmita una baliza se vuelve más alta que para otros aparatos. Es decir, la CW se puede expresar como un parámetro utilizado para determinar la probabilidad de que se transmita una baliza o el número de veces que se transmiten las balizas por unidad de tiempo.

Asimismo, la CW se puede expresar como un parámetro utilizado para determinar la relación de transmisión de las balizas transmitidas por cada aparato. Además, la CW también se puede expresar como un parámetro utilizado para determinar el tiempo de transmisión de la baliza o un período de tiempo de espera hasta la transmisión de la baliza.

Cabe señalar que el valor de CW puede ser cambiado dentro del intervalo de CWmin (valor mínimo) a CWmax (valor máximo). Cuando se configura la CWmin, se maximiza la cantidad de veces que se transmiten las balizas por unidad de tiempo. En cada aparato, CWinit (>CWmin) se configura como un valor inicial, y las balizas son transmitidas utilizando el valor inicial mientras no se ejecuta ningún procesamiento de configuración automática de los parámetros de la comunicación.

La figura 3 es un diagrama que muestra un aparato de comunicación A 300 (denominado aparato A en lo sucesivo) y un aparato de comunicación B 301 (denominado aparato B en lo sucesivo). Todos estos aparatos tienen las disposiciones que se muestran en las figuras 1 y 2 descritas anteriormente.

Ambos aparatos A y B crean respectivamente una red A 302 (a la que se hará referencia como red A en lo sucesivo) y una red B 303 (a la que se hará referencia como red B en lo sucesivo) en un estado en el que no está determinado si funcionan como un aparato proveedor de los parámetros de la comunicación o como un aparato receptor.

Los aparatos A y B descubren el aparato del otro y determinan qué aparato funciona como aparato proveedor. Como resultado, el aparato que funciona como aparato proveedor proporciona los parámetros de la comunicación al que funciona como aparato receptor.

Las redes A y B son redes ad hoc creadas, respectivamente, por los aparatos A y B. La red ad hoc se denomina IBSS (Independent Basic Service Set, Conjunto de Servicios Básicos Independientes), y las redes respectivas se distinguen utilizando varios BSSID como identificadores de red. El BSSID es un identificador de red que adopta un valor aleatorio generado por un aparato que crea una red. Cabe señalar que un SSID es un identificador de red que puede estar configurado de antemano en un aparato o que el usuario puede configurar como un valor arbitrario, y es diferente del BSSID. Tal como se puede ver a partir de la descripción anterior, el BSSID no es un parámetro de la comunicación que se proporciona desde el aparato proveedor al aparato receptor mediante el procesamiento de configuración automática de los parámetros de la comunicación.

La figura 4 es un gráfico que muestra un ejemplo de la secuencia de procesamiento cuando se pulsan los botones de configuración 106 en los aparatos A y B, y el procesamiento de configuración automática de los parámetros de la comunicación se ejecuta entre los aparatos A y B.

Cuando los botones de configuración 106 son pulsados respectivamente en los aparatos A y B, el aparato A crea una red A única (F401), y el aparato B también crea una red B única (F402). Supóngase que el botón de configuración 106 del aparato B es pulsado antes, y el aparato B crea una red primero.

Cada uno de los aparatos A y B es configurado como “candidato a aparato proveedor” indicando que su función de operación (a la que se hará referencia como función en lo sucesivo) no se configura como un aparato proveedor ni un aparato receptor (F403, F404), y se inicia un temporizador T1 como un tiempo límite hasta que se determine la función de operación (F405, F406).

Los aparatos A y B transmiten balizas (señales de notificación) (F407, F408). Una señal de baliza incluye un elemento de información que notifica que el aparato tiene una función de procesamiento de configuración automática de los parámetros de la comunicación en la red creada, o que el procesamiento de configuración

automática está en curso. Asimismo, la baliza también puede incluir un elemento de información que indique "candidato a aparato proveedor" como la función actual.

Puesto que estas balizas incluyen diferentes BSSID en correspondencia con las redes A y B, el aparato que recibió la baliza puede reconocer una red a la que pertenece el aparato de origen de transmisión de esa baliza.

Posteriormente, el aparato B transmite la señal de búsqueda A (F409). La señal de búsqueda A también incluye un elemento de información que indica que el aparato tiene una función de procesamiento de configuración automática de los parámetros de la comunicación, o que el procesamiento de configuración automática está en curso, y un elemento de información que indica "candidato a aparato proveedor" como función actual, como en la baliza.

Tras la recepción de la señal A de búsqueda transmitida desde el aparato B, el aparato A transmite la señal A de respuesta de búsqueda al aparato B (F410). La señal A de respuesta de búsqueda también incluye un elemento de información que indica que el aparato tiene una función de procesamiento de configuración automática de los parámetros de la comunicación o que el procesamiento de configuración automática está en curso, y un elemento de información que indica "candidato a aparato proveedor" como función actual, como en la baliza y la señal A de búsqueda.

Cuando el temporizador T1 del aparato B ha alcanzado un límite de tiempo antes de que se detecte ningún aparato proveedor (F411), el aparato B configura "aparato proveedor" como su función de operación (F412).

El aparato A transmite a su vez la señal A de búsqueda (F413). La señal A de búsqueda transmitida desde el aparato A también incluye un elemento de información que indica que el aparato tiene una función de procesamiento de configuración automática de los parámetros de la comunicación o el procesamiento de configuración automática está en progreso, y un elemento de información que indica "candidato a aparato proveedor" como la función actual.

Tras la recepción de la señal A de búsqueda transmitida desde el aparato A, el aparato B transmite la señal B de respuesta de búsqueda al aparato A (F414). La señal B de respuesta de búsqueda incluye un elemento de información que indica que el aparato tiene una función de procesamiento de configuración automática de los parámetros de la comunicación o que el procesamiento de configuración automática está en curso, y la función actual, como en la baliza y la señal A de búsqueda. En este momento, puesto que el aparato B determina "aparato proveedor" como función operativa, la señal B de respuesta de búsqueda incluye un elemento de información que indica "aparato proveedor". Además del elemento de información que indica "aparato proveedor" como función, se puede añadir un elemento de información que indica que el aparato está listo para proporcionar los parámetros de la comunicación.

El aparato A recibe la señal B de respuesta de búsqueda transmitida desde el aparato B, y confirma que la función del aparato B es "aparato proveedor", y el aparato B está listo para proporcionar los parámetros de la comunicación. Por lo tanto, el aparato A detiene el temporizador T1 (F415), configura "aparato receptor" como su función (F416) y participa en la red B creada por el aparato B (F417). Entonces, los aparatos A y B pueden intercambiar mensajes de comunicación (mensajes de protocolo) para ser intercambiados en el procesamiento del protocolo de configuración automática de los parámetros de la comunicación.

Cabe señalar que el procesamiento de protocolo de configuración automática significa procesamiento que intercambia diversos mensajes de comunicación que están configurados de antemano para proporcionar los parámetros de la comunicación desde un aparato proveedor a un aparato receptor. Cabe señalar que la WPS denomina a este procesamiento de protocolo "Protocolo de registro" (véase la referencia 1 no de patente). En la siguiente descripción de esta realización, por razones de sencillez, el aparato receptor transmite un mensaje de activación de la configuración de los parámetros de la comunicación al aparato proveedor, y el aparato proveedor ejecuta el procesamiento de suministro de los parámetros de la comunicación al aparato receptor en respuesta a este mensaje. A continuación, tras la finalización del procesamiento de suministro de los parámetros de la comunicación, el aparato proveedor transmite un mensaje de finalización de configuración de los parámetros de la comunicación.

Cuando el aparato A participa en la red B en F417, puesto que los parámetros de la comunicación tales como una clave de cifrado y una clave de autenticación no están configurados en el aparato A, los aparatos A y B no pueden establecer comunicaciones utilizando cifrado y autenticación.

Cabe señalar que tras la determinación de la función de aparato proveedor de los parámetros de la comunicación o de aparato receptor entre los aparatos A y B, se utilizan la señal de búsqueda y la señal de respuesta de búsqueda.

Sin embargo, en lugar de intercambiar la señal de búsqueda y la señal de respuesta de búsqueda, las funciones pueden ser determinadas utilizando información de balizas que se intercambian entre sí.

Cuando el aparato A participa en la red creada por el aparato B, transmite un mensaje de activación de la configuración de los parámetros de la comunicación al aparato B (F418), y el aparato B, como aparato proveedor, ejecuta el procesamiento de suministro de los parámetros de la comunicación al aparato A como aparato receptor (F419). Tras la finalización del procesamiento de suministro de los parámetros de la comunicación, el aparato B transmite un mensaje de finalización de configuración de los parámetros de la comunicación al aparato A (F420). A continuación, se completa el procesamiento de configuración de los parámetros de la comunicación, y los parámetros de la comunicación son compartidos entre los aparatos A y B.

A continuación, los aparatos A y B ejecutan el procesamiento de conexión de la comunicación utilizando los parámetros de la comunicación compartidos (F421).

Cabe señalar que puesto que el procesamiento de la conexión de comunicación se inicia simultáneamente con el final del procesamiento de la configuración de los parámetros de la comunicación, los aparatos A y B pueden comunicarse entre sí sin obligar al usuario a realizar ninguna operación. En este caso, un aparato puede transmitir una señal de solicitud de conexión que indica explícitamente el inicio del procesamiento de la conexión de comunicación. En el modo ad hoc, aunque no se ejecuta ningún procesamiento de asociación a diferencia de un modo de infraestructura, el aparato, como origen de la solicitud de conexión, puede ser reconocido rápidamente tras la recepción de la señal de solicitud de conexión.

En esta realización, el aparato B transmite los parámetros de la comunicación de la red B al aparato A, y el procesamiento de la conexión de comunicación se ejecuta utilizando estos parámetros de la comunicación. En este caso, cuando el aparato A transmite una señal de solicitud de conexión al aparato B, el aparato B puede detectar que el aparato A participa en la red B y también puede obtener fácilmente el número de participantes.

Antes del inicio del procesamiento de la conexión de comunicación, el aparato puede confirmar con el usuario si desea o no iniciar la conexión, y puede iniciar el procesamiento de la conexión de comunicación según la operación del usuario. Por ejemplo, tras la finalización del procesamiento de configuración de los parámetros de la comunicación, la unidad de visualización 105 puede mostrar un mensaje que solicita al usuario que seleccione si iniciar o no la conexión, y el procesamiento de la conexión de comunicación puede ser iniciado según la entrada del usuario desde la unidad de entrada 109.

El aparato B puede transmitir, al aparato A, parámetros de comunicación que indican una red diferente de la red B. Por ejemplo, el aparato B puede proporcionar los parámetros de la comunicación necesarios para comunicarse mediante la red C al aparato A, y los aparatos A y B pueden comunicarse entre sí mediante la red C después del procesamiento de suministro. En este caso, el aparato A o B puede iniciar el procesamiento de la conexión de la comunicación en respuesta a la detección del otro aparato en la red C como activador.

La figura 8 es un diagrama de flujo que muestra un ejemplo de la secuencia de funcionamiento ejecutada cuando se pulsan los botones de configuración 106 en los aparatos A y B, se determinan las funciones de operación de los aparatos A y B, es decir, aparato proveedor y aparato receptor, y se realiza a continuación el procesamiento de configuración automática de los parámetros de la comunicación.

El control ejecutado por estos dos aparatos se describirá a continuación haciendo referencia a este diagrama de flujo.

El botón de configuración 106 se pulsa para indicar el inicio del procesamiento de configuración de los parámetros de la comunicación (S801).

El aparato en el que se ha pulsado el botón de configuración 106 comprueba si ya es participante de una red en ese momento (S802). El aparato es un participante de una red cuando configura la red utilizando parámetros de la comunicación compartidos por el procesamiento de configuración de los parámetros de la comunicación que ya ha sido realizado con otro aparato. Si el aparato ya es un participante de la red, configura “aparato proveedor” como su función para controlar otro nuevo aparato para participar en la red participante (S815). A continuación, el aparato comienza a transmitir balizas que incluyen, por ejemplo, información que indica que la función es “aparato proveedor” (S816).

Después de eso, tras la recepción de un mensaje de activación de la configuración de los parámetros de la comunicación desde un nuevo aparato como posible participante de la red, el aparato inicia el procesamiento de suministro de los parámetros de la comunicación (S817). Es decir, en el procesamiento de suministro de los parámetros de la comunicación iniciado en la etapa S817, cuando el aparato ya es un participante de la

red, el aparato proporciona los parámetros de la comunicación de la red de la que ese aparato es un participante. Cabe señalar que, cuando el aparato ya es un participante de la red en la actualidad, lanza el procesamiento de notificación de inicio que se muestra en la figura 6 (que se describirá más adelante). Supóngase que una baliza (señal de notificación), una señal de búsqueda (solicitud de sondeo) y una señal de respuesta de búsqueda (respuesta de sondeo) incluyen los siguientes elementos de información como elementos obligatorios u opciones según las señales:

- un elemento de información, que notifica que el aparato tiene una función de procesamiento de configuración automática de los parámetros de la comunicación o que el procesamiento de configuración automática está en curso;
- un elemento de información, que indica la función del aparato; y
- un elemento de información, que indica si una función de suministro está activa o no.

Si se determina en la etapa S802 que el aparato no participa en ninguna red, ese aparato crea una red por sí mismo para determinar la función de operación (S803), configura "candidato a aparato proveedor" como la función (S804) y activa el procesamiento de descubrimiento de aparato proveedor que se describirá más adelante (S805). Cabe señalar que el aparato crea una red en un canal arbitrario de la LAN inalámbrica en la etapa S803. Cabe señalar que el canal de la LAN inalámbrica es un canal de comunicación (canal de frecuencia) autorizado para ser utilizado en las comunicaciones de la LAN inalámbrica. Por ejemplo, en el caso de una LAN inalámbrica compatible con el estándar IEEE 802.11g, los canales de comunicación comprendidos entre el canal 1 y el canal 13 están disponibles en Japón. El procesamiento de descubrimiento de aparato proveedor en la etapa S805 se describirá más adelante haciendo referencia a las figuras 17, 19 y 20.

Como resultado del procesamiento de descubrimiento del aparato proveedor, si se descubre un aparato que tiene "aparato proveedor" como su función (S806), el aparato configura "aparato receptor" como su función (S807), y participa en una red creada por el aparato proveedor (S808). Después de que el aparato participa en la red, el aparato comienza a transmitir balizas que incluyen información que indica que la función es "aparato receptor" (S809). Cabe señalar que, puesto que el aparato no recibe ningún parámetro de comunicación proporcionado por el aparato proveedor en este momento, no puede realizar comunicaciones utilizando cifrado y autenticación en la red en la que ese aparato se ha convertido en participante. El aparato que se ha convertido en un participante de la red transmite un mensaje de activación de la configuración de los parámetros de la comunicación al aparato proveedor, para solicitar que proporcione los parámetros de la comunicación, y comienza a recibir el procesamiento de los parámetros de la comunicación desde el aparato proveedor (S810).

Por otro lado, si un aparato que tiene "aparato proveedor" como función no puede ser descubierto como resultado del procesamiento de descubrimiento de aparato proveedor (S806), el aparato configura "aparato proveedor" como función del aparato (S815). A continuación, el aparato comienza a transmitir balizas que incluyen información que indica que la función es "aparato proveedor" (S816), y comienza el procesamiento de suministro de los parámetros de la comunicación tras la recepción de un mensaje de activación de la configuración de los parámetros de la comunicación desde el aparato receptor (S817). En el procesamiento de suministro de los parámetros de la comunicación iniciado en la etapa S817, el aparato proporciona los parámetros de la comunicación de la red creada en la etapa S803 si el aparato no es un participante de ninguna red.

Por otra parte, el aparato, cuya función es "aparato receptor" y que ha comenzado el procesamiento de recepción de los parámetros de la comunicación desde el aparato proveedor, confirma si el procesamiento de recepción de los parámetros de la comunicación se ha completado (S811). Si se completa el procesamiento de recepción de los parámetros de la comunicación, ese aparato realiza una pantalla que indica el éxito del procesamiento de configuración de los parámetros de la comunicación para que el usuario pueda identificarlo controlando la unidad de visualización 105 para mostrar un mensaje en una pantalla LCD, para que parpadee o se encienda un LED, para cambiar el color del LED o para generar un sonido (S814) arbitrario, finalizando de este modo el procesamiento (S822). Si ha ocurrido un error (S812), el aparato notifica el error para que sea identificable por parte del usuario controlando de manera similar la unidad de pantalla 105 para mostrar un mensaje en una pantalla LCD, para que parpadee o se encienda un LED, cambie el color del LED o genere un sonido (S813) arbitrario, finalizando de este modo el procesamiento (S822).

Por otro lado, el aparato, cuya función es "aparato proveedor" y que ha iniciado el procesamiento de suministro de los parámetros de la comunicación, confirma si el procesamiento de suministro de los parámetros de la comunicación se ha completado (S818). Si el procesamiento de suministro de los parámetros de la comunicación se ha completado, ese aparato realiza una pantalla que indica el éxito del procesamiento de configuración de los parámetros de la comunicación para que el usuario pueda identificarlo controlando la unidad de visualización 105 para mostrar un mensaje en una pantalla LCD, para que parpadee o se encienda un LED, para cambiar el color del LED o para generar un sonido (S821) arbitrario, finalizando de este modo el procesamiento (S822). Si ha ocurrido un error (S819), el aparato notifica el error para que

sea identificable por el usuario controlando la unidad de pantalla 105 para mostrar un mensaje en una pantalla LCD, para que parpadee o se encienda un LED, cambie el color del LED o genere un sonido (S820) arbitrario, finalizando de este modo el procesamiento (S822).

La figura 17 es un diagrama de flujo que muestra un ejemplo de la secuencia de funcionamiento tras la ejecución del procesamiento de descubrimiento del aparato proveedor en la etapa S805 de la figura 8. El control del procesamiento de descubrimiento del aparato proveedor se describirá a continuación haciendo referencia a este diagrama de flujo.

Cuando se inicia el procesamiento de descubrimiento del aparato proveedor, el aparato inicia el temporizador T1 (S1701). El aparato transmite balizas (señales de notificación) en un canal de comunicación en el que está creada la red (en lo sucesivo denominado canal propio) (S1702). Para determinar el intervalo de transmisión de una baliza en el canal propio y el de una señal de búsqueda (señal de sondeo) en otros canales de comunicación, el aparato determina el intervalo de baliza del canal propio (S1703). Después de que se transmite la señal de búsqueda (después del procesamiento de la etapa S1707 que se describirá más adelante), el aparato espera hasta el siguiente tiempo de transmisión de baliza determinado por el intervalo de baliza.

El aparato determina si el temporizador T1 ha alcanzado o no un tiempo límite (S1704). Si el temporizador T1 aún no ha alcanzado el límite de tiempo, el aparato transmite una baliza (señal de notificación) en el canal propio (S1705). Cabe señalar que el período de transmisión de la baliza puede estar determinado por la duración del intervalo de la baliza o por una duración aleatoria mayor.

El aparato configura un canal de búsqueda (S1706). Tras la configuración del canal de búsqueda, el aparato ejecuta, por ejemplo, el siguiente procesamiento. En el caso de una LAN inalámbrica compatible con el estándar IEEE 802.11g en Japón, los canales comprendidos entre el canal 1 y el canal 13 pueden ser utilizados como canales de la LAN inalámbrica. En esta realización, el procesamiento de configuración de canales se ejecuta como sigue. Es decir, en el primer procesamiento de configuración del canal de búsqueda, se configura el canal 1. A continuación, el número de canal se incrementa en incrementos de 1 canal hasta el canal 13 cada vez que se ejecuta el procesamiento en la etapa S1706. A continuación, en el procesamiento en la etapa S1706, después de configurar el canal 13, se configura de nuevo el canal 1. Cabe señalar que en EE. UU., puesto que los canales del canal 1 al canal 11 están disponibles, cuando el procesamiento de configuración se ejecuta a su vez desde el canal 1, como en Japón, el canal 1 se configura nuevamente en la siguiente etapa S1706 después de configurar el canal 11.

Además del procedimiento de cambio de canales en incrementos de un canal, también está disponible un procedimiento de cambio intermitente de canales. Debido a la propiedad de radio del estándar IEEE 802.11g, puesto que una onda de radio se filtra a los canales vecinos aunque sea débilmente, se puede recibir una señal de búsqueda transmitida en uno de los canales vecinos y se puede devolver una señal de respuesta. Por lo tanto, en el procesamiento de la configuración del primer canal, el canal 2 se configura como un canal de búsqueda, y se puede buscar un ancho de banda del canal 1 al canal 3. Es decir, se busca un aparato asociado de comunicación en un ancho de banda de tres canales para tener como centro el canal de comunicación configurado. Asimismo, en el procesamiento de configuración del segundo canal, se configura el canal 5 para buscar un ancho de banda del canal 4 al canal 6. A continuación, se configura el canal 8 en el tercer procesamiento, se configura el canal 11 en el cuarto procesamiento y se configura el canal 13 en el quinto procesamiento. En el sexto procesamiento, el canal a configurar vuelve a ser el canal 2. Se puede utilizar dicho procedimiento de configuración de canales de búsqueda.

Cabe señalar que la selección de canales puede adoptar un orden de configuración aleatorio en lugar del orden de configuración secuencial mencionado anteriormente, o el procesamiento de búsqueda puede ser ejecutado una pluralidad de veces utilizando un canal idéntico. Asimismo, además de los procedimientos mencionados anteriormente, los canales se pueden agrupar mediante un procedimiento predeterminado, y el procesamiento de búsqueda puede ser ejecutado para los grupos respectivos.

Tal como se describió anteriormente, el procesamiento de configuración del canal de búsqueda en la etapa S1706 está procesando que cambia un canal a configurar según un algoritmo predeterminado.

La descripción volverá al diagrama de flujo mostrado en la figura 17. El aparato transmite una señal de búsqueda (solicitud de sondeo) a la red de comunicación utilizando el canal de búsqueda configurado en la etapa S1706 (S1707). Después de la transmisión de la señal de búsqueda, el aparato espera la recepción de una respuesta de búsqueda hasta el siguiente tiempo de transmisión de la baliza (S1708). Si no se ha recibido una respuesta de búsqueda cuando se alcanza el tiempo de transmisión de la siguiente baliza, el proceso vuelve a la etapa S1704 para determinar el período de tiempo restante del temporizador T1. Si el temporizador aún no ha alcanzado un límite de tiempo, el aparato repite el procesamiento desde la transmisión de la baliza utilizando de nuevo el canal propio.

Si se recibe una respuesta de búsqueda en la etapa S1708, el aparato confirma el contenido de la señal de respuesta de búsqueda recibida para determinar si la función de un aparato asociado es "aparato proveedor de los parámetros de la comunicación" (S1709). Si la función del aparato asociado es "aparato proveedor de los parámetros de la comunicación", el aparato guarda el resultado de la búsqueda (S1710), y finaliza el procesamiento de descubrimiento del aparato proveedor. Si la función del aparato asociado no es "aparato proveedor" como resultado del procesamiento de determinación en la etapa S1709, el proceso vuelve a la etapa S1704 para determinar el período de tiempo restante del temporizador T1. Si el temporizador aún no ha alcanzado un límite de tiempo, el aparato repite el procesamiento desde la transmisión de baliza utilizando de nuevo el canal propio. Cabe señalar que si el temporizador T1 ha alcanzado un límite de tiempo en la etapa S1704, se determina que no se ha detectado ningún aparato proveedor, finalizando de este modo el procesamiento de descubrimiento del aparato proveedor.

Al ejecutar el procesamiento de descubrimiento del aparato proveedor mencionado anteriormente, la transmisión de baliza utilizando el canal propio y el procesamiento de búsqueda utilizando otro canal pueden ser ejecutados alternativamente.

Un ejemplo de ejecución del procesamiento de descubrimiento del aparato proveedor mientras se cambia un canal utilizado para transmitir una baliza y el utilizado para transmitir una señal de búsqueda y para esperar la recepción de una señal de respuesta de búsqueda, y el efecto de ese procesamiento, se describirá a continuación haciendo referencia a las figuras 19 y 20.

La figura 19 es un gráfico que muestra un ejemplo en el que no se ejecuta el procesamiento que se muestra en la figura 17, y se explora un aparato proveedor mientras cambia un canal a su vez después de la transmisión de balizas utilizando el canal propio. El aparato A transmite balizas utilizando el canal propio durante solo un período (a). Después de eso, el aparato A transmite una señal de búsqueda y espera la recepción de una respuesta de búsqueda mientras cambia todos los canales hasta que se descubre un aparato proveedor durante un período (b).

Por otro lado, el aparato B también transmite balizas utilizando el canal propio durante solo un período (d) como en el aparato A. Después de eso, el aparato B transmite una señal de búsqueda y espera la recepción de una respuesta de búsqueda mientras cambia todos los canales hasta que se descubre un aparato proveedor durante un período (e).

Supóngase que el aparato A transmite una señal de búsqueda y espera la recepción de una señal de respuesta de búsqueda utilizando un canal en el que el aparato B forma una red, durante un período (b'). En este caso, puesto que el aparato B no transmite ninguna baliza utilizando el canal propio durante el período (b'), no puede recibir la señal de búsqueda del aparato A, y no puede devolver ninguna señal de respuesta de búsqueda.

Asimismo, supóngase que el aparato B transmite una señal de búsqueda y espera la recepción de una señal de respuesta de búsqueda utilizando un canal en el que el aparato A forma una red, durante un período (e'). También en este caso, puesto que el aparato A no transmite ninguna baliza utilizando el canal propio durante el período (e'), no puede recibir la señal de búsqueda del aparato B y no puede devolver ninguna señal de respuesta de búsqueda.

De esta manera, cuando ambos aparatos ejecutan el procesamiento de descubrimiento del aparato proveedor, el período de notificación de baliza del canal propio es corto, y el intervalo hasta que se notifica una baliza utilizando el canal propio es largo. Por lo tanto, el aparato A no puede detectar el aparato B, y el aparato B no puede detectar el aparato A.

Por lo tanto, mediante la ejecución del procesamiento de descubrimiento del aparato proveedor descrito en esta realización, se puede reducir la posibilidad de que ocurra dicha situación. La figura 20 es un gráfico que muestra un ejemplo en el que los aparatos A y B ejecutan el procesamiento de descubrimiento del aparato proveedor que se muestra en la figura 17. El aparato A transmite balizas utilizando el canal propio durante un período (a). Después de eso, el aparato A ejecuta el procesamiento de búsqueda utilizando el primer canal durante un período (b). A continuación, el aparato A transmite balizas de nuevo utilizando el canal propio (c) y ejecuta el procesamiento de búsqueda utilizando el segundo canal (d). De esta manera, el aparato A ejecuta alternativamente la transmisión de la baliza utilizando el canal propio, y el procesamiento de la transmisión de la señal de búsqueda y la espera de recepción de la señal de respuesta de búsqueda utilizando otro canal.

El aparato B también ejecuta el mismo procesamiento que en el aparato A. Con este procesamiento, por ejemplo, el período (d) en el que el aparato A ejecuta el procesamiento de búsqueda utilizando un canal en el que el aparato B forma la red se superpone a un período (o) en el que el aparato B notifica balizas. Como resultado, cuando el aparato B devuelve una señal de respuesta de búsqueda en respuesta a una señal de búsqueda transmitida desde el aparato A, el aparato A puede detectar el aparato B.

Asimismo, un período (r) en el que el aparato B ejecuta el procesamiento de búsqueda utilizando un canal en el que el aparato A forma la red se superpone a un período (g) en el que el aparato A notifica las balizas. Como consecuencia, cuando el aparato A devuelve una señal de respuesta de búsqueda en respuesta a una señal de búsqueda transmitida desde el aparato B, el aparato B puede detectar el aparato A.

Tal como se describió anteriormente, mediante la ejecución del procesamiento de descubrimiento del aparato proveedor descrito en esta realización, se puede aumentar la probabilidad de que se detecte un aparato de comunicación asociado.

Cabe señalar que la figura 17 ha explicado el procedimiento en el que se busca un aparato proveedor que ha iniciado el procesamiento de configuración de los parámetros de la comunicación esperando la recepción de una respuesta de sondeo a una solicitud de sondeo (exploración activa). Puesto que un aparato proveedor que está ejecutando el procesamiento de configuración de los parámetros de la comunicación transmite una baliza a la que se añade información adicional, lo que significa un procesamiento de configuración automática de los parámetros de la comunicación, un aparato receptor puede utilizar un procedimiento de espera para la recepción de esa baliza transmitida durante un período de tiempo predeterminado (escaneo pasivo).

La etapa S1709 ha explicado el procedimiento en el que se determina si la función de un socio incluida en el elemento de información de la señal de respuesta de búsqueda recibida es “aparato proveedor”. Cuando la función de un socio incluida en el elemento de información de la señal de respuesta de búsqueda recibida es “candidato a aparato proveedor”, se puede determinar si la función se determina o no como “aparato proveedor” utilizando la información incluida en la señal de respuesta de búsqueda. Más específicamente, por ejemplo, un aparato que transmite una señal de respuesta de búsqueda transmite la señal de respuesta de búsqueda que almacena un período de tiempo transcurrido después de pulsar el botón de configuración 106. El aparato que recibió la señal de respuesta de búsqueda compara el período de tiempo transcurrido almacenado en la señal de respuesta de búsqueda con un período de tiempo transcurrido después de pulsar su propio botón de configuración 106. Como resultado de la comparación, si el botón de configuración 106 del aparato que recibió la señal de respuesta de búsqueda fue pulsado antes que el aparato que transmitió la señal de respuesta de búsqueda, el aparato que recibió la señal de respuesta de búsqueda configura “aparato proveedor” como la función, y el proceso avanza a la etapa S816.

Por otro lado, como resultado de la comparación, si el botón de configuración 106 del aparato que transmitió la señal de respuesta de búsqueda fue pulsado antes que el aparato que recibió la señal de respuesta de búsqueda, el aparato que recibió la señal de respuesta de búsqueda transmite una señal de notificación al aparato que transmitió la señal de respuesta de búsqueda, y el aparato que recibió la señal de notificación puede configurar “aparato proveedor” como función.

Tal como se describió anteriormente, cuando la señal de respuesta de búsqueda incluye un tiempo en el que se realizó una operación de usuario para emitir una instrucción de inicio del procesamiento de configuración de los parámetros de la comunicación, y el aparato asociado de comunicación descubierto no está configurado como un aparato proveedor, qué aparato es un aparato proveedor se puede determinar haciendo referencia a ese tiempo. Cuando el tiempo incluido en la señal de respuesta de búsqueda es anterior al tiempo en el que se emitió la instrucción de inicio del procesamiento de configuración de los parámetros de la comunicación al aparato que recibió la señal de respuesta de búsqueda, el aparato asociado de comunicación se determina como un aparato proveedor. Con este procesamiento, un aparato proveedor puede ser determinado con prontitud. Cabe señalar que la información a comparar no se limita al período de tiempo transcurrido después de pulsar el botón 106. Por ejemplo, se puede comparar la dirección de MAC del aparato, o se puede comparar un valor de la función de sincronización de tiempos (TSF, Timing Synchronization Function) incluido en la señal de respuesta de búsqueda.

A continuación se describirá un caso en el que se añade un nuevo aparato a una red ad hoc ya existente utilizando el procesamiento de configuración automática de los parámetros de la comunicación. Cabe señalar que la red ad hoc ya existente indica una red ad hoc que está configurada por una pluralidad de aparatos que utilizan parámetros de la comunicación compartidos entre los aparatos que ejecutaron el procesamiento de configuración de los parámetros de la comunicación.

La figura 5 es un diagrama que muestra un primer aparato de comunicación A 500 (denominado aparato A en lo sucesivo), un segundo aparato de comunicación B 501 (denominado aparato B en lo sucesivo), un tercer aparato de comunicación C 503 (denominado aparato C en lo sucesivo), y la red 502. Los aparatos A, B y C tienen las disposiciones mencionadas anteriormente mostradas en las figuras 1 y 2.

A continuación se examinará un caso en el que cuando el aparato C está a punto de participar en la red 502 configurada por los aparatos A y B, se accionan los botones de configuración de los aparatos B y C.

La figura 6 es un diagrama de flujo para explicar la operación de procesamiento de notificaciones de un aparato proveedor. Cuando un aparato ya es un participante de la red en la etapa S802 en la figura 8, ese aparato inicia el procesamiento que se muestra en la figura 6.

Cuando se inicia el procesamiento, la unidad de control de baliza 213 del aparato proveedor aumenta la frecuencia de transmisión de la baliza (relación de transmisión, el número de veces de transmisión) por unidad de tiempo mediante el aparato proveedor (S601).

Cabe señalar que la red ad hoc de la LAN inalámbrica según el estándar IEEE 802.11 especifica que un aparato que devuelve una respuesta de sondeo es un aparato que transmitió una baliza inmediatamente antes de la recepción de una solicitud de sondeo.

A continuación, en la etapa S601, el aparato proveedor configura la CW para que sea un valor menor que el valor inicial. Con esta configuración, el número de veces que las balizas son transmitidas por unidad de tiempo por el aparato proveedor resulta ser mayor que otros aparatos que son participantes de la red. Como resultado, en el procesamiento de búsqueda del aparato proveedor (etapa S805 en la figura 8) por un nuevo aparato participante, se puede detectar una respuesta de sondeo del aparato proveedor dentro de un corto período de tiempo.

De esta manera, puesto que la frecuencia de transmisión de la baliza del aparato proveedor aumenta, cuando un nuevo aparato como posible participante busca un aparato proveedor, puede recibir una respuesta de sondeo del aparato proveedor con mayor probabilidad. Cuando el nuevo aparato como posible participante busca un aparato proveedor mediante un escaneo pasivo, puede recibir una baliza del aparato proveedor con mayor probabilidad.

Como resultado, se puede reducir la probabilidad de que transcurra el tiempo límite del procesamiento de configuración de los parámetros de la comunicación mientras un nuevo aparato como posible participante no puede detectar el aparato proveedor. Cuando el nuevo aparato como posible participante puede detectar un aparato proveedor en un corto período de tiempo, se puede acortar el período de tiempo requerido hasta la finalización del procesamiento que proporciona el parámetro de comunicación.

Después de eso, el aparato proveedor transmite un mensaje de notificación de inicio que notifica el inicio del procesamiento de configuración automática de los parámetros de la comunicación (S602). Cabe señalar que el aparato proveedor puede unidifundir este mensaje de notificación de inicio a cada aparato como participante de la red. Este mensaje de notificación de inicio también se puede expresar como un mensaje que notifica que el aparato B inició una operación como aparato proveedor.

El aparato proveedor espera hasta que el procesamiento de suministro activado termina como un error (S606), el procesamiento de suministro de los parámetros de la comunicación al aparato receptor se completa (S603) o recibe una notificación de error o un mensaje de notificación de finalización de otro aparato (S605, S608).

Si el procesamiento de suministro ha tenido éxito, es decir, si el procesamiento de suministro de los parámetros de la comunicación al aparato receptor se ha completado (S603), el aparato proveedor transmite un mensaje de notificación de finalización (S604). Cabe señalar que el aparato proveedor puede unidifundir este mensaje de notificación de finalización a cada aparato como participante de la red.

Si el aparato proveedor transmite el mensaje de notificación de finalización en la etapa S604 o recibe un mensaje de notificación de finalización de otro aparato (S605), el proceso salta a la etapa S609.

Si el procesamiento de suministro ha fallado (S606), el aparato proveedor transmite un mensaje de notificación de error (S607). Cabe señalar que el aparato proveedor puede transmitir el mensaje de notificación de error a cada aparato como participante de la red.

Si el aparato proveedor transmite el mensaje de notificación de error en la etapa S607 o recibe un mensaje de notificación de error de otro aparato (S608), el proceso avanza a la etapa S609.

En la etapa S609, la unidad de control de baliza 213 del aparato proveedor reconfigura la CW al valor inicial para restaurar la frecuencia de transmisión de baliza aumentada en la etapa S601 (S609). Cabe señalar que el tiempo de reconfiguración de la CW al valor inicial no está especialmente limitado siempre que la CW se reconfigure después del inicio del procesamiento de suministro. Es decir, la CW puede ser reconfigurada inmediatamente después del inicio del procesamiento, después de completar el procesamiento de suministro o después de un error. Si la CW se reconfigura inmediatamente después del inicio del procesamiento, puesto que la frecuencia de transmisión de la baliza (el número de veces de transmisión) disminuye, el consumo de energía requerido para la transmisión de la baliza se puede reducir de manera eficiente. El mensaje de notificación de inicio transmitido en la etapa S602 se transmite de manera repetitiva hasta que el

procesamiento de suministro termina como un error, se proporcionan los parámetros de la comunicación al aparato receptor o se recibe un mensaje de notificación de otro aparato.

La figura 7 es un diagrama de flujo para explicar la operación de procesamiento de la respuesta de proxy de un aparato (aparato A) como participante de la red distinto del aparato proveedor. Cuando el aparato A recibe el mensaje de notificación de inicio, el procesamiento mostrado en la figura 7 se inicia.

Tras la detección de la recepción del mensaje de notificación de inicio, la unidad 208 de control de configuración automática del aparato A inicia un temporizador utilizado para determinar si ha transcurrido un tiempo límite de los procesos que se describirán en las etapas S702 a S707 (S701).

A continuación, la unidad 208 de control de configuración automática cambia el contenido de la información a incluir en una baliza y la señal de respuesta de búsqueda (respuesta de sonda) a transmitir (S702). En la etapa S702, la unidad 208 de control de configuración automática añade información de identificación utilizada para identificar de manera única un aparato proveedor (aparato B) a la baliza y la señal de respuesta de búsqueda a transmitir. Como información de identificación, por ejemplo, se almacena información de dirección de MAC del aparato proveedor. De esta manera, incluso cuando el aparato A que no es un aparato proveedor devuelve una señal de respuesta de búsqueda, un aparato como origen de la transmisión de una señal de búsqueda puede detectar la presencia de un aparato proveedor.

La unidad de control de baliza 213 configura la CW para que sea un valor mayor que el valor inicial (S703), para disminuir la frecuencia de transmisión de la baliza (relación de transmisión).

Por lo tanto, el número de veces que el aparato transmite balizas por unidad de tiempo como participante de la red distinto del aparato proveedor es menor que el aparato proveedor. Como resultado, en el procesamiento de búsqueda del aparato proveedor (etapa S805 en la figura 8) por parte de un nuevo aparato como posible participante, se puede detectar una respuesta de sondeo del aparato proveedor en un corto período de tiempo.

Después de eso, el aparato A espera un mensaje de notificación de finalización o un mensaje de notificación de error transmitido desde el aparato proveedor (S704, S705). Tras la recepción del mensaje de notificación, la unidad de control de baliza 213 del aparato A reconfigura (restaura) la CW al valor inicial para restaurar la frecuencia de transmisión de baliza disminuida en la etapa S703 (S706). Además, la unidad 208 de control de configuración automática restaura el contenido de la información que se incluirá en una baliza y la señal de respuesta de búsqueda que se transmitirá a aquellos antes del cambio en la etapa S702 (S707). Es decir, la unidad 208 de control de configuración automática elimina la información de identificación que se utiliza para identificar de manera única el aparato proveedor (aparato B) y se añade a la baliza y a la señal de respuesta de búsqueda a transmitir.

Cabe señalar que si el temporizador configurado en la etapa S701 ha alcanzado un límite de tiempo, el aparato receptor aborta los procesos en las etapas S702 a S707. Si los procesos en las etapas S702 y S703 ya se han realizado en el momento de expiración del tiempo límite del temporizador, el proceso de reconfiguración se ejecuta como en las etapas S706 y S707.

La figura 9 es un diagrama de secuencia para explicar las operaciones de los respectivos aparatos en esta realización. El aparato A recibe los parámetros de la comunicación proporcionados por el aparato B mediante el procesamiento de configuración automática de los parámetros de la comunicación, y ya es un participante de la red 502 definida por esos parámetros de la comunicación (F901). El aparato C aún no ha pasado por el procesamiento de suministro de los parámetros de la comunicación.

Cuando el usuario acciona el botón de configuración del aparato B, el aparato B inicia el procesamiento mostrado en la figura 8 (F902). Puesto que el aparato B ya es un participante de la red 502 que utiliza los parámetros de la comunicación compartidos con el aparato A mediante el procesamiento de configuración automática de los parámetros de la comunicación, configura “aparato proveedor” como la función e inicia el procesamiento de suministro de los parámetros de la comunicación (F902).

El aparato B inicia el procesamiento de notificación de inicio que se muestra en la figura 6 (F903). Después de que se inicia el procesamiento de notificación de inicio, el aparato B transmite un mensaje de notificación de inicio y aumenta la frecuencia de transmisión de la baliza (F904).

El aparato A que recibió el mensaje de notificación de inicio inicia el procesamiento de respuesta de proxy que se muestra en la figura 7 y disminuye la frecuencia de transmisión de la baliza (F905).

De esta manera, cuando el aparato B aumenta la frecuencia de transmisión de la baliza y el aparato A disminuye la frecuencia de transmisión de la baliza, el aparato C como nuevo posible participante puede detectar el aparato B como el aparato proveedor en un período de tiempo más corto.

Cuando el usuario acciona el botón de configuración 106 del aparato C, el aparato C inicia el procesamiento mostrado en la figura 8. Puesto que el aparato C no es un participante de la red, ejecuta el procesamiento para crear una red, configurando "candidato a aparato proveedor" como su función, y así sucesivamente, y a continuación comienza el procesamiento de búsqueda de aparato proveedor. Cabe señalar que la figura 9 muestra el procesamiento de búsqueda y los procesos subsiguientes, y no muestra los procesos anteriores a ellos. El aparato C transmite señales de búsqueda para detectar un aparato proveedor (F906).

En la red 502, el aparato A o B devuelve una señal de respuesta de búsqueda en respuesta a la señal de búsqueda transmitida desde el aparato C (F907a, F907b).

Cuando el aparato A devuelve la señal de respuesta de búsqueda, devuelve la señal de respuesta de búsqueda que almacena la información de identificación (dirección de MAC) del aparato B como un aparato proveedor (F907b). Cuando el aparato B devuelve la señal de respuesta de búsqueda, devuelve la señal de respuesta de búsqueda que almacena información que indica que es un aparato proveedor (F907a). De esta manera, incluso cuando el aparato C recibe las señales de respuesta de búsqueda de cualquier aparato en la red 502, seguramente puede detectar el aparato B como el aparato proveedor.

Tras la detección de la presencia del aparato proveedor, el aparato C configura el "aparato receptor" como su función (F908). A continuación, el aparato C participa en la red 502 y recibe los parámetros de la comunicación necesarios para realizar las comunicaciones en la red 502 desde el aparato B como aparato proveedor (F909).

Después de que el aparato B proporciona los parámetros de la comunicación al aparato C, transmite un mensaje de notificación de finalización al aparato A (F910). Después de la transmisión del mensaje de notificación de finalización, el aparato B restaura la frecuencia de transmisión de la baliza aumentada en F903. Tras la recepción del mensaje de notificación de finalización, el aparato A restaura la frecuencia de transmisión de la baliza disminuida en F905.

Tal como se describió anteriormente, el usuario puede controlar automáticamente el aparato C para que participe en la red 502 accionando solo el botón de configuración 106.

Cabe señalar que la figura 9 ha explicado el caso en el que se acciona el botón de configuración 106 del aparato B. También, se puede suponer un caso en el que se acciona el botón de configuración 106 del aparato A. Incluso cuando se acciona el botón de configuración 106 del aparato A, puesto que el aparato A se convierte en el aparato proveedor a través de la etapa S802 en la figura 8, puede agregar el aparato C a la red 502 de la misma manera que en la figura 9.

Con el procesamiento mencionado anteriormente, los aparatos de comunicación pueden compartir fácilmente los parámetros de la comunicación. Tal como se describió anteriormente, al accionar los botones de configuración 106 en los aparatos A y B, se ejecuta el procesamiento de la conexión de comunicación entre los aparatos A y B para configurar la red 502.

El procesamiento de la conexión de comunicación puede ser iniciado automáticamente después de completar el procesamiento de configuración de los parámetros de la comunicación, tal como se ha descrito anteriormente, o puede ser iniciado en respuesta a una nueva operación de pulsación del botón de configuración 106 o una introducción de comando de conexión por parte de la unidad de entrada 109.

Cabe señalar que el procesamiento de la conexión de comunicación difiere según el procedimiento de autenticación y el procedimiento de cifrado de los parámetros de la comunicación compartidos.

En esta realización, las combinaciones adoptadas como procedimiento de autenticación y procedimiento de cifrado son las que se muestran, por ejemplo, en la figura 10.

La autenticación abierta es un procedimiento de autenticación definido como "Autenticación de sistema abierto" en el estándar IEEE 802.11 y véase el estándar IEEE 802.11 para obtener más información. La autenticación compartida es un procedimiento de autenticación definido como "Autenticación de clave compartida" en los estándares IEEE 802.11 e IEEE 802.11i, y utiliza un protocolo WEP como procedimiento de cifrado.

Cabe señalar que "WEP" es una abreviatura de "Wired Equivalent Privacy, Privacidad equivalente por cable", y véase el estándar IEEE 802.11 o IEEE 802.11i para obtener más información. Además, un procedimiento de autenticación de WPA, un procedimiento de autenticación de WPA-PSK, un procedimiento de autenticación de WPA2 y un procedimiento de autenticación de WPA2-PSK son los estándares de procedimientos de autenticación especificados por Wi-Fi Alliance. Estos procedimientos se basan en una

RSNA (Robust Security Network Association, Asociación de red de seguridad robusta) en el estándar IEEE 802.11i.

"TKIP" es una abreviatura de "Temporal Key Integrity Protocol, Protocolo de integridad de clave temporal". Además, "CCMP" es una abreviatura de "CTR con protocolo de CBC-MAC" y utiliza un protocolo AES como procedimiento de cifrado. "AES" es una abreviatura de "Advanced Encryption Standard, Estándar de cifrado avanzado".

Véase la especificación de Wi-Fi Alliance o la especificación de prueba para obtener información sobre estos procedimientos. Los procedimientos de autenticación de WPA-PSK y WPA2-PSK son aquellos que utilizan una clave previamente compartida. Los procedimientos de autenticación de WPA y WPA2 requieren la autenticación del usuario por parte de un servidor de autenticación, que se prepara por separado, y obtiene una clave de cifrado de un canal de comunicación del servidor de autenticación. Véase el estándar IEEE 802.11i para obtener información sobre estos procedimientos.

El procedimiento de procesamiento de la conexión difiere según los procedimientos de autenticación. Los procedimientos de autenticación que se admiten actualmente incluyen seis procedimientos diferentes, es decir, la autenticación abierta, la autenticación compartida, la autenticación de WPA, la autenticación de WPA-PSK, la autenticación de WPA2 y la autenticación de WPA2-PSK, tal como se muestra en la tabla. De estos procedimientos, la autenticación de WPA y la autenticación de WPA2, y la autenticación de WPA-PSK y la autenticación de WPA2-PSK son esencialmente los mismos procedimientos de autenticación. Por esta razón, los procedimientos de autenticación de WPA y WPA2 y los procedimientos de autenticación de WPA2 y WPA2-PSK se consideran como los mismos procedimientos, y a continuación se explicarán cuatro procedimientos de autenticación diferentes (abierto, compartido, WPA y WPA-PSK).

Sin embargo, puesto que la autenticación de WPA requiere un servidor de autenticación independiente que se configura externamente y ejecuta el procesamiento de autenticación con ese servidor de autenticación, se requiere un procesamiento complicado cuando todos los aparatos de comunicación funcionan al mismo nivel, tal como en la presente invención. Por lo tanto, no se proporcionará una descripción de la autenticación de WPA.

En esta realización, la autenticación abierta, la autenticación compartida y la autenticación de WPA-PSK se explicarán respectivamente a continuación.

En primer lugar, se describirá la autenticación abierta. En la autenticación abierta, los aparatos de comunicación configuran parámetros de la comunicación compartidos por el procesamiento de configuración automática de los parámetros de la comunicación, y buscan el aparato de los demás para configurar una red IBSS.

A continuación, se describirá la autenticación compartida. No se proporcionará una descripción detallada de la autenticación compartida, puesto que está incluida en las especificaciones IEEE 802.11 e IEEE 802.11i. Tras la realización de la autenticación compartida, se debe determinar un solicitante y un respondedor.

En el modo de infraestructura, una STA (estación) funciona como solicitante y un AP (punto de acceso) funciona como respondedor. Por otro lado, en el modo ad hoc, no existe AP. Por esta razón, para implementar la autenticación de clave compartida en la red IBSS, la STA debe incluir una función de respondedor y un algoritmo de determinación de la función de solicitante/respondedor.

Este algoritmo de determinación de la función de solicitante/respondedor puede adoptar el mismo procedimiento que el algoritmo de determinación de la función de solicitante/autenticador en la autenticación de WPA-PSK que se describirá más adelante. Por ejemplo, en el procesamiento de configuración automática de los parámetros de la comunicación, un aparato proveedor de los parámetros de la comunicación puede funcionar como respondedor, y un aparato receptor de los parámetros de la comunicación puede funcionar como solicitante.

Finalmente, se explicará la autenticación de WPA-PSK. La autenticación de WPA-PSK está estandarizada en el documento IEEE 802.11i y WPA, y también se especifica un procedimiento de operación en la red IBSS. La figura 12 describe una secuencia especificada en el estándar IEEE 802.11i. Véase el estándar IEEE 802.11i para obtener más información y, a continuación, se explicará una descripción general.

Supóngase que existen los aparatos A y B que completan el procesamiento de configuración automática de los parámetros de la comunicación. Después de completar el procesamiento de configuración automática de los parámetros de la comunicación, el procesamiento de conexión de comunicación se ejecuta utilizando los parámetros de la comunicación configurados automáticamente o en respuesta a una operación del usuario.

Los aparatos A y B buscan el asociado de cada uno (F1201). Si estos aparatos pueden reconocerse entre sí, uno de los aparatos A y B, que tiene una dirección de MAC más alta, sirve como autenticador, y el otro aparato sirve como solicitante. A continuación, los aparatos A y B ejecutan el primer procesamiento de intercambio de 4 vías y el procesamiento de intercambio de clave de grupo (F1202 y F1203).

Cabe señalar que el procesamiento de intercambio de 4 vías es un mecanismo que intercambia números aleatorios entre el autenticador y el solicitante, y genera una clave de cifrado de un paquete de unidifusión denominada clave por parejas basada en una clave compartida previamente para cada sesión. El procesamiento de intercambio de clave de grupo es un mecanismo que envía una clave de cifrado de un paquete de multidifusión o de un paquete de difusión que posee el autenticador.

Después de eso, los aparatos A y B intercambian las funciones del autenticador y el solicitante, y ejecutan el procesamiento de intercambio de 4 vías y el procesamiento de intercambio de clave de grupo nuevamente (F1204 y F1205). Con los procesos anteriores, los aparatos A y B pueden realizar comunicaciones cifradas.

De esta manera, en caso de que el procedimiento cumpla totalmente con la especificación IEEE 802.11i, puesto que el procesamiento de intercambio de 4 vías y el procesamiento de intercambio de clave de grupo se repiten una pluralidad de veces, el procesamiento general se vuelve redundante. Puesto que se ejecutan el procesamiento redundante y el algoritmo de determinación de funciones, se requiere mucho tiempo hasta que se completa la conexión. Por lo tanto, también se puede utilizar un procedimiento para reducir el procesamiento redundante y acortar el tiempo de procesamiento.

Existen algunos de dichos procedimientos y, en este caso, se explicarán los siguientes cuatro procedimientos:

primer procedimiento: los procesos de intercambio de 4 vías se combinan en una sola vez;
segundo procedimiento: las claves de grupo se combinan en una por cada red;
tercer procedimiento: todas las claves de grupo y las claves por parejas se combinan en una sola; y
cuarto procedimiento: el intercambio de claves se ejecuta junto con el procesamiento de configuración automática de los parámetros de la comunicación.

La figura 11 muestra las diferencias de los números de veces de secuencias de intercambio de claves y los números de claves por parejas y claves de grupo poseídas por los cuatro procedimientos mencionados anteriormente.

En primer lugar, se explicará el número de claves poseídas. Cuando una red IBSS ad hoc que incluye n aparatos de comunicación es totalmente compatible con el estándar IEEE 802.11i, se requieren n-1 claves por parejas, tantas como el número de otros aparatos de comunicación. En cuanto a las claves de grupo, además de tantas claves de grupo como el número de otros aparatos de comunicación, se requiere un total de dos claves de grupo, es decir, una clave de grupo actual y una clave de grupo inmediatamente anterior para el aparato. Por lo tanto, se requieren n+1 claves de grupo en total. La razón por la que se requieren dos claves de grupo para el aparato es que existe un aparato que tiene diferentes claves de grupo en una red idéntica en un período de transición que depende del estado de progreso del intercambio de clave de grupo.

En el primer procedimiento, solo se reduce el número de secuencias, y el número de claves poseídas permanece invariable.

En el segundo procedimiento, se requieren de manera similar n-1 claves por parejas, y solo se requiere una clave de grupo en total.

En el tercer procedimiento, puesto que una clave de grupo se utiliza intacta como clave por parejas, el número de claves por parejas resulta ser cero, y solo se posee una clave de grupo.

En el cuarto procedimiento, se requieren de manera similar n-1 claves por parejas. Puesto que los aparatos respectivos pueden poseer claves de grupo, o una clave de grupo en total, se pueden requerir n+1 claves de grupo o solo una clave de grupo según el caso.

A continuación se describirá el número de secuencias de intercambio de claves ejecutadas por otros aparatos. En caso de que el procedimiento cumpla totalmente con el estándar IEEE 802.11i, el procesamiento de intercambio de 4 vías se ejecuta dos veces y el procesamiento de intercambio de clave de grupo se ejecuta dos veces, tal como se ha descrito utilizando la figura 12.

En el primer procedimiento, el número de veces que se ejecuta el procesamiento de intercambio de 4 vías como procesamiento redundante se reduce a uno. El procesamiento de intercambio de clave de grupo aún se ejecuta dos veces.

En el segundo procedimiento, puesto que en la red solo se utiliza una clave de grupo combinada, esa clave solo necesita ser distribuida a un nuevo terminal. Por lo tanto, el procesamiento de intercambio de clave de grupo se ejecuta una vez. Asimismo, el procesamiento de intercambio de 4 vías puede ser ejecutado una vez, según el primer procedimiento, o dos veces de dos maneras, según el estándar IEEE 802.11i.

En el tercer procedimiento, puesto que una clave que se configura de antemano se utiliza como clave por parejas y clave de grupo, no se ejecuta ninguna secuencia de intercambio de claves.

En el cuarto procedimiento, puesto que el procesamiento equivalente al procesamiento de intercambio de claves se realiza en el procesamiento de configuración automática de los parámetros de la comunicación de WPS, no se ejecuta ningún procesamiento de intercambio de 4 vías independiente. El procesamiento de intercambio de clave de grupo se ejecuta un número arbitrario de veces.

Tal como se ha descrito haciendo referencia a la figura 11, estos procedimientos son ventajosos en términos del número de secuencias de intercambio de claves y el número de claves poseídas en comparación con el procedimiento mencionado anteriormente que cumple con el estándar IEEE 802.11i.

Los cuatro procedimientos mencionados anteriormente se describirán en detalle a continuación utilizando los diagramas de secuencia.

El primer procedimiento se describirá a continuación haciendo referencia a la figura 13.

Supóngase que existen los aparatos A y B que completan el procesamiento de configuración automática de los parámetros de la comunicación. Después de completar el procesamiento de configuración automática de los parámetros de la comunicación, el procesamiento de conexión de comunicación se ejecuta utilizando los parámetros de la comunicación configurados automáticamente o en respuesta a una operación del usuario.

Los aparatos A y B buscan el asociado de cada uno (F1301). Si estos aparatos se pueden reconocer entre sí, uno de los aparatos A y B, que tiene una dirección de MAC más alta, sirve como autenticador, y el otro aparato sirve como solicitante. A continuación, los aparatos A y B ejecutan un procesamiento de intercambio de 4 vías y un procesamiento de intercambio de clave de grupo (F1302 y F1303).

Después de eso, los aparatos A y B intercambian las funciones de autenticador y solicitante, y ejecutan nuevamente el procesamiento de intercambio de clave de grupo (F1304). Con el procesamiento anterior, se permiten las comunicaciones.

Tal como se describió anteriormente, con el primer procedimiento, el número de veces que se ejecuta el procesamiento de intercambio de 4 vías, que es dos veces por par de aparatos en la especificación IEEE 802.11i, se reduce a uno.

Puesto que el procesamiento de intercambio de 4 vías es necesario para compartir una clave por parejas entre los aparatos de comunicación que ejecutan el procesamiento de intercambio de 4 vías, si ese procesamiento se ejecuta continuamente dos veces, la seguridad no se puede mejorar, lo que da como resultado un procesamiento redundante. Por lo tanto, en el primer procedimiento, se cambia el procedimiento convencional, y el número de veces que se ejecuta el procesamiento de intercambio de 4 vías se reduce a una, acortando de este modo el tiempo requerido para el procesamiento de conexión normal.

El segundo procedimiento se describirá a continuación haciendo referencia a la figura 14. Supóngase que existen los aparatos A y B que completan el procesamiento de configuración automática de los parámetros de la comunicación. Después de completar el procesamiento de configuración automática de los parámetros de la comunicación, el procesamiento de conexión de comunicación se ejecuta utilizando los parámetros de la comunicación configurados automáticamente o en respuesta a una operación del usuario.

Los aparatos A y B buscan el asociado de cada uno (F1401). Si estos aparatos pueden reconocerse entre sí, uno de los aparatos A y B, que tiene una dirección de MAC más alta, funciona como autenticador, y el otro aparato funciona como solicitante. A continuación, los aparatos A y B ejecutan un procesamiento de intercambio de 4 vías y un procesamiento de intercambio de clave de grupo (F1402 y F1403). Con el procesamiento anterior, se permiten las comunicaciones.

En la especificación IEEE 802.11i, se configuran diferentes claves de grupo para los respectivos aparatos de comunicación. Sin embargo, en el segundo procedimiento, solo se utiliza una clave de grupo combinada por cada red.

Las claves por parejas se preparan para los respectivos canales de comunicación, pero normalmente se utiliza una clave de grupo por cada red. Como resultado, el procesamiento de intercambio de clave de grupo, que debe ser ejecutado dos veces en el procedimiento compatible con el estándar IEEE 802.11i, solo se debe

ejecutar una vez. Puesto que solo se configura una clave de grupo, el procesamiento de cifrado/descifrado de un paquete de difusión y un paquete de multidifusión resulta ser simple, porque no es necesario guardar una clave diferente para cada aparato que transmitió dichos paquetes.

El tercer procedimiento es el mismo que WPA-Ninguno (Sistema de clave compartida previamente global opcional de IBSS) descrito en la referencia 2 no de patente.

Puesto que los detalles del WPA-Ninguno se describen en la referencia mencionada anteriormente, no se dará una descripción detallada del mismo. En el WPA normal, se aplica un número aleatorio a un elemento como origen de una clave por parejas mediante un procesamiento de intercambio de 4 vías para generar una clave de sesión. Por otro lado, en WPA-Ninguno, un elemento como origen de una clave por parejas se aplica intacto como clave de sesión.

Es decir, una gran funcionalidad característica del tercer procedimiento radica en que no se ejecuta ningún procesamiento de intercambio de claves. Por lo tanto, la seguridad resulta ser menor que el procesamiento de conexión de WPA normal, que genera una clave de sesión para cada conexión. Por lo tanto, cuando se adopta este procedimiento, el procesamiento de configuración automática de los parámetros de la comunicación se inicia para cada conexión, y las claves de comunicación de los parámetros de la comunicación compartidos se generan aleatoriamente para cada conexión, mejorando de este modo la seguridad.

El cuarto procedimiento se describirá a continuación haciendo referencia a la figura 15. Tal como se describió anteriormente utilizando la figura 4, se ejecutan el procesamiento de búsqueda de socios de comunicación y el procesamiento de determinación de funciones en el procesamiento de configuración automática de parámetros de la comunicación (F1501). Posteriormente, mediante el procesamiento de configuración automática de los parámetros de la comunicación, los parámetros de la comunicación son transferidos desde un aparato proveedor de parámetros de la comunicación a un aparato receptor de parámetros de la comunicación (F1502). Durante el procesamiento en F1502, el procesamiento de intercambio de claves, que no se ejecuta en el procedimiento convencional, se ejecuta simultáneamente con el procesamiento de configuración de los parámetros de la comunicación.

Tras la ejecución simultánea, por ejemplo, un número aleatorio utilizado en el procesamiento de intercambio de mensajes del procesamiento de configuración de los parámetros de la comunicación se utiliza también como el del procesamiento de intercambio de claves. Por lo tanto, en el momento en que finaliza F1502, los aparatos A y B comparten una clave por parejas. Después de completar el procesamiento de configuración automática de los parámetros de la comunicación, se ejecuta el procesamiento de intercambio de claves de grupo (F1503). Tal como se ha descrito anteriormente, el cuarto procedimiento se caracteriza por que el procesamiento de intercambio de claves se ejecuta junto con el procesamiento de configuración automática de los parámetros de la comunicación.

Con el cuarto procedimiento, puesto que las claves por parejas entre aparatos son diferentes incluso en una red idéntica, la seguridad se puede mejorar. Puesto que en el procesamiento de configuración de los parámetros de la comunicación se ejecuta un procesamiento equivalente al procesamiento de intercambio de 4 vías, el tiempo total de conexión se puede acortar.

En esta descripción, el procesamiento de intercambio de claves de grupo se ejecuta por separado. Sin embargo, cuando el procesamiento de intercambio de claves de grupo también se ejecuta en el procesamiento de configuración de los parámetros de la comunicación, el tiempo total de conexión se puede acortar aún más.

En cuanto a los cinco procedimientos mencionados anteriormente, incluido el que cumple con el estándar IEEE 802.11i, un sistema puede seleccionar uno de estos procedimientos, y se puede proporcionar información que indica un procedimiento a utilizar incluido en los parámetros de la comunicación. Asimismo, estos procedimientos pueden ser cambiados dinámicamente dependiendo del modo de procesamiento de configuración automática de los parámetros de la comunicación.

A continuación se describirá un caso haciendo referencia a la figura 16 en el que los procedimientos son conmutados dinámicamente dependiendo del modo de procesamiento de configuración automática de los parámetros de la comunicación.

Supóngase que WPA-PSK, WPA2-PSK o similar, que requiere procesamiento de intercambio de claves, se selecciona como parámetros de la comunicación mediante el procesamiento de configuración automática de los parámetros de la comunicación. En este caso, se determina un procedimiento de intercambio de claves que ya se utiliza en una red (S1601). Con este procesamiento de determinación, si ya se seleccionó un procedimiento de intercambio de clave arbitrario (Sí en S1601-2), ese procedimiento se utiliza intacto. Si no

se seleccionó especialmente ningún procedimiento (No en S1601-2), se determina un modo de procesamiento de configuración automática de los parámetros de la comunicación (S1602).

El modo de procesamiento incluye, por ejemplo, un modo en el que los parámetros de la comunicación configurados mediante el procesamiento de configuración automática de los parámetros de la comunicación se utilizan de manera permanente, o los parámetros de la comunicación se utilizan como información de sesión temporal. Por ejemplo, en el caso del modo de procesamiento que utiliza permanentemente los parámetros de la comunicación configurados (un modo que utiliza parámetros de la comunicación idénticos cuando una comunicación inalámbrica se realiza de nuevo después de que se apaga la fuente de alimentación), se selecciona un procedimiento que garantice una alta seguridad (por ejemplo, el primer procedimiento o el cuarto procedimiento). En el caso del modo que utiliza los parámetros de la comunicación como información de sesión temporal (un modo que borra o desactiva los parámetros de la comunicación configurados una vez que se apaga la fuente de alimentación), se puede seleccionar un procedimiento que priorice la carga de procesamiento sobre la seguridad (por ejemplo, el segundo procedimiento o el tercer procedimiento).

Si no se configura un procedimiento de intercambio de claves a utilizar basándose en el modo de procesamiento (No en S1602-2), se determina el número de aparatos de comunicación incluidos en una red idéntica (S1603). A continuación, se selecciona un procedimiento de intercambio de claves adecuado basándose en el número de aparatos de comunicación (S1604). Por ejemplo, en el caso de dos aparatos de comunicación, se selecciona el procedimiento totalmente compatible con el estándar IEEE 802.11i o el primero o el cuarto procedimiento. En el caso de tres o más aparatos de comunicación, se puede seleccionar el segundo o el tercer procedimiento.

Tal como se ha descrito anteriormente, según esta realización, cuando se acciona el botón de configuración de un aparato como participante de una red, ese aparato funciona como aparato proveedor y ejecuta el procesamiento de suministro de los parámetros de la comunicación. Por esta razón, cuando el usuario selecciona un aparato arbitrario sin considerar un aparato proveedor o un aparato receptor de los participantes de la red, un nuevo aparato puede recibir los parámetros de la comunicación suministrados.

Es decir, al accionar el botón de configuración de un aparato arbitrario sin seleccionar ningún aparato proveedor, se puede agregar un nuevo aparato a la red. Puesto que la frecuencia de transmisión de baliza aumentada es restaurada después de completar el procesamiento de suministro, se puede reducir el consumo de energía requerido para la transmisión de la baliza. Cabe señalar que, cuando la frecuencia de transmisión de la baliza es restaurada inmediatamente después del inicio del procesamiento de suministro de los parámetros de la comunicación, el consumo de energía requerido para la transmisión de la baliza se puede reducir de manera más eficiente.

Cuando se agrega un nuevo aparato a la red después de que los parámetros de la comunicación son suministrados de manera fácil y segura, aumentan las opciones sobre los algoritmos de intercambio de claves y se determina y configura automáticamente un algoritmo de intercambio de claves, lo que reduce el estrés del usuario al formar una red. Asimismo, se puede formar una red de manera segura, fácil y rápida.

<Segunda realización>

En la primera realización, en el procesamiento de descubrimiento del aparato proveedor descrito utilizando la figura 17, un aparato ejecuta alternativamente el procesamiento de transmisión de balizas en su canal de la LAN inalámbrica y el procesamiento de descubrimiento del aparato proveedor en otro canal de la LAN inalámbrica. Con este procesamiento, el aparato y el otro aparato pueden detectar fácilmente el aparato del otro. Por el contrario, la segunda realización explicará un ejemplo en el que el procesamiento de descubrimiento del aparato proveedor se ejecuta en un canal predeterminado de la LAN inalámbrica.

La figura 18 es un diagrama de flujo que muestra un ejemplo de la secuencia de funcionamiento del procesamiento de descubrimiento del aparato proveedor que se ejecutará en la segunda realización.

El control del procesamiento de descubrimiento del aparato proveedor se describirá a continuación haciendo referencia a este diagrama de flujo.

Un aparato inicia el procesamiento descrito utilizando la figura 8 en respuesta a una instrucción de inicio de procesamiento de configuración automática de los parámetros de la comunicación (pulsando el botón de configuración 106), e inicia el procesamiento de descubrimiento del aparato proveedor en la etapa S805. Después de que se inicia el procesamiento de descubrimiento del aparato proveedor, el aparato inicia el temporizador T1 (S1801).

El aparato cambia un canal de la LAN inalámbrica del canal actual de la LAN inalámbrica a un canal predeterminado de la LAN inalámbrica (S1802). Cabe señalar que, como canal predeterminado de la LAN

inalámbrica, se puede utilizar uno predeterminado de los canales de comunicación disponibles en una red de comunicación. Como canal predeterminado de la LAN inalámbrica, se puede utilizar un canal de comunicación que no se utiliza en una comunicación normal de entre los disponibles en una red de comunicación. Utilizando diferentes canales de comunicación como un canal de comunicación utilizado en una comunicación normal y el utilizado en el procesamiento de descubrimiento del aparato proveedor, el procesamiento de descubrimiento del aparato proveedor puede ser ejecutado sin influir en la comunicación entre otros aparatos.

Después de cambiar el canal de la LAN inalámbrica, el aparato inicia el procesamiento de transmisión de baliza (señal de notificación) (S1803). Después de que se inicia el procesamiento de transmisión de baliza, supóngase que el aparato ejecuta el control de transmisión de baliza utilizando un intervalo de baliza basado en el estándar IEEE 802.11, y sigue transmitiendo señales de baliza periódicamente.

El aparato determina si el temporizador T1 ha alcanzado un tiempo límite (S1804). Si el temporizador T1 aún no ha alcanzado un tiempo límite, el aparato transmite una señal de búsqueda (solicitud de sondeo) (S1805). Después de que se ha transmitido la señal de búsqueda, el aparato determina si se recibe una respuesta de búsqueda (S1806). Si no se recibe respuesta a la búsqueda, el proceso vuelve a la etapa S1804 para determinar el período de tiempo restante del temporizador T1. Si el temporizador aún no ha alcanzado un límite de tiempo, el aparato repite de nuevo el procesamiento desde la transmisión de una señal de búsqueda.

Si se recibe una respuesta de búsqueda en la etapa S1806, el aparato confirma el contenido de la señal de respuesta de búsqueda recibida para determinar si la función de un aparato asociado es “aparato proveedor de parámetros de la comunicación” (S1807). Si la función del aparato asociado es “aparato proveedor de parámetros de la comunicación”, el aparato guarda el resultado de la búsqueda (S1808), finalizando de este modo el proceso de descubrimiento del aparato proveedor.

Como resultado del procesamiento de determinación en la etapa S1807, si la función del aparato asociado no es “aparato proveedor de parámetros de la comunicación”, el proceso vuelve a la etapa S1804 para determinar el período de tiempo restante del temporizador T1. Si el temporizador aún no ha alcanzado un límite de tiempo, el aparato repite de nuevo el procesamiento desde la transmisión de una señal de búsqueda. Cabe señalar que si el temporizador T1 ha alcanzado un límite de tiempo en la etapa S1804, el aparato determina que no se detecta ningún aparato proveedor, finalizando de este modo el procesamiento de descubrimiento del aparato proveedor.

Cabe señalar que el procesamiento de configuración automática de los parámetros de la comunicación ejecutado por el procesamiento de recepción de parámetros de la comunicación en la etapa S810 y el procesamiento de suministro de parámetros de la comunicación en la etapa S817 se ejecutan utilizando el canal de comunicación predeterminado. Por lo tanto, cuando el proceso avanza de la etapa S802 a la etapa S815, el canal de comunicación predeterminado se configura como canal de comunicación en la etapa S815. Después de que el procesamiento de suministro de parámetros de la comunicación haya tenido éxito o haya finalizado como un error, el canal de comunicación es restaurado al estado anterior al inicio del procesamiento de configuración automática de los parámetros de la comunicación. En esta realización, por ejemplo, el canal de comunicación es restaurado en las etapas S820 y S821. Asimismo, cuando el procesamiento de recepción de los parámetros de la comunicación finaliza como un error, el canal de comunicación puede ser restaurado al estado anterior al inicio del procesamiento de configuración automática de los parámetros de la comunicación. En esta realización, por ejemplo, el canal de comunicación puede ser restaurado en la etapa S813.

Tal como se describió anteriormente, según esta realización, puesto que el procesamiento de descubrimiento del aparato proveedor se ejecuta en el canal predeterminado de la LAN inalámbrica, un aparato proveedor puede ser detectado muy rápidamente. El procesamiento de la conexión de la comunicación puede ser interrumpido durante el procesamiento de configuración automática de los parámetros de la comunicación. Sin embargo, puesto que el procesamiento de descubrimiento del aparato proveedor finaliza rápidamente, se puede acortar un período de tiempo interrumpido del procesamiento de la conexión de comunicación.

Se han descrito las realizaciones preferentes de la presente invención, pero son ejemplos a efectos de la descripción de la presente invención, y el alcance de la presente invención no está limitado solamente a estas realizaciones. Se pueden realizar diversas modificaciones de las realizaciones sin apartarse del alcance de la presente invención.

En los ejemplos descritos en las realizaciones anteriores, el valor de CW se cambia para aumentar el número de veces que las balizas son transmitidas por unidad de tiempo por el aparato proveedor para que sea mayor que el de otros aparatos. Sin embargo, se pueden utilizar otros parámetros siempre que el aparato proveedor pueda aumentar el número de veces que se transmiten las balizas, para que sea mayor que el de otros aparatos. Por ejemplo, si se puede cambiar el intervalo de transmisión de las balizas (ciclo de las balizas), el

aparato proveedor disminuye el intervalo de transmisión de las balizas, aumentando de este modo el número de veces que se transmiten balizas por unidad de tiempo.

En la descripción anterior, la CW se cambia para que sea mayor o menor que el valor inicial. Puesto que los aparatos respectivos no siempre tienen el mismo valor inicial de CW, si la CW es cambiada a un valor mínimo (CWmin) o a un valor máximo (CWmax) dentro de un intervalo variable, la frecuencia de transmisión de la baliza (el número de veces) puede ser cambiado de manera más fiable. El mensaje de notificación de inicio se describe como un mensaje que notifica que se ha iniciado el proceso de configuración automática de los parámetros de la comunicación.

Sin embargo, el mensaje de notificación de inicio también se puede expresar como un mensaje que notifica el accionamiento del botón de configuración 106 o un mensaje que permite al aparato proveedor proporcionar parámetros de la comunicación a otro aparato receptor.

La descripción anterior se ha realizado tomando como ejemplo la LAN inalámbrica compatible con el estándar IEEE 802.11. Sin embargo, la presente invención puede ser llevada a cabo para otros medios inalámbricos, tales como USB inalámbrico, MBOA, Bluetooth®, UWB y ZigBee. Asimismo, la presente invención puede ser llevada a cabo para medios de comunicación por cable, tal como una LAN por cable.

Cabe señalar que "MBOA" es una abreviatura de "MultiBand OFDM Alliance". Además, la UWB incluye USB inalámbrico, 1394 inalámbrico, WINET y similares.

El identificador de red, el procedimiento de cifrado, la clave de cifrado, el procedimiento de autenticación y la clave de autenticación se han ejemplificado como los parámetros de la comunicación. Sin embargo, se pueden utilizar otros tipos de información, o se pueden incluir otros tipos de información en los parámetros de la comunicación citados anteriormente.

Tal como se describió anteriormente, según la presente invención, incluso cuando las funciones no están determinadas de antemano en el procesamiento de configuración automática de los parámetros de la comunicación, el procesamiento de configuración de los parámetros de la comunicación y el procesamiento de participación en la red pueden ser ejecutados apropiadamente sin ninguna selección de funciones por parte del usuario.

Otras realizaciones

Aspectos de la presente invención también pueden ser realizados por un ordenador de un sistema o aparato (o dispositivos tales como una CPU o MPU) que lee y ejecuta un programa grabado en un dispositivo de memoria para realizar las funciones de la realización o las realizaciones descritas anteriormente, y mediante un procedimiento, cuyas etapas son realizadas por un ordenador de un sistema o aparato, por ejemplo, leyendo y ejecutando un programa grabado en un dispositivo de memoria para realizar las funciones de la realización o las realizaciones descritas anteriormente. Con este fin, el programa es proporcionado al ordenador, por ejemplo, a través de una red o desde un medio de grabación de diversos tipos que funciona como dispositivo de memoria (por ejemplo, un medio legible por ordenador).

Si bien la presente invención se ha descrito haciendo referencia a realizaciones a modo de ejemplo, se debe comprender que la invención no está limitada a las realizaciones a modo de ejemplo dadas a conocer.

REIVINDICACIONES

1. Aparato de comunicación (101, 201) conectable a una red de comunicación, que comprende:

un medio de notificación, configurado para notificar la presencia del aparato de comunicación utilizando un canal de comunicación asignado al aparato de comunicación entre los canales de comunicación disponibles para una comunicación inalámbrica, en el que en un primer período durante el cual el medio de notificación notifica la presencia del aparato de comunicación, el aparato de comunicación es capaz de recibir una señal de búsqueda de otro aparato de comunicación, y de enviar a dicho otro aparato de comunicación una señal de respuesta de búsqueda en respuesta a dicha señal de búsqueda;
un medio de búsqueda, configurado para buscar otro aparato de comunicación mediante la transmisión de una señal de búsqueda utilizando un canal de búsqueda, en el que el canal de búsqueda es uno de los canales de comunicación disponibles para una comunicación inalámbrica;
un medio de control, configurado para controlar la realización del procesamiento por el medio de notificación durante el primer período, y para realizar el procesamiento por el medio de búsqueda para buscar otro aparato de comunicación después del primer período, en el que el medio de control está configurado para establecer el canal de búsqueda en un segundo canal de comunicación y controlar el medio de búsqueda para buscar otro aparato de comunicación utilizando el segundo canal de comunicación tras ejecutar una búsqueda de otro aparato de comunicación utilizando un primer canal de comunicación, en el que el canal de búsqueda utilizado para una búsqueda por el medio de búsqueda es cambiado intermitentemente, y el medio de control está configurado para controlar el medio de notificación de modo que la longitud del primer período sea igual a la duración del intervalo de baliza o una duración aleatoria mayor que la del intervalo de baliza; y
un medio proveedor, configurado para proporcionar información predeterminada, identificable por un usuario, para indicar el éxito de un procesamiento compartido para compartir un parámetro de comunicación con un aparato de comunicación asociado descubierto.

2. Aparato de comunicación, según la reivindicación 1, en el que la información predeterminada indica que el procesamiento compartido se ha realizado correctamente.

3. Aparato de comunicación, según la reivindicación 2, en el que el medio proveedor proporciona información de error identificable por el usuario, distinta de la información predeterminada, en caso de que se produzca un error en el procesamiento compartido.

4. Aparato de comunicación, según la reivindicación 2 o la reivindicación 3, que comprende, además, un dispositivo de visualización,
en el que el medio de suministro proporciona la información predeterminada al usuario mostrando la información predeterminada en el dispositivo de visualización.

5. Aparato de comunicación, según la reivindicación 3, que comprende, además, un dispositivo de visualización,
en el que el medio proveedor proporciona la información de error al usuario mostrando la información de error en el dispositivo de visualización.

6. Aparato de comunicación, según cualquiera de las reivindicaciones 1 a 5, en el que la señal de respuesta de búsqueda transmitida por el aparato de comunicación incluye un elemento de información que indica la función del aparato proveedor o del aparato receptor de parámetros de comunicación, determinada por el aparato de comunicación.

7. Aparato de comunicación, según la reivindicación 6, en el que la señal de respuesta de búsqueda incluye un elemento de información que indica que el aparato de comunicación tiene como función ejecutar un procesamiento compartido o información que indica que el procesamiento compartido está en ejecución.

8. Aparato de comunicación, según cualquiera de las reivindicaciones 1 a 6, en el que el aparato de comunicación ejecuta el procesamiento compartido basándose en un protocolo de registro regulado en una configuración protegida de Wi-Fi (WPS).

9. Procedimiento para controlar un aparato de comunicación (101, 201) que puede ser conectado a una red de comunicación, que comprende:

una etapa de notificación para notificar la presencia del aparato de comunicación utilizando un canal de comunicación asignado al aparato de comunicación de entre los canales de comunicación disponibles para una comunicación inalámbrica, en el que, en un primer período durante el cual la etapa de notificación notifica la presencia del aparato de comunicación, el aparato de comunicación es capaz de recibir una señal de búsqueda de otro aparato de comunicación y de enviar a dicho otro aparato de comunicación una señal de respuesta de búsqueda en respuesta a dicha señal de búsqueda;

una etapa de búsqueda, para buscar otro aparato de comunicación transmitiendo una señal de búsqueda utilizando un canal de búsqueda, en el que el canal de búsqueda es uno de los canales de comunicación disponibles para una comunicación inalámbrica;

una etapa de control, para controlar que la etapa de notificación se realice durante el primer período y la etapa de búsqueda se realice después del primer período, en el que la etapa de control controla la etapa de búsqueda para establecer el canal de búsqueda en un segundo canal de comunicación y buscar otro aparato de comunicación utilizando el segundo canal de comunicación tras ejecutar una búsqueda de otro aparato de comunicación utilizando un primer canal de comunicación, y en el que el canal de búsqueda utilizado para una búsqueda en la etapa de búsqueda es cambiado intermitentemente, y la etapa de control controla la etapa de notificación de modo que la longitud del primer período sea la duración del intervalo de baliza o una duración aleatoria mayor que la del intervalo de baliza; y

una etapa de suministro, para proporcionar información predeterminada identificable por un usuario para indicar el éxito de un procesamiento compartido para compartir un parámetro de comunicación con un aparato de comunicación asociado descubierto.

10. Programa informático, que comprende instrucciones que, cuando el programa es ejecutado por un ordenador, hacen que el ordenador lleve a cabo el procedimiento según la reivindicación 9.

FIG. 1

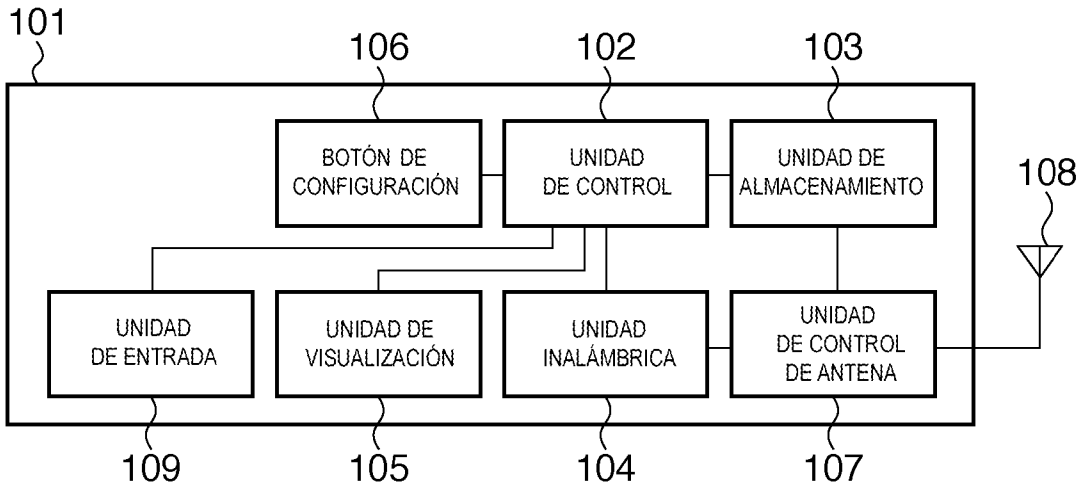

101
106
102
103
BOTÓN DE CONFIGURACIÓN
UNIDAD DE CONTROL
UNIDAD DE ALMACENAMIENTO
108
UNIDAD DE ENTRADA
UNIDAD DE VISUALIZACIÓN
UNIDAD INALÁMBRICA
UNIDAD DE CONTROL DE ANTENA
109
105
104
107

FIG. 2

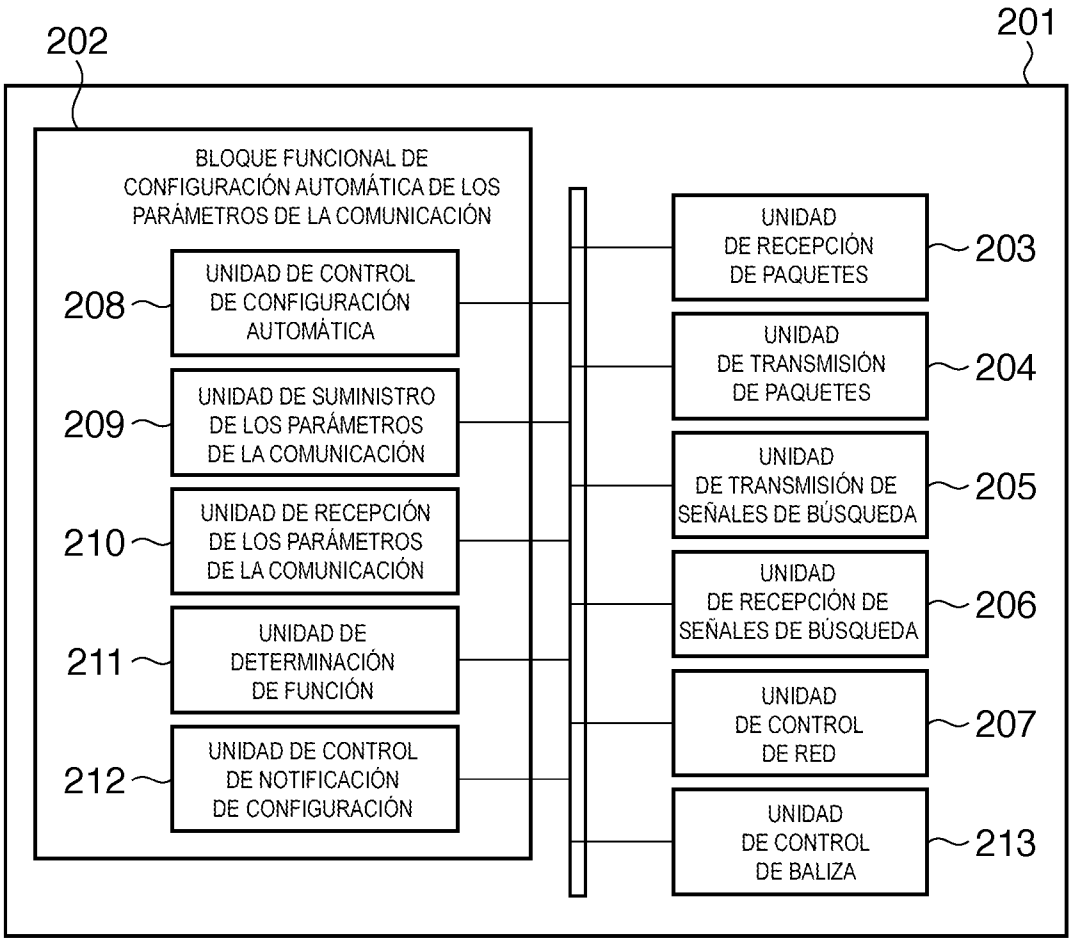

202
201
BLOQUE FUNCIONAL DE CONFIGURACIÓN AUTOMÁTICA DE LOS PARÁMETROS DE LA COMUNICACIÓN
208
UNIDAD DE CONTROL DE CONFIGURACIÓN AUTOMÁTICA
209
UNIDAD DE SUMINISTRO DE LOS PARÁMETROS DE LA COMUNICACIÓN
210
UNIDAD DE RECEPCIÓN DE LOS PARÁMETROS DE LA COMUNICACIÓN
211
UNIDAD DE DETERMINACIÓN DE FUNCIÓN
212
UNIDAD DE CONTROL DE NOTIFICACIÓN DE CONFIGURACIÓN
UNIDAD DE RECEPCIÓN DE PAQUETES
203
UNIDAD DE TRANSMISIÓN DE PAQUETES
204
UNIDAD DE TRANSMISIÓN DE SEÑALES DE BÚSQUEDA
205
UNIDAD DE RECEPCIÓN DE SEÑALES DE BÚSQUEDA
206
UNIDAD DE CONTROL DE RED
207
UNIDAD DE CONTROL DE BALIZA
213

FIG. 3

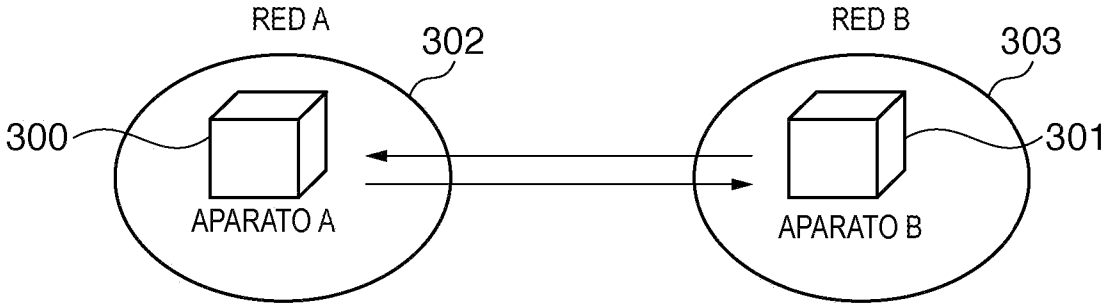

RED A
302
RED B
303
300
301
APARATO A
APARATO B

FIG. 4

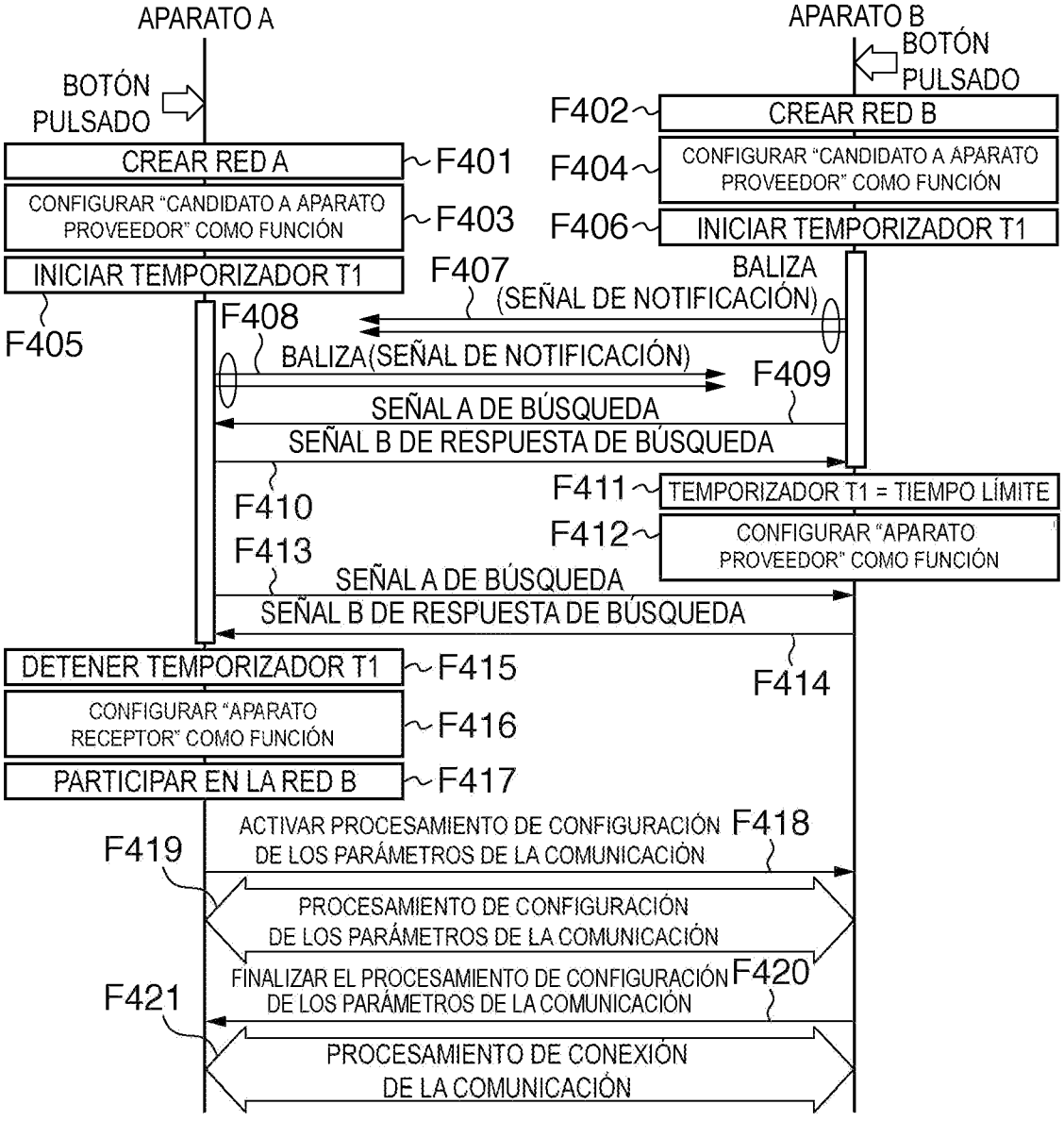

APARATO A
APARATO B
BOTÓN PULSADO
BOTÓN PULSADO
F402
CREAR RED B
CREAR RED A
F401
F404
CONFIGURAR "CANDIDATO A APARATO PROVEEDOR" COMO FUNCIÓN
CONFIGURAR "CANDIDATO A APARATO PROVEEDOR" COMO FUNCIÓN
F403
F406
INICIAR TEMPORIZADOR T1
INICIAR TEMPORIZADOR T1
F407
BALIZA (SEÑAL DE NOTIFICACIÓN)
F405
F408
BALIZA(SEÑAL DE NOTIFICACIÓN)
F409
SEÑAL A DE BÚSQUEDA
SEÑAL B DE RESPUESTA DE BÚSQUEDA
F410
F411
TEMPORIZADOR T1 = TIEMPO LÍMITE
F412
CONFIGURAR "APARATO PROVEEDOR" COMO FUNCIÓN
F413
SEÑAL A DE BÚSQUEDA
SEÑAL B DE RESPUESTA DE BÚSQUEDA
F414
DETENER TEMPORIZADOR T1
F415
CONFIGURAR "APARATO RECEPTOR" COMO FUNCIÓN
F416
PARTICIPAR EN LA RED B
F417
F418
ACTIVAR PROCESAMIENTO DE CONFIGURACIÓN DE LOS PARÁMETROS DE LA COMUNICACIÓN
F419
PROCESAMIENTO DE CONFIGURACIÓN DE LOS PARÁMETROS DE LA COMUNICACIÓN
F420
FINALIZAR EL PROCESAMIENTO DE CONFIGURACIÓN DE LOS PARÁMETROS DE LA COMUNICACIÓN
F421
PROCESAMIENTO DE CONEXIÓN DE LA COMUNICACIÓN

FIG. 5

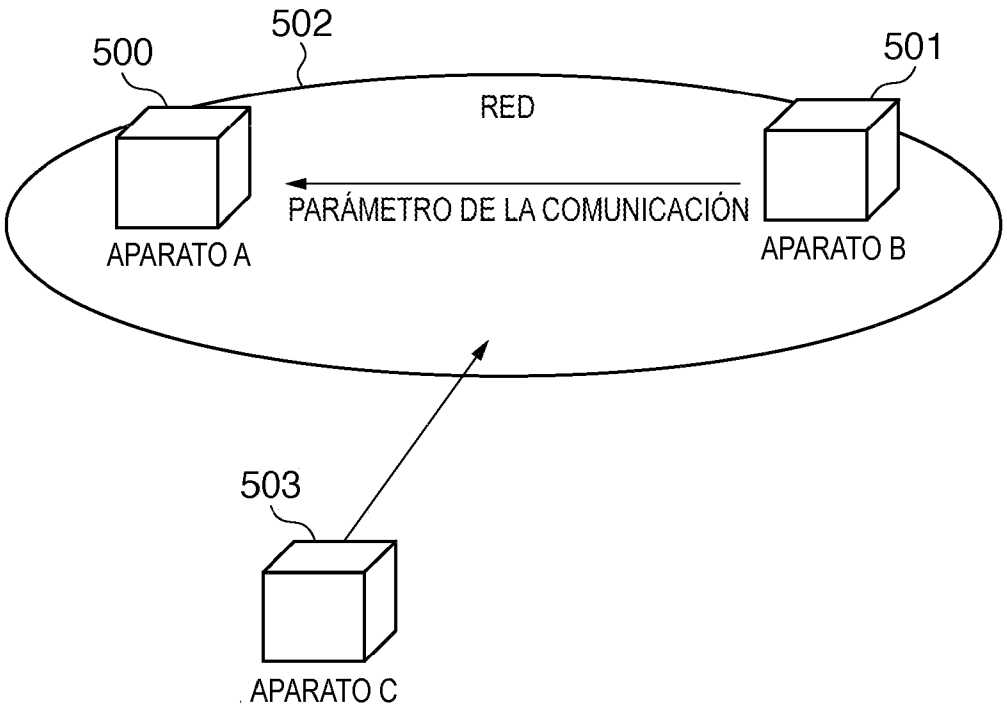

500
502
501
RED
PARÁMETRO DE LA COMUNICACIÓN
APARATO A
APARATO B
503
APARATO C

FIG. 6

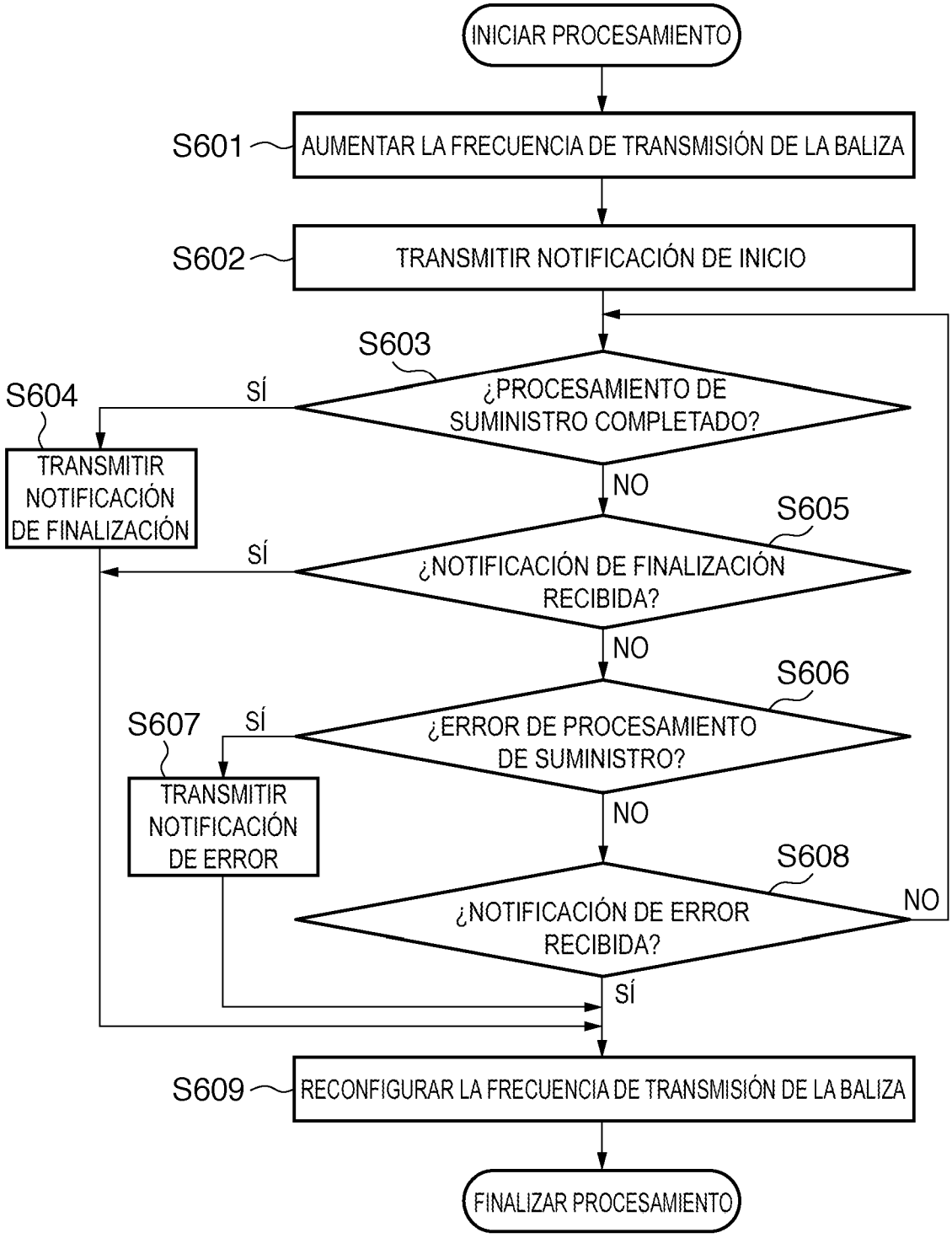

INICIAR PROCESAMIENTO
S601
AUMENTAR LA FRECUENCIA DE TRANSMISIÓN DE LA BALIZA
S602
TRANSMITIR NOTIFICACIÓN DE INICIO
S603
¿PROCESAMIENTO DE SUMINISTRO COMPLETADO?
SÍ
S604
TRANSMITIR NOTIFICACIÓN DE FINALIZACIÓN
NO
S605
¿NOTIFICACIÓN DE FINALIZACIÓN RECIBIDA?
SÍ
NO
S606
¿ERROR DE PROCESAMIENTO DE SUMINISTRO?
S607
SÍ
TRANSMITIR NOTIFICACIÓN DE ERROR
NO
S608
¿NOTIFICACIÓN DE ERROR RECIBIDA?
NO
SÍ
S609
RECONFIGURAR LA FRECUENCIA DE TRANSMISIÓN DE LA BALIZA
FINALIZAR PROCESAMIENTO

FIG. 7

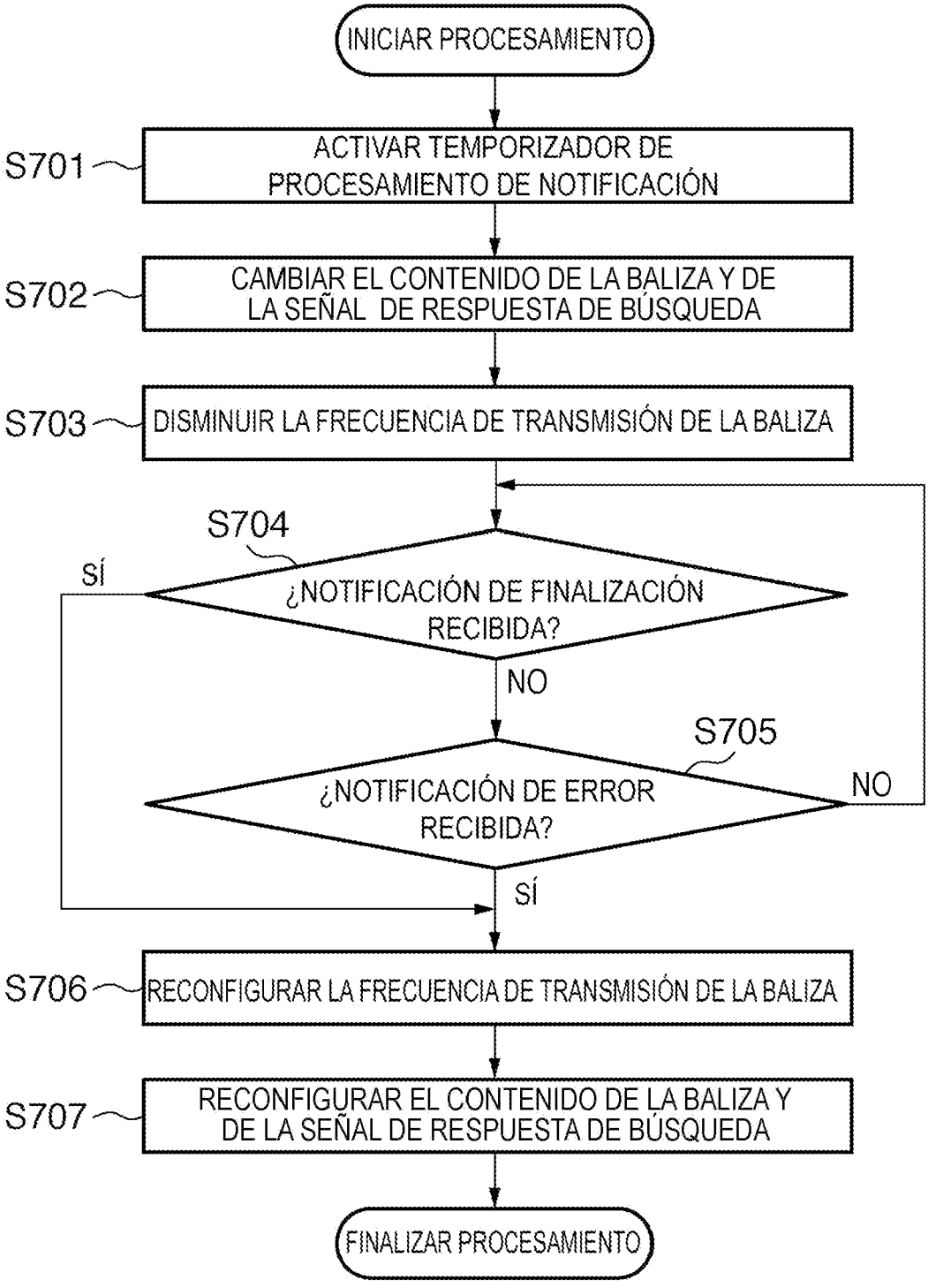

INICIAR PROCESAMIENTO
S701
ACTIVAR TEMPORIZADOR DE PROCESAMIENTO DE NOTIFICACIÓN
S702
CAMBIAR EL CONTENIDO DE LA BALIZA Y DE LA SEÑAL DE RESPUESTA DE BÚSQUEDA
S703
DISMINUIR LA FRECUENCIA DE TRANSMISIÓN DE LA BALIZA
S704
¿NOTIFICACIÓN DE FINALIZACIÓN RECIBIDA?
SÍ
NO
S705
¿NOTIFICACIÓN DE ERROR RECIBIDA?
NO
SÍ
S706
RECONFIGURAR LA FRECUENCIA DE TRANSMISIÓN DE LA BALIZA
S707
RECONFIGURAR EL CONTENIDO DE LA BALIZA Y DE LA SEÑAL DE RESPUESTA DE BÚSQUEDA
FINALIZAR PROCESAMIENTO

FIG. 8

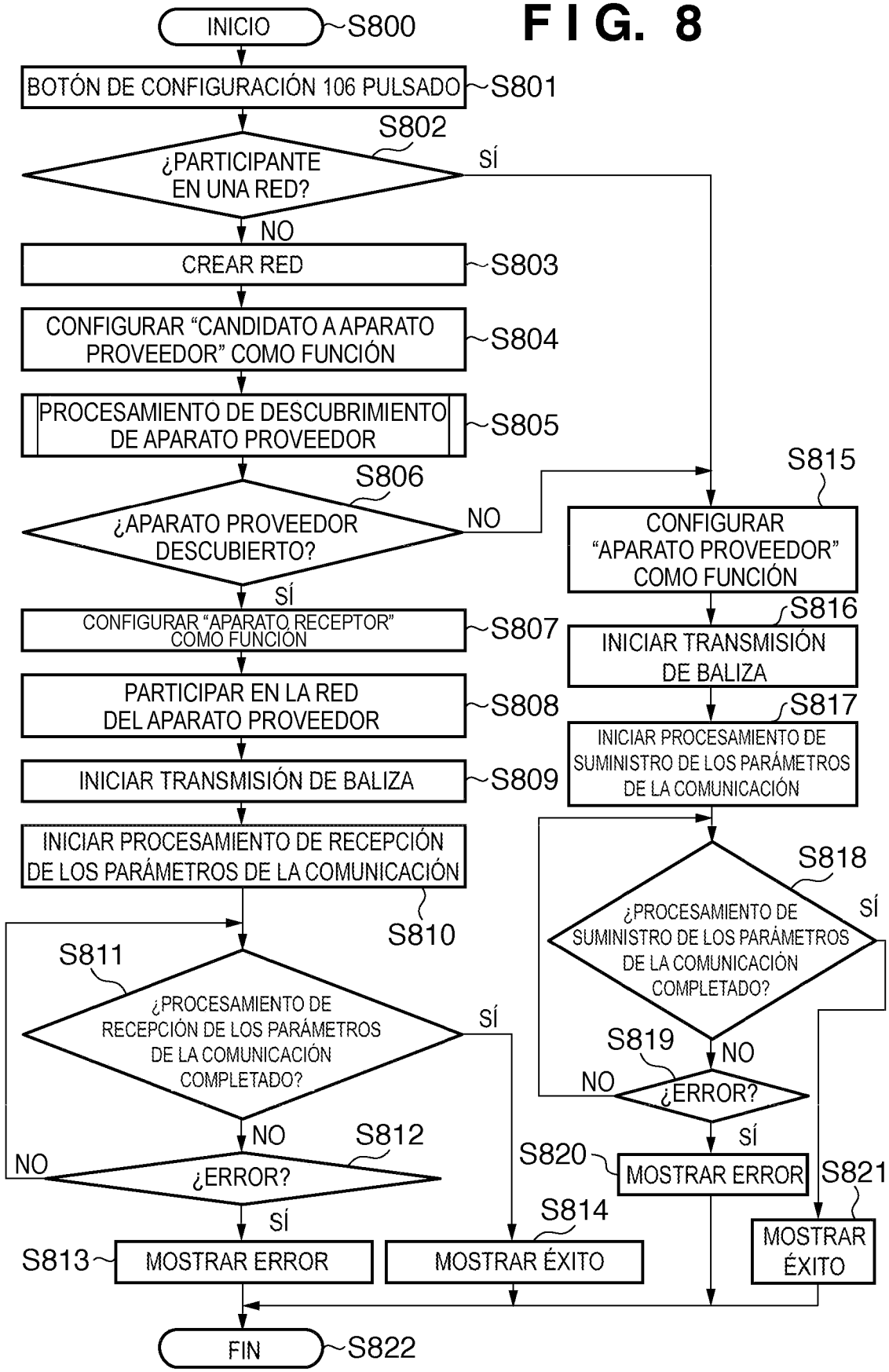
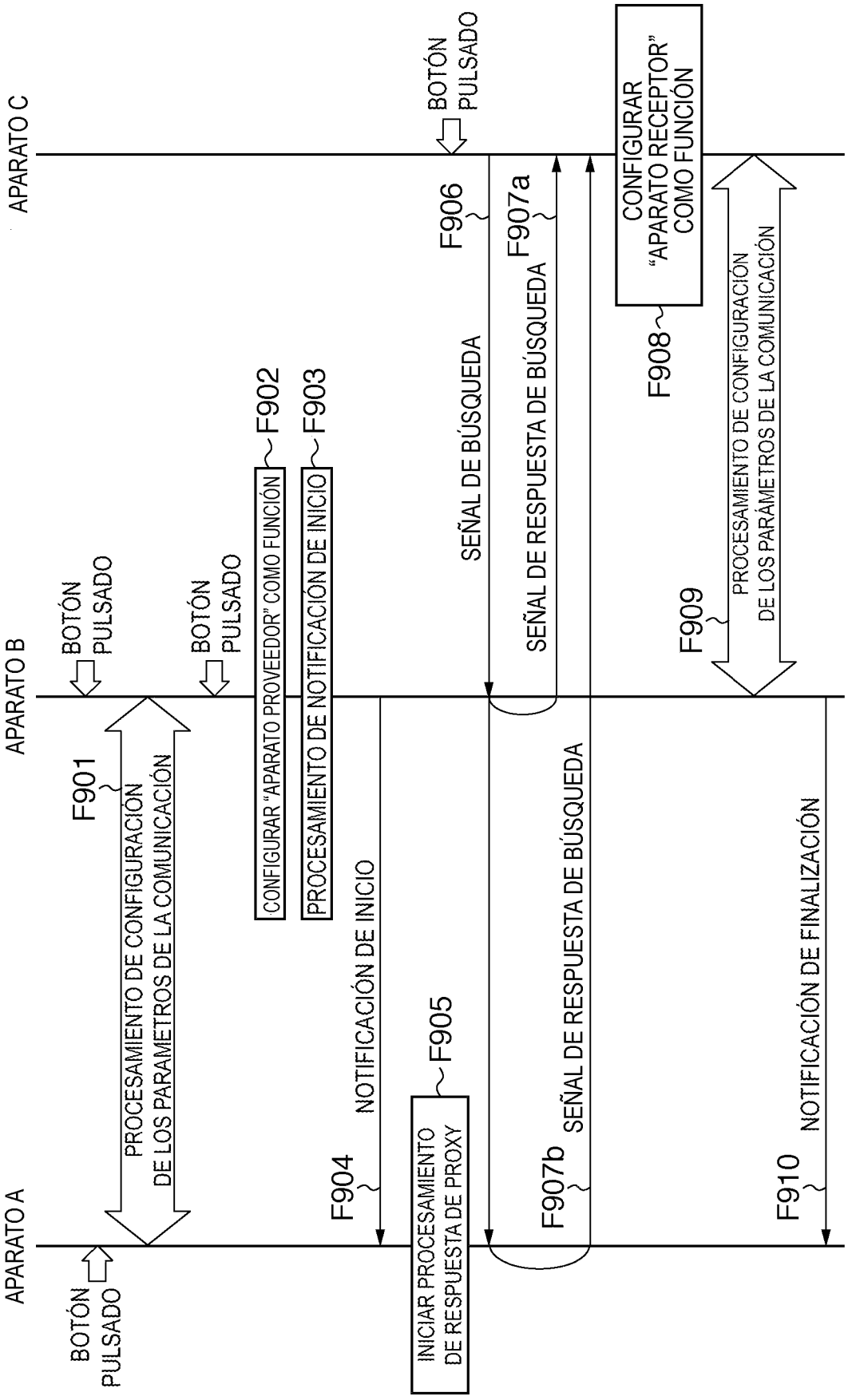

INICIO
S800
BOTÓN DE CONFIGURACIÓN 106 PULSADO
S801
S802
¿PARTICIPANTE EN UNA RED?
SÍ
NO
CREAR RED
S803
CONFIGURAR "CANDIDATO A APARATO PROVEEDOR" COMO FUNCIÓN
S804
PROCESAMIENTO DE DESCUBRIMIENTO DE APARATO PROVEEDOR
S805
S806
¿APARATO PROVEEDOR DESCUBIERTO?
NO
SÍ
CONFIGURAR "APARATO RECEPTOR" COMO FUNCIÓN
S807
PARTICIPAR EN LA RED DEL APARATO PROVEEDOR
S808
INICIAR TRANSMISIÓN DE BALIZA
S809
INICIAR PROCESAMIENTO DE RECEPCIÓN DE LOS PARÁMETROS DE LA COMUNICACIÓN
S810
S811
¿PROCESAMIENTO DE RECEPCIÓN DE LOS PARÁMETROS DE LA COMUNICACIÓN COMPLETADO?
SÍ
NO
S812
NO
¿ERROR?
SÍ
S813
MOSTRAR ERROR
S815
CONFIGURAR "APARATO PROVEEDOR" COMO FUNCIÓN
S816
INICIAR TRANSMISIÓN DE BALIZA
S817
INICIAR PROCESAMIENTO DE SUMINISTRO DE LOS PARÁMETROS DE LA COMUNICACIÓN
S818
¿PROCESAMIENTO DE SUMINISTRO DE LOS PARÁMETROS DE LA COMUNICACIÓN COMPLETADO?
SÍ
S819
NO
NO
¿ERROR?
SÍ
S820
MOSTRAR ERROR
S821
MOSTRAR ÉXITO
S814
MOSTRAR ÉXITO
FIN
S822

FIG. 9


APARATO A
APARATO B
APARATO C
BOTÓN PULSADO
BOTÓN PULSADO
BOTÓN PULSADO
F901
PROCESAMIENTO DE CONFIGURACIÓN DE LOS PARAMETROS DE LA COMUNICACIÓN
CONFIGURAR "APARATO PROVEEDOR" COMO FUNCIÓN
F902
PROCESAMIENTO DE NOTIFICACIÓN DE INICIO
F903
NOTIFICACIÓN DE INICIO
F904
INICIAR PROCESAMIENTO DE RESPUESTA DE PROXY
F905
SEÑAL DE BÚSQUEDA
F906
SEÑAL DE RESPUESTA DE BÚSQUEDA
F907a
SEÑAL DE RESPUESTA DE BÚSQUEDA
F907b
CONFIGURAR "APARATO RECEPTOR" COMO FUNCIÓN
F908
PROCESAMIENTO DE CONFIGURACIÓN DE LOS PARÁMETROS DE LA COMUNICACIÓN
F909
NOTIFICACIÓN DE FINALIZACIÓN
F910

F I G. 10

PROCEDIMIENTO DE AUTENTICACIÓN/CIFRADO ADMITIDO

PROCEDIMIENTO DE AUTENTICACIÓN	PROCEDIMIENTO DE CIFRADO
Abierta	NO CIFRADO
	WEP
Compartida	WEP
WPA	TKIP
	CCMP
WPA-PSK	TKIP
	CCMP
WPA2	TKIP
	CCMP
WPA2-PSK	TKIP
	CCMP

FIG. 11

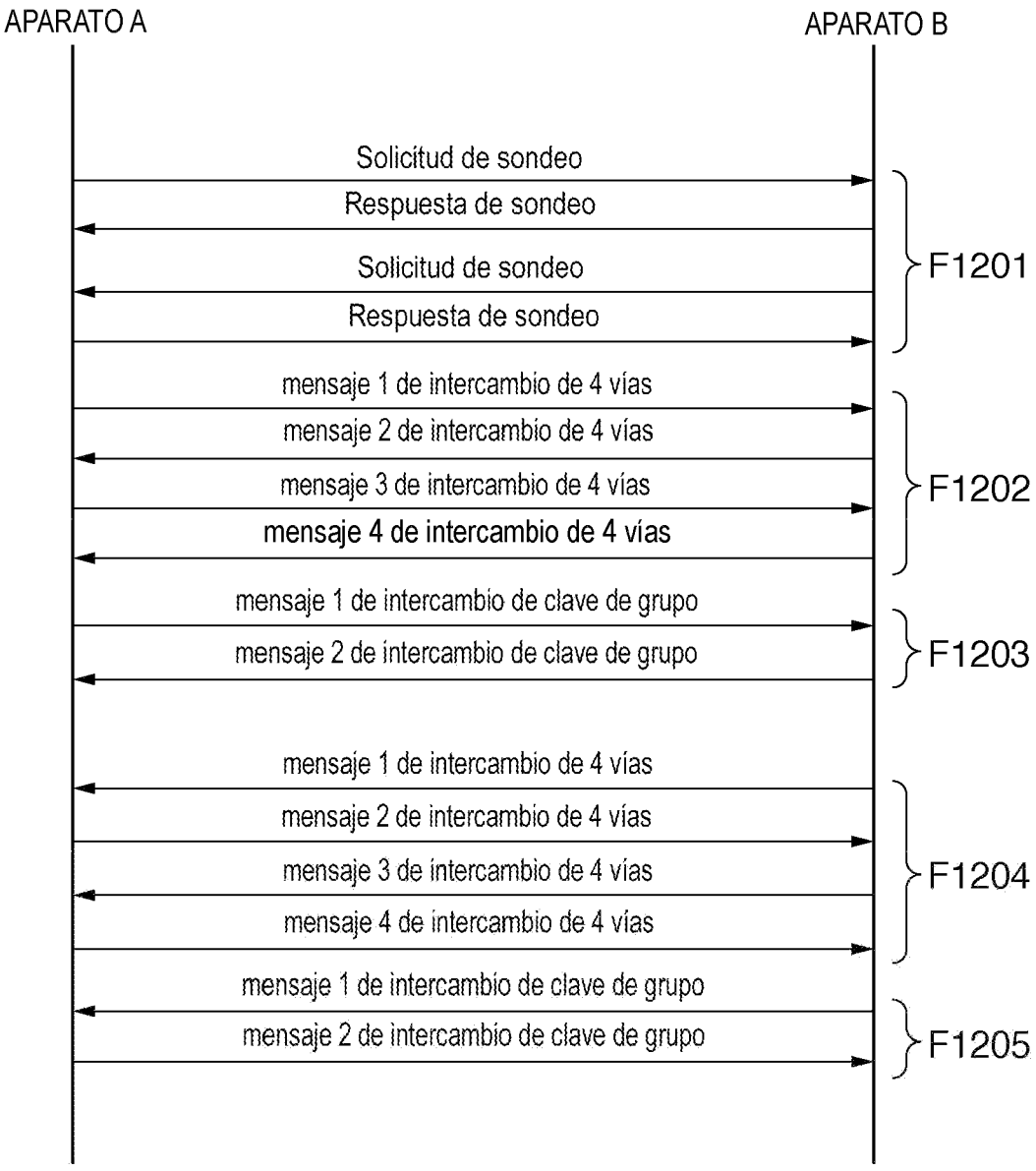
NÚMERO DE CLAVES GUARDADAS

PROCEDIMIENTO	Clave por parejas	Clave de grupo	Total
IEEE802. 11i Espec. completa	n – 1	n + 1	2n
(1) reducir secuencia	n – 1	n + 1	2n
(2) reducir clave	n – 1	1	n
(3) WPA-Ninguno	0	1	1
(4) Intercambio de clave de WPA sobre intercambio de WPS	n – 1	n + 1 o 1	2n o n

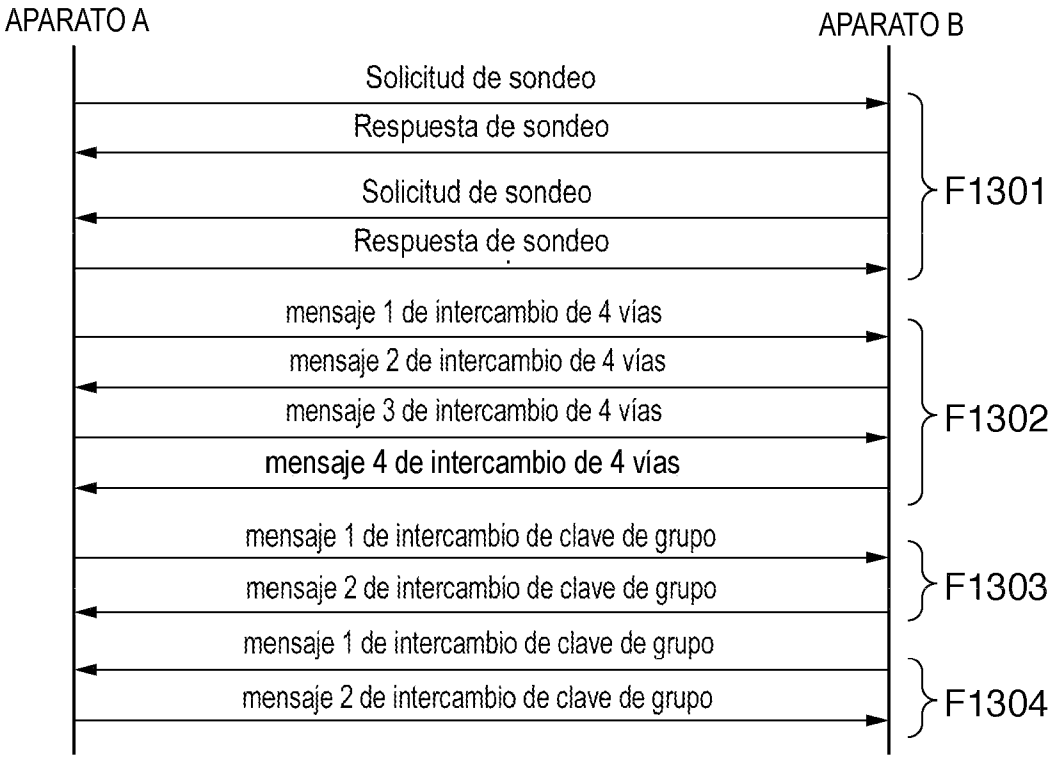
NÚMERO DE INTERCAMBIOS DE CLAVE EJECUTADOS POR OTRO APARATO

PROCEDIMIENTO	Intercambio de 4 vías	Intercambio de clave de grupo
IEEE802. 11i Espec. completa	2	2
(1) Reducir secuencia	1	2
(2) Reducir clave	1 o 2	1
(3) WPA-Ninguno	0	0
(4) Cambio de clave de WPA sobre intercambio de WPS	0	0 o 1 o 2

FIG. 12


APARATO A
APARATO B
Solicitud de sondeo
Respuesta de sondeo
Solicitud de sondeo
Respuesta de sondeo
F1201
mensaje 1 de intercambio de 4 vías
mensaje 2 de intercambio de 4 vías
mensaje 3 de intercambio de 4 vías
mensaje 4 de intercambio de 4 vías
F1202
mensaje 1 de intercambio de clave de grupo
mensaje 2 de intercambio de clave de grupo
F1203
mensaje 1 de intercambio de 4 vías
mensaje 2 de intercambio de 4 vías
mensaje 3 de intercambio de 4 vías
mensaje 4 de intercambio de 4 vías
F1204
mensaje 1 de intercambio de clave de grupo
mensaje 2 de intercambio de clave de grupo
F1205

F I G. 13


APARATO A
APARATO B
Solicitud de sondeo
Respuesta de sondeo
Solicitud de sondeo
Respuesta de sondeo
F1301
mensaje 1 de intercambio de 4 vías
mensaje 2 de intercambio de 4 vías
mensaje 3 de intercambio de 4 vías
mensaje 4 de intercambio de 4 vías
F1302
mensaje 1 de intercambio de clave de grupo
mensaje 2 de intercambio de clave de grupo
F1303
mensaje 1 de intercambio de clave de grupo
mensaje 2 de intercambio de clave de grupo
F1304

F I G. 14

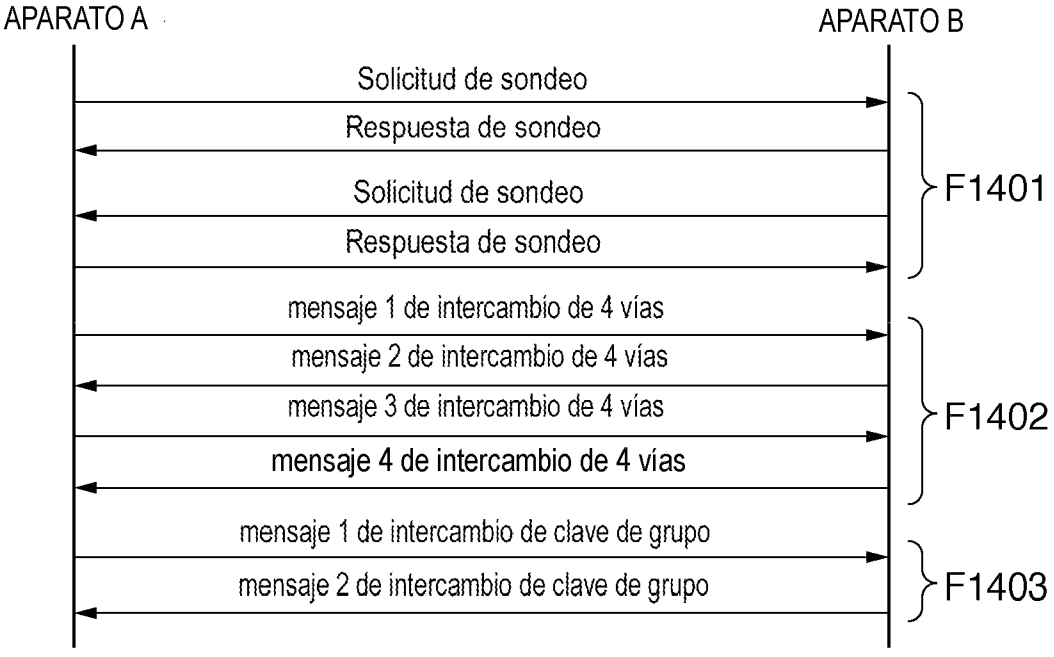

APARATO A
APARATO B
Solicitud de sondeo
Respuesta de sondeo
Solicitud de sondeo
Respuesta de sondeo
F1401
mensaje 1 de intercambio de 4 vías
mensaje 2 de intercambio de 4 vías
mensaje 3 de intercambio de 4 vías
mensaje 4 de intercambio de 4 vías
F1402
mensaje 1 de intercambio de clave de grupo
mensaje 2 de intercambio de clave de grupo
F1403

FIG. 15

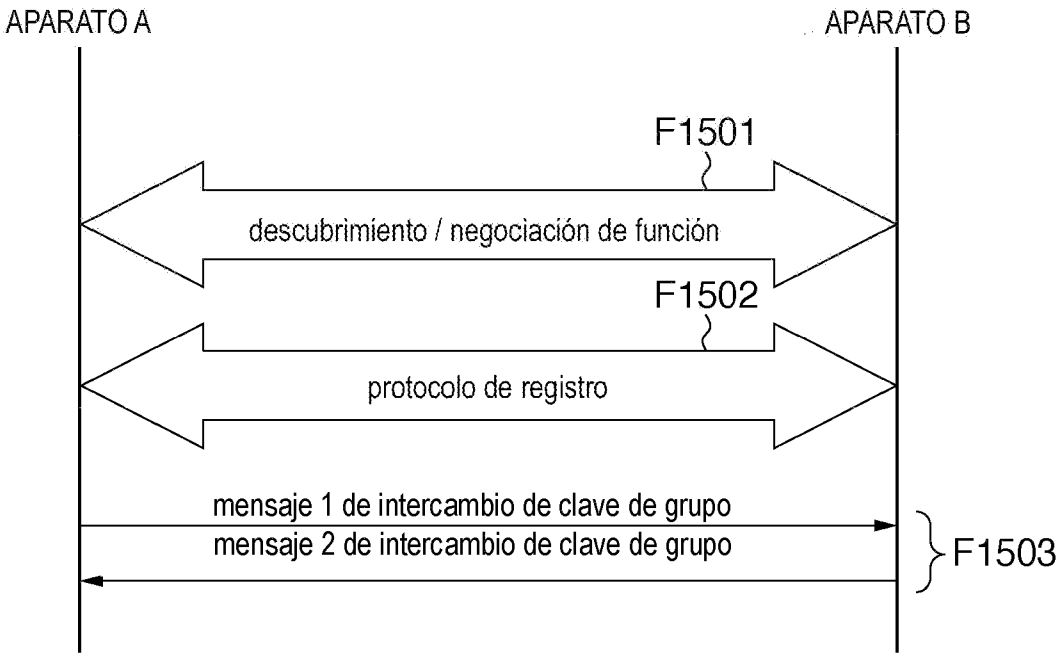

APARATO A
APARATO B
F1501
descubrimiento / negociación de función
F1502
protocolo de registro
mensaje 1 de intercambio de clave de grupo
mensaje 2 de intercambio de clave de grupo
F1503

FIG. 16

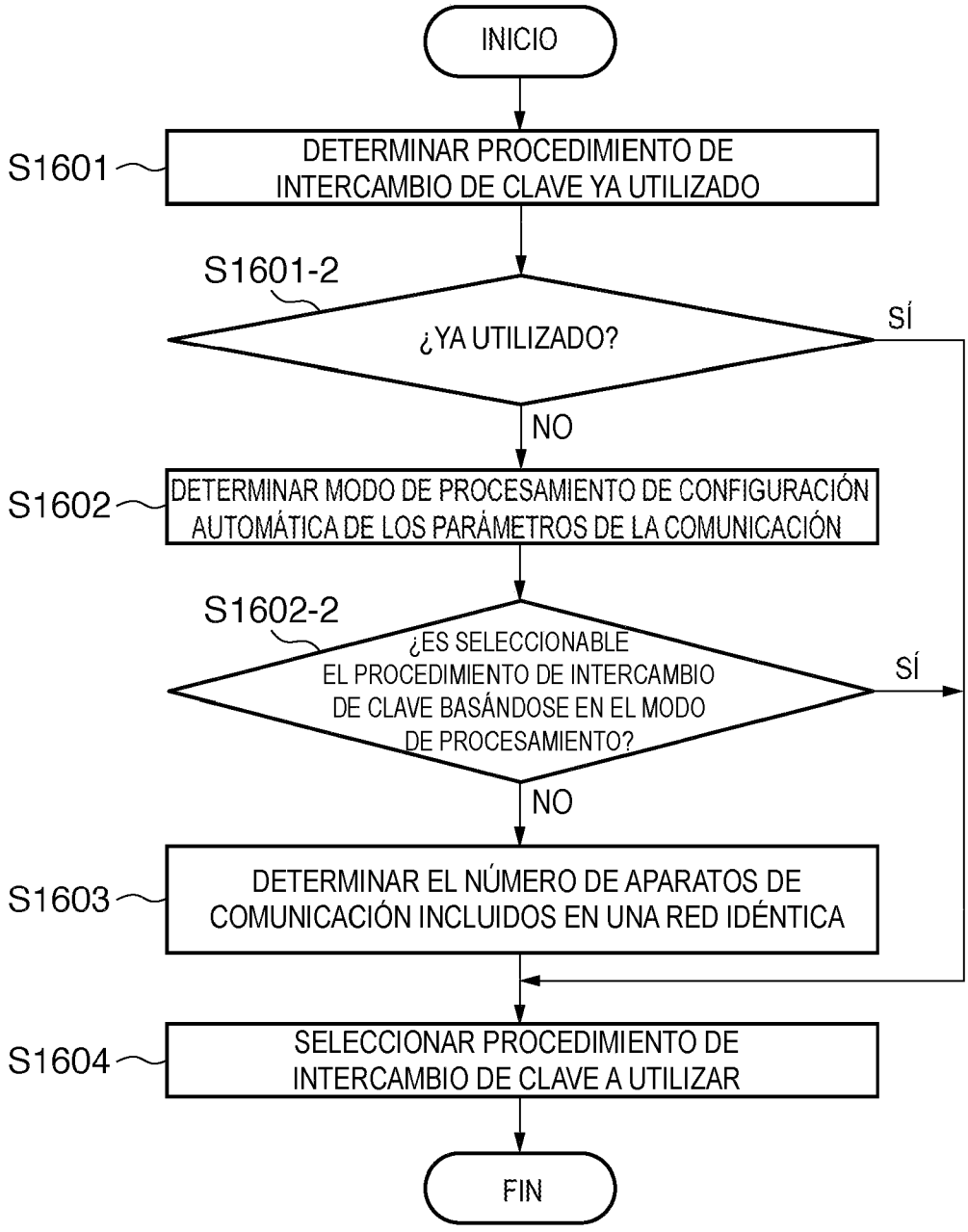

INICIO
S1601
DETERMINAR PROCEDIMIENTO DE INTERCAMBIO DE CLAVE YA UTILIZADO
S1601-2
¿YA UTILIZADO?
SÍ
NO
S1602
DETERMINAR MODO DE PROCESAMIENTO DE CONFIGURACIÓN AUTOMÁTICA DE LOS PARÁMETROS DE LA COMUNICACIÓN
S1602-2
¿ES SELECCIONABLE EL PROCEDIMIENTO DE INTERCAMBIO DE CLAVE BASÁNDOSE EN EL MODO DE PROCESAMIENTO?
SÍ
NO
S1603
DETERMINAR EL NÚMERO DE APARATOS DE COMUNICACIÓN INCLUIDOS EN UNA RED IDÉNTICA
S1604
SELECCIONAR PROCEDIMIENTO DE INTERCAMBIO DE CLAVE A UTILIZAR
FIN

FIG. 17

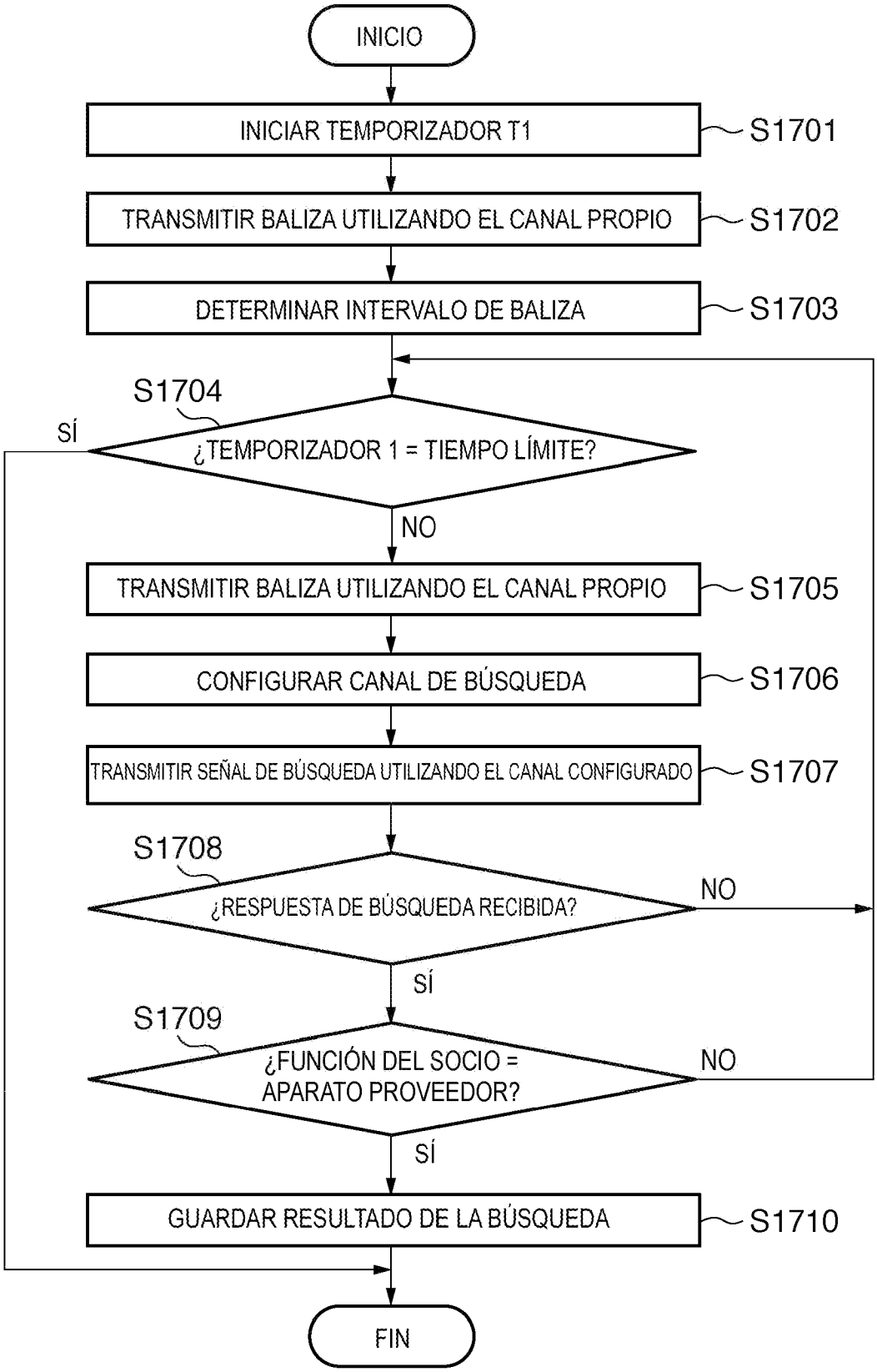

INICIO
INICIAR TEMPORIZADOR T1
S1701
TRANSMITIR BALIZA UTILIZANDO EL CANAL PROPIO
S1702
DETERMINAR INTERVALO DE BALIZA
S1703
S1704
¿TEMPORIZADOR 1 = TIEMPO LÍMITE?
SÍ
NO
TRANSMITIR BALIZA UTILIZANDO EL CANAL PROPIO
S1705
CONFIGURAR CANAL DE BÚSQUEDA
S1706
TRANSMITIR SEÑAL DE BÚSQUEDA UTILIZANDO EL CANAL CONFIGURADO
S1707
S1708
¿RESPUESTA DE BÚSQUEDA RECIBIDA?
NO
SÍ
S1709
¿FUNCIÓN DEL SOCIO = APARATO PROVEEDOR?
NO
SÍ
GUARDAR RESULTADO DE LA BÚSQUEDA
S1710
FIN

FIG. 18

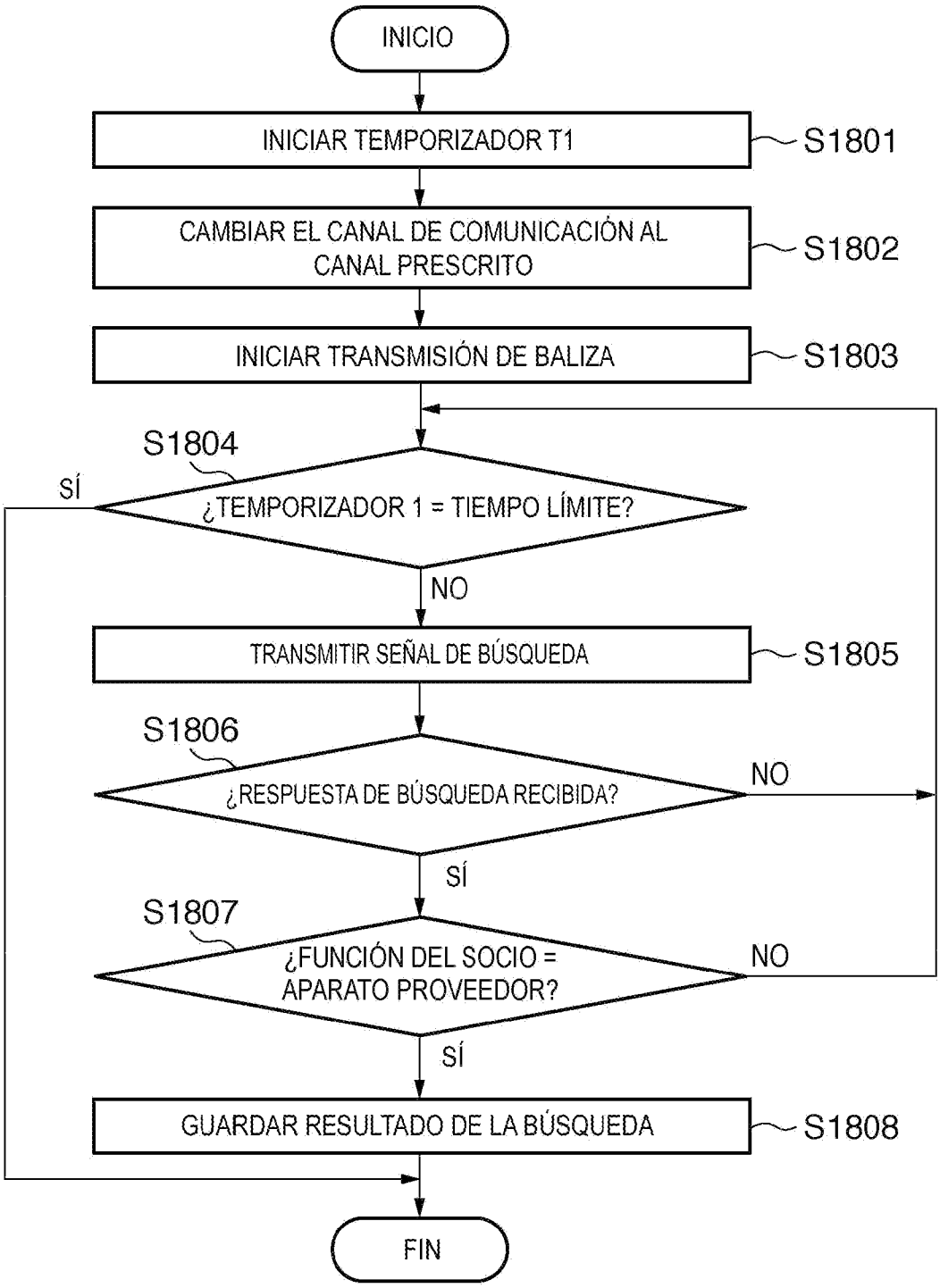

INICIO
INICIAR TEMPORIZADOR T1
S1801
CAMBIAR EL CANAL DE COMUNICACIÓN AL CANAL PRESCRITO
S1802
INICIAR TRANSMISIÓN DE BALIZA
S1803
S1804
¿TEMPORIZADOR 1 = TIEMPO LÍMITE?
SÍ
NO
TRANSMITIR SEÑAL DE BÚSQUEDA
S1805
S1806
¿RESPUESTA DE BÚSQUEDA RECIBIDA?
NO
SÍ
S1807
¿FUNCIÓN DEL SOCIO = APARATO PROVEEDOR?
NO
SÍ
GUARDAR RESULTADO DE LA BÚSQUEDA
S1808
FIN

FIG. 19

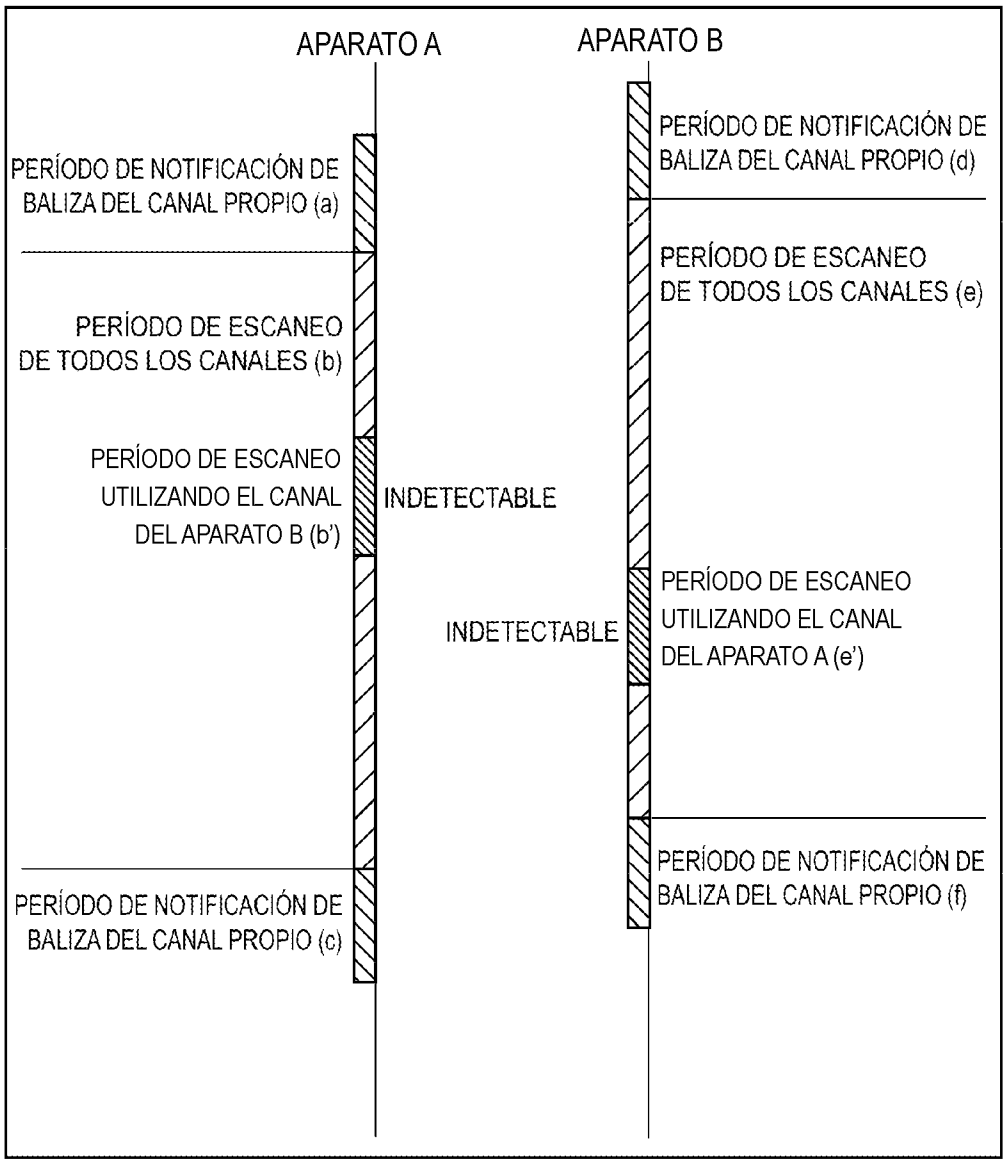
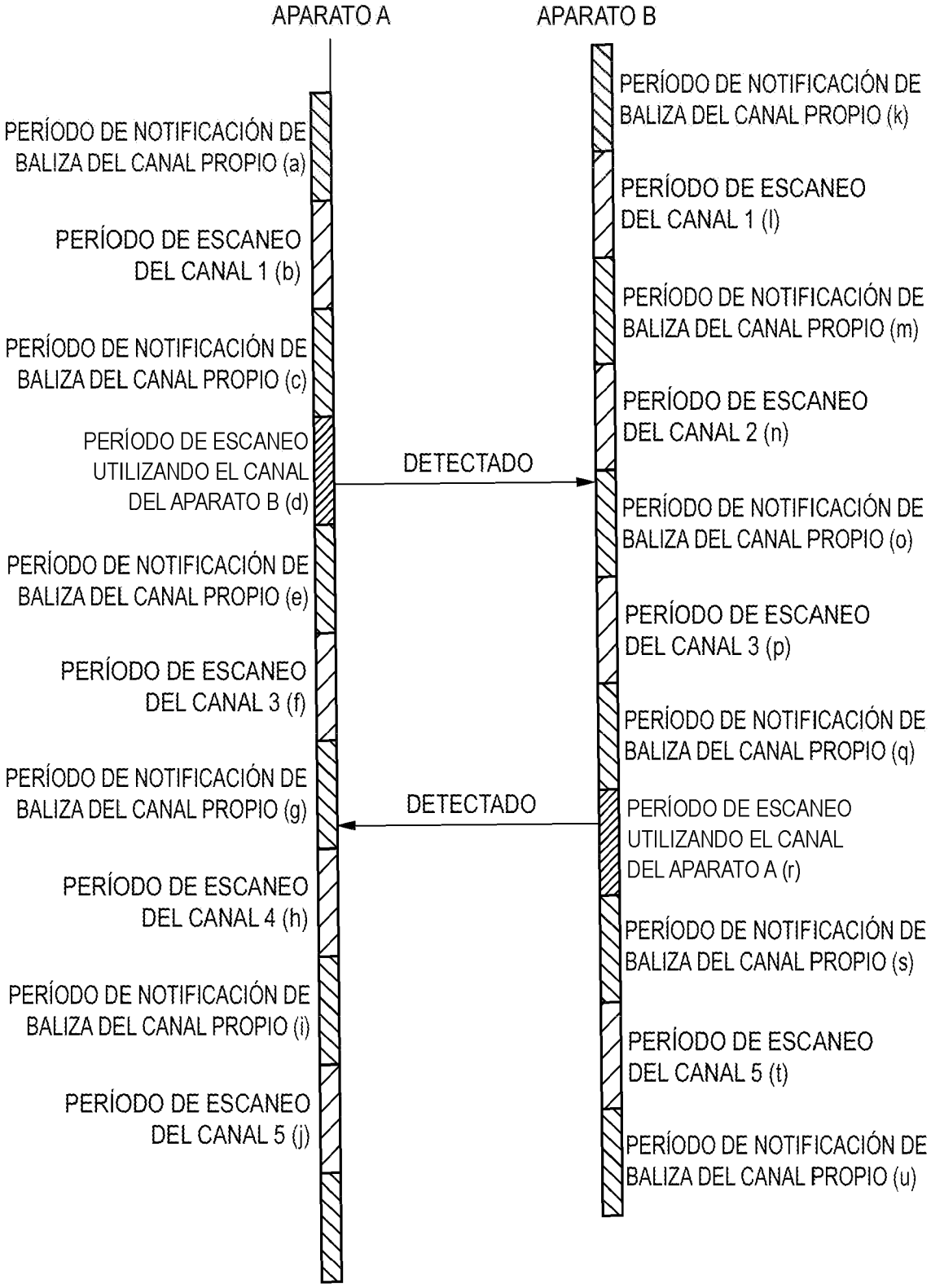

APARATO A
APARATO B
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (a)
PERÍODO DE ESCANEO DE TODOS LOS CANALES (b)
PERÍODO DE ESCANEO UTILIZANDO EL CANAL DEL APARATO B (b')
INDETECTABLE
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (c)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (d)
PERÍODO DE ESCANEO DE TODOS LOS CANALES (e)
INDETECTABLE
PERÍODO DE ESCANEO UTILIZANDO EL CANAL DEL APARATO A (e')
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (f)

FIG. 20


APARATO A
APARATO B
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (a)
PERÍODO DE ESCANEO DEL CANAL 1 (b)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (c)
PERÍODO DE ESCANEO UTILIZANDO EL CANAL DEL APARATO B (d)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (e)
PERÍODO DE ESCANEO DEL CANAL 3 (f)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (g)
PERÍODO DE ESCANEO DEL CANAL 4 (h)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (i)
PERÍODO DE ESCANEO DEL CANAL 5 (j)
DETECTADO
DETECTADO
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (k)
PERÍODO DE ESCANEO DEL CANAL 1 (l)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (m)
PERÍODO DE ESCANEO DEL CANAL 2 (n)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (o)
PERÍODO DE ESCANEO DEL CANAL 3 (p)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (q)
PERÍODO DE ESCANEO UTILIZANDO EL CANAL DEL APARATO A (r)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (s)
PERÍODO DE ESCANEO DEL CANAL 5 (t)
PERÍODO DE NOTIFICACIÓN DE BALIZA DEL CANAL PROPIO (u)