(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 790 352**

(51) Int. CI.:

H04W 40/24 (2009.01)
H04W 40/32 (2009.01)
H04W 36/22 (2009.01)
H04W 84/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.05.2012 E 18184350 (9)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3410779**

(54) Título: **Traspaso/migración de dispositivo eficiente en redes de malla**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.10.2020

(73) Titular/es:

ITRON GLOBAL SARL (100.0%)
2111 North Molter Road
Liberty Lake WA 99019, US

(72) Inventor/es:

POPA, DANIEL;
NGUYEN, VIET HUNG;
MANI, MEHDI;
MAINAUD, BASTIEN y
GARRISON STUBER, MICHAEL T.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Traspaso/migración de dispositivo eficiente en redes de malla

Antecedentes

Con el advenimiento de la tecnología de dispositivos inteligentes, hoy en día se ha implementado un número cada vez mayor de dispositivos inteligentes para usos residenciales, comerciales y militares. Los ejemplos de estos dispositivos incluyen contadores de servicio público inteligentes, sensores, dispositivos de control, encaminadores, reguladores, etc. En general, cuando se implementa un nuevo dispositivo, un técnico irá a un sitio en donde se implementará el nuevo dispositivo y configurará manualmente el nuevo dispositivo en el sitio. El técnico puede, por ejemplo, configurar y autenticar el nuevo dispositivo con una red. El técnico puede entonces registrar el nuevo dispositivo con la red y posiblemente un servidor central que mantiene información de cada dispositivo en la red.

La forma convencional de registrarse y unirse a una red inalámbrica supone una gran carga para la red inalámbrica y puede generar congestión en una red ya cargada. El enfoque convencional para unirse a una red inalámbrica consta de tres etapas: en primer lugar, un nodo de unión ha de completar la autenticación 802.1x, entonces el nodo se comunica con un servidor de Protocolo de Configuración Dinámica de Anfitrión (DHCP) para adquirir una dirección de protocolo de Internet (IP) y, por último, el nodo contacta con un servidor de gestión de red (NMS) para obtener la información de configuración requerida. Estas tres etapas exigen un intenso intercambio de paquetes de extremo a extremo, que proporciona una carga considerable para redes de comunicación inalámbrica expuestas a condiciones exigentes.

Wanshi Qui y col.: "An efficient self-healing process for ZigBee sensor networks" (ISBN: 978-1-4244-0976-1; 2007), propone un proceso para que una red ZigBee se repare a sí misma después de un fallo de nodo o ruptura de comunicación. El proceso deja que un nodo desconectado se reconecte a la red junto con tantos nodos descendientes como sea posible.

Sumario

De acuerdo con un primer aspecto, se proporciona un método como se define en la reivindicación 1. De acuerdo con un segundo aspecto, se proporciona un dispositivo como se define en la reivindicación 5. En las reivindicaciones dependientes se definen características opcionales de aspectos.

Breve descripción de los dibujos

La descripción detallada se expone con referencia a las figuras adjuntas. En las figuras, el dígito o dígitos más a la izquierda de un número de referencia identifican la figura en la que aparece por primera vez el número de referencia. El uso de los mismos números de referencia en figuras diferentes indica unos elementos similares o idénticos.

La figura 1 ilustra un entorno ilustrativo utilizable para implementar el registro y/o la migración de un dispositivo en una red.
La figura 2 ilustra el dispositivo ilustrativo de la figura 1 con más detalle.
La figura 3 ilustra un método ilustrativo de registro de dispositivo en una red.
La figura 4 ilustra un método ilustrativo para determinar si permitir o rechazar una solicitud de un dispositivo para unirse a una red.
La figura 5 ilustra un método ilustrativo de migración de dispositivo de una red a otra.

Descripción detallada

Vista general

Como se observó anteriormente, la implementación existente de un nuevo dispositivo requiere, en general, que un técnico configure y autentique manualmente el nuevo dispositivo con una red en el sitio y conecte el nuevo dispositivo a la red. Este proceso de conexión y autenticación puede ser engorroso y consumir mucho tiempo. La situación se vuelve más complicada cuando la red está a su capacidad máxima o cerca de la misma (por ejemplo, tiene un ancho de banda restante limitado o nulo para soportar el nuevo dispositivo). En ese caso, el técnico puede intentar conectar el nuevo dispositivo a otra red disponible, si existe alguna. Estas situaciones no solo presentan dificultades para implementar nuevos dispositivos y migrar nodos de una red a otra, sino que también crean problemas a la hora de sincronizar diferentes dispositivos dentro de y entre redes.

Esta divulgación describe métodos para el registro automatizado de dispositivos y la migración de dispositivos en una red de encaminamiento autónoma. Los métodos permiten el registro automático de un nuevo dispositivo en una red a través de un número mínimo de intercambios entre el nuevo dispositivo y la red. Además, los métodos permiten la migración o el traspaso de un dispositivo desde una red a otra red debido a una condición de la red y/o una condición del nuevo dispositivo que se va a implementar en la red.

En general, un dispositivo puede solicitar unirse a una red. En algunas implementaciones, el dispositivo solicitante puede, o no, saber qué dispositivo asociado con la red es responsable de direccionar o controlar una admisión de un nuevo dispositivo para unirse a la red. En algunas implementaciones, el dispositivo solicitante puede transmitir una solicitud para unirse a la red, que puede ser escuchado por dispositivos vecinos (es decir, dispositivos que están dentro del alcance de transmisión del dispositivo solicitante). De forma adicional, o como alternativa, el dispositivo solicitante puede descubrir dispositivos vecinos en la red al escuchar por casualidad transmisiones desde los dispositivos vecinos. El dispositivo solicitante puede entonces enviar la solicitud directamente a los dispositivos vecinos a través de un mensaje o baliza, por ejemplo.

En respuesta a la recepción de la solicitud, el dispositivo vecino puede analizar la solicitud y saber que el dispositivo solicitante solicita unirse a la red. En una implementación, el dispositivo vecino puede transmitir la solicitud del dispositivo solicitante a un dispositivo de control que es responsable de direccionar o controlar una admisión de un nuevo dispositivo para unirse a la red. Como alternativa, el dispositivo vecino puede retransmitir la solicitud a un dispositivo en la red que sea un dispositivo primario del dispositivo vecino, dirigiendo el dispositivo primario para retransmitir la solicitud al dispositivo de control u otro dispositivo que esté jerárquicamente más cerca del dispositivo de control que el dispositivo primario. En una implementación, el dispositivo vecino puede retransmitir la solicitud a su dispositivo primario si, por ejemplo, el dispositivo vecino no sabe qué dispositivo es responsable de direccionar o controlar una admisión de un nuevo dispositivo para unirse a la red.

Independientemente de si la solicitud se retransmite al dispositivo de control o al dispositivo primario, el dispositivo vecino puede insertar una dirección de destino (por ejemplo, una dirección IP del dispositivo de control o el dispositivo primario) en la solicitud, indicando un destino al que la solicitud está dirigido.

En respuesta a la recepción de la solicitud, el dispositivo de control asociado con la red puede determinar si permite o rechaza la solicitud del dispositivo solicitante para unirse a la red. En una implementación, el dispositivo de control puede determinar si permitir o rechazar la solicitud del dispositivo solicitante basándose en una condición del dispositivo solicitante. A modo de ejemplo y no de limitación, el dispositivo de control puede determinar si el dispositivo solicitante es un dispositivo aislado basándose en información incluida en la solicitud recibida. En una implementación, se puede determinar que el dispositivo solicitante está aislado si el dispositivo solicitante es incapaz de unirse a redes que no sean la red del dispositivo de control. De forma adicional, o como alternativa, se puede determinar que el dispositivo solicitante esté aislado si el dispositivo solicitante no detecta ninguna otra red que cubra el área en donde se encuentra el dispositivo solicitante. De forma adicional, o como alternativa, se puede determinar que el dispositivo solicitante está aislado si el dispositivo solicitante no detecta otras redes o se ve forzado a migrar de otra red a la red del dispositivo de control, y esta otra red y la red de control son las únicas redes que cubren el área en la que se encuentra el dispositivo solicitante. De forma adicional, o como alternativa, se puede determinar que el dispositivo solicitante está aislado si el dispositivo solicitante ha agotado (es decir, no ha podido unirse) sin éxito todas las redes detectadas en su área, excepto la red del dispositivo de control. De forma adicional, o como alternativa, se puede determinar que el dispositivo solicitante está aislado si la red del dispositivo de control es la única red que puede proporcionar conectividad entre el dispositivo solicitante y servidores tales como servidores de Autenticación, Autorización y/o Contabilidad (AAA) asociados con la red.

De forma adicional, o como alternativa, el dispositivo de control puede determinar si permite o rechaza la solicitud del dispositivo solicitante de unirse a la red basándose en una condición de la red. Por ejemplo, el dispositivo de control puede determinar si una carga en la red, tal como un número actual de dispositivos, un tráfico actual, una tasa de caída de paquetes actual o promedio, un uso de ancho de banda actual o promedio, etc. en la red es mayor o igual a un umbral predeterminado. De forma adicional, o como alternativa, el dispositivo de control puede almacenar o recuperar estadísticas de carga o red (como la tasa de caída de paquetes actual o promedio, uso de ancho de banda actual o promedio, etc.) acerca de la red y determinar si la carga o estadísticas de la red (por ejemplo, el uso de ancho de banda actual) es mayor o igual a un umbral predeterminado.

Basándose en la determinación, el dispositivo de control puede permitir o rechazar la solicitud del dispositivo solicitante. Por ejemplo, en respuesta a determinar que el dispositivo solicitante es un dispositivo aislado, el dispositivo de control puede permitir que la solicitud del dispositivo solicitante se una a la red. Si el dispositivo de control determina adicionalmente que la carga (o las estadísticas) en la red, por ejemplo, el uso de ancho de banda actual es o son mayores o iguales que el umbral o umbrales respectivos, el dispositivo de control puede forzar que uno o más dispositivos en la red abandonen la red o migren de la red a otra red. A modo de ejemplo y sin limitación, el dispositivo de control puede seleccionar uno o más dispositivos basándose en el conocimiento de qué dispositivos en la red son capaces de migrar o unirse a otra red, y puede forzar o solicitar que uno o más dispositivos abandonen la red del dispositivo de control. De esta forma, el dispositivo de control puede reducir la carga a un nivel suficiente o predeterminado para permitir que el dispositivo aislado solicitante se una a la red.

En respuesta a la determinación de permitir que la solicitud del dispositivo solicitante se una a la red (independientemente de la condición de la red), el dispositivo de control puede preparar adicionalmente información relacionada con la unión a la red para el dispositivo solicitante. La información puede incluir, pero no se limita a, una clave de grupo asociada con la red, información de configuración para el dispositivo solicitante para establecerse con

la red y/o una nueva dirección (como una dirección IP) asignada al dispositivo solicitante, etc. El dispositivo de control puede enviar la información al dispositivo solicitante a través del dispositivo vecino.

Los métodos descritos permiten que el dispositivo solicitante que desea unirse a la red realice una única toma de contacto con la red para unirse a la red. En algunas implementaciones, el dispositivo vecino, que está ubicado en una proximidad del dispositivo solicitante y está a un salto del dispositivo solicitante, puede retransmitir la solicitud al dispositivo de control en nombre del dispositivo solicitante, salvando de este modo al dispositivo solicitante de enviar, de forma aleatoria o sin meta alguna, la solicitud a la red. Los métodos descritos permiten adicionalmente una migración fluida de un dispositivo existente en la red a otra red, evitando de este modo que la red sobrecargue, sature o agote los recursos de la red. Además, el dispositivo de control puede almacenar o recuperar otras estadísticas tales como porcentaje de uso de ancho de banda, porcentaje de dispositivos aislados entre todos los dispositivos, etc., que están asociados con la red y enviar un aviso o alerta a un administrador de anuncios si uno o más de estas otras estadísticas alcanzan el umbral o umbrales predeterminados respectivos. Esto facilita que el administrador decida si añadir nuevo hardware de soporte para mejorar el ancho de banda de la red y/o redisponer o reubicar físicamente algunos de los dispositivos en la red.

En los ejemplos descritos en el presente documento, el dispositivo de control recibe la solicitud, determina si permite o rechaza la solicitud, determina si fuerza, o no, que uno o más dispositivos de la red abandonen la red y prepara información relacionada para habilitar el dispositivo solicitante para unirse a la red. Sin embargo, en otras implementaciones, otros uno o más dispositivos o servicios pueden realizar algunas o todas estas funciones. Por ejemplo, el dispositivo de control puede enviar o radiodifundir información de la condición de la red a una parte o a la totalidad de los dispositivos en la red regularmente o según sea necesario. El dispositivo de control puede indicar en la información enviada o transmitida que la red no aceptará la publicidad de nuevos dispositivos, excepto dispositivos aislados. En consecuencia, en una implementación, un dispositivo (por ejemplo, el dispositivo vecino) o el servicio puede determinar si permitir o rechazar la solicitud del dispositivo solicitante para unirse a la red, mientras que otro dispositivo o servicio puede determinar si forzar que uno o más dispositivos en la red abandonen la red, y otro dispositivo o servicio más puede preparar información relacionada con la habilitación del dispositivo solicitante para que se una a la red.

La aplicación describe múltiples y variadas implementaciones e implementaciones. La siguiente sección describe un entorno ilustrativo que es adecuado para poner en práctica diversas implementaciones. A continuación, la aplicación describe ejemplos de sistemas, dispositivos y procesos para implementar el registro del dispositivo y la migración de dispositivo.

Entorno ilustrativo

La figura 1 es un diagrama esquemático de una arquitectura 100 ilustrativa utilizable para implementar el registro del dispositivo y la migración de dispositivo. La arquitectura 100 incluye una pluralidad de nodos o dispositivos 102-1, 102-2, 102-3, 102-4, 102-5, … , 102-N (denominados, de forma colectiva, dispositivos 102) acoplados comunicativamente entre sí a través de trayectorias de comunicación directa o "enlaces". En este ejemplo, N representa una cantidad de dispositivos dispuestos en un área de encaminamiento autónomo (ARA), tal como una red de área extensa (WAN), red de área metropolitana (MAN), red de área local (LAN), red de área vecina (NAN), red de área personal (PAN), o similares. Aunque en la figura 1 solo se muestra un ARA, en la práctica, pueden existir múltiples ARA y pueden definir, de forma colectiva, una red más grande, tal como una red de infraestructura de medición avanzada (AMI). En cualquier momento dado, cada dispositivo individual puede ser miembro de un ARA particular. Con el paso del tiempo, sin embargo, los dispositivos pueden migrar de un ARA a otra ARA geográficamente próxima o superpuesta basándose en una diversidad de factores, tales como cargas respectivas en las ARA, interferencia o similares.

Como se analizó anteriormente, el término "enlace" se refiere a una trayectoria de comunicación directa entre dos dispositivos (sin pasar a través de o ser propagada por otro dispositivo). El enlace puede ser a través de una trayectoria de comunicación cableada o inalámbrica. Cada enlace puede representar una pluralidad de canales a través de los cuales un dispositivo puede transmitir o recibir datos. Cada uno de la pluralidad de canales se puede definir mediante un intervalo de frecuencia que es igual o diferente para cada uno de la pluralidad de canales. En algunos casos, la pluralidad de canales comprende canales de radiofrecuencia (RF). La pluralidad de canales puede comprender un canal de control y múltiples canales de datos. En algunos casos, el canal de control se utiliza para comunicar uno o más mensajes entre dispositivos para especificar uno de los canales de datos que se utilizarán para transferir datos. En general, las transmisiones en el canal de control son más cortas en relación con las transmisiones en los canales de datos.

En una implementación, algunos o todos los dispositivos 102 pueden implementarse como cualquiera de una diversidad de dispositivos tales como, por ejemplo, contadores de servicio público inteligentes (por ejemplo, contadores de electricidad, gas y/o agua), sensores (por ejemplo, sensores de temperatura), estaciones meteorológicas, sensores de frecuencia, etc.), dispositivos de control, transformadores, encaminadores, servidores, relés (por ejemplo, relés celulares), interruptores, válvulas, combinaciones de los anteriores, o cualquier dispositivo acoplable a una red de comunicación y capaz de enviar y/o recibir datos.

De forma adicional, o como alternativa, en algunas implementaciones, algunos o todos los dispositivos 102 pueden implementarse como cualquiera de una diversidad de dispositivos informáticos convencionales que incluyen, por ejemplo, un portátil u ordenador portátil, un dispositivo de mano, un equipo ultraportátil, un dispositivo de Internet, un dispositivo de lectura portátil, un dispositivo lector de libros electrónicos, una tableta o un ordenador de tipo pizarra, una consola de juegos, un dispositivo móvil (por ejemplo, un teléfono móvil, un asistente digital personal, un teléfono inteligente, etc.), un reproductor de medios, etc. o una combinación de los mismos.

En este ejemplo, los dispositivos 102 se pueden configurar adicionalmente para comunicarse con una oficina central 104 a través de un dispositivo de borde (por ejemplo, el dispositivo 102-4) que sirve como punto de conexión del ARA a una red o redes de retroceso 106, tales como Internet. En una implementación, el dispositivo de borde puede incluir, pero no se limita a, un repetidor celular, un encaminador celular, un encaminador de borde, una raíz DODAG (Grafo acíclico dirigido orientado a destino), un nodo o dispositivo raíz de la red ARA, etc. En este ejemplo ilustrado, el dispositivo 102-1 sirve como un dispositivo de retransmisión y/o reenvío celular para otros nodos en el ARA, por ejemplo, retransmitiendo comunicaciones desde los otros dispositivos 102-2 - 102-N del ARA desde y hacia la oficina central 104 a través de la red o redes 106.

En una implementación, algunos o todos los dispositivos 102 pueden incluir una unidad de procesamiento 108. La unidad de procesamiento 108 puede incluir uno o más procesador(es) 110 acoplados de forma comunicativa a la memoria 112. La memoria 112 se puede configurar para almacenar uno o más módulos de software y/o firmware, que son ejecutables en el procesador o procesadores 110 para implementar diversas funciones. Si bien los módulos se describen en el presente documento como software y/o firmware almacenados en memoria y ejecutables en un procesador, en otras implementaciones, cualquiera o todos los módulos pueden implementarse total o parcialmente por hardware (por ejemplo, como un ASIC, una unidad de procesamiento especializado, etc.) para ejecutar las funciones descritas.

La memoria 112 puede comprender medios legibles por ordenador y puede tomar la forma de memoria volátil, tal como memoria de acceso aleatorio (RAM) y/o memoria no volátil, tal como memoria de solo lectura (ROM) o RAM flash. Los medios legibles por computadora incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier método o tecnología para el almacenamiento de información, tal como instrucciones legibles por computadora, estructuras de datos, módulos de programa u otros datos para su ejecución por uno o más procesadores de un dispositivo informático. Los ejemplos de medios legibles por ordenador incluyen, pero no se limitan a, memoria de cambio de fase (PRAM), memoria de acceso aleatorio estática (SRAM), memoria de acceso aleatorio dinámica (DRAM), otros tipos de memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de solo lectura programable borrable eléctricamente (EEPROM), memoria flash u otra tecnología de memoria, disco compacto - memoria de solo lectura (CD-ROM), discos versátiles digitales (DVD) u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio de no transmisión que pueda usarse para almacenar información para el acceso de un dispositivo informático. Como se define en el presente documento, los medios legibles por ordenador no incluyen medios de comunicación, tales como señales de datos modulados y ondas portadoras.

En una implementación, algunos o todos los dispositivos 102 pueden incluir adicionalmente una radio 114. La radio 114 comprende un transceptor de radiofrecuencia (RF) configurado para transmitir y/o recibir señales de RF a través de uno o más de una pluralidad de canales/frecuencias. En algunas implementaciones, algunos o todos los dispositivos 102 incluyen una única radio 114 configurada para enviar y recibir datos en múltiples canales diferentes, tales como el canal de control y múltiples canales de datos de cada enlace de comunicación. La radio 114 se puede configurar adicionalmente para implementar una pluralidad de diferentes técnicas de modulación, velocidades de datos, protocolos, intensidades de señal y/o niveles de potencia. La arquitectura 100 puede representar una red heterogénea de dispositivos, en la que los dispositivos 102 pueden incluir diferentes tipos de dispositivos (por ejemplo, contadores inteligentes, relés celulares, sensores, etc.), diferentes generaciones o modelos de dispositivos y/o dispositivos que de otro modo son capaces de transmitir en diferentes canales y usar diferentes técnicas de modulación, velocidades de datos, protocolos, intensidades de señal y/o niveles de potencia.

De forma adicional, o como alternativa, en algunas implementaciones, algunos o todos los dispositivos 102 pueden incluir una interfaz de red 116, y/o una interfaz de entrada/salida 118. La unidad de procesamiento 108 se puede configurar adicionalmente para recibir y actuar sobre datos desde la interfaz 116 de red, recibidos de la interfaz de entrada/salida 118, y/o almacenados en la memoria 112.

La red o redes 106, mientras tanto, representan una red de retroceso, que puede comprender una red inalámbrica o cableada, o una combinación de las mismas. La red o redes 106 pueden ser una colección de redes individuales interconectadas entre sí y que funcionan como una única red grande (por ejemplo, Internet o una intranet). Además, las redes individuales pueden ser redes inalámbricas o cableadas, o una combinación de las mismas.

La oficina central 104 se puede implementar mediante uno o más dispositivos informáticos, tales como servidores, ordenadores personales, ordenadores portátiles, encaminadores, conmutadores, etc. El uno o más dispositivos informáticos pueden estar equipados con uno o más procesador(es) acoplados de forma comunicativa a la memoria. En algunos ejemplos, la oficina central 104 incluye un sistema centralizado de gestión de datos de contador que realiza

el procesamiento, análisis, almacenamiento y/o gestión de datos recibidos desde uno o más de los dispositivos 102. Por ejemplo, la oficina central 104 puede procesar, analizar, almacenar y/o gestionar datos obtenidos a partir de un contador de servicio público inteligente, sensor, dispositivo de control, encaminador, regulador, servidor, relé, interruptor, válvula y/u otros dispositivos inteligentes. De forma adicional, o como alternativa, la oficina central 104 puede incluir un sistema de gestión de red (NMS) para mantener un registro de dispositivos de la red AMI, ajustes de configuración del dispositivo, información de versión y similares. Aunque el ejemplo de la figura 1 ilustra la oficina central 104 en una única ubicación, en algunos ejemplos la oficina central puede distribuirse entre múltiples ubicaciones y/o se puede eliminar por completo (por ejemplo, en el caso de una plataforma informática distribuida altamente descentralizada).

En una implementación, la arquitectura puede incluir adicionalmente un servidor de autenticación 120 responsable de autenticar identidades de los dispositivos 102 en la red ARA. En algunas implementaciones, la arquitectura 100 puede incluir adicionalmente otros servidores 122, que pueden controlar o soportar la admisión de nuevos dispositivos a la red ARA. En una implementación, los otros servidores 122 pueden incluir un servidor de seguridad responsable de mantener y/o proporcionar servicios de seguridad a la red ARA.

Dispositivo ilustrativo

La figura 2 es un diagrama esquemático que muestra detalles adicionales del dispositivo 102 (por ejemplo, un dispositivo 102-2 representativo) de la figura 1. En este ejemplo, la radio 114 incluye una antena 200 acoplada a un extremo frontal de RF 202 y un procesador de banda base 204. El extremo frontal de RF 202 puede proporcionar funciones de transmisión y/o de recepción. El extremo frontal de RF 202 puede incluir componentes analógicos y/o de hardware de alta frecuencia que proporcionan funcionalidad, tales como sintonización y/o atenuación de señales proporcionadas por la antena y obtenidas a partir de uno o más de los dispositivos 102. El extremo frontal de RF 202 puede proporcionar una señal al procesador de banda base 204.

En un ejemplo, la totalidad o parte del procesador de banda base 204 se puede configurar como una radio definida por software (SW). En un ejemplo, el procesador de banda base 204 proporciona funcionalidad de selección de frecuencia y/o de canal a la radio 114. Por ejemplo, la radio definida por SW puede incluir mezcladores, filtros, amplificadores, moduladores y/o desmoduladores, detectores, etc., implementados en software ejecutado por un procesador o circuito integrado específico de aplicación (ASIC) u otro dispositivo o dispositivos informáticos integrados. La radio definida por SW puede utilizar un procesador o procesadores 110 y software definido o almacenado en la memoria 112. Como alternativa, la radio 114 se puede implementar, al menos en parte, usando componentes analógicos.

La unidad de procesamiento 108 puede incluir adicionalmente un reloj 206 configurado para mantener un tiempo. El reloj 206 se puede configurar adicionalmente para proporcionar uno o más temporizadores de cuenta hacia delante o de cuenta atrás. Tales temporizadores pueden usarse en salto de frecuencia entre múltiples canales de comunicación.

Un módulo de salto de frecuencia 208 se puede configurar para comunicarse con el procesador de banda base 204 y el reloj 206. En un ejemplo, el módulo de salto de frecuencia 208 está configurado para obtener información de tiempo y/o establecer temporizadores de salto de frecuencia en el reloj 206. Tal información de tiempo y/o temporizadores indicará al módulo de salto de frecuencia 208 cuándo "saltar" o sintonizar un canal o frecuencia diferente. Adicionalmente, el módulo de salto de frecuencia 208 se puede configurar para dirigir la radio definida por SW u otro componente de la radio 114 para realizar los cambios de frecuencia reales. En consecuencia, el módulo de salto de frecuencia 208 puede ser capaz de cambiar repetidamente entre frecuencias acordadas, en momentos acordados y de comunicarse con otro dispositivo o dispositivos durante períodos de tiempo acordados y en protocolos acordados.

En algunas implementaciones (por ejemplo, cuando el dispositivo es un contador de servicio público), la memoria 112 también puede incluir un módulo de metrología 210 configurado para recopilar datos de consumo de uno o más recursos (por ejemplo, electricidad, agua, gas natural, etc.), que entonces puede transmitirse a uno o más dispositivos 102 para su propagación, con el tiempo, a la oficina central 104 u otro destino.

De forma adicional, o como alternativa, el dispositivo 102 puede incluir un módulo de descubrimiento 212, un módulo de radiodifusión 214, un módulo de envío 216, un módulo de cifrado/descifrado 218, un módulo de recepción 220, un módulo de análisis 222, un módulo de retransmisión 224, un módulo de control 226, un módulo de autenticación 228 y/o un módulo de asignación de direcciones 230, dependiendo de un papel o funcionalidad del dispositivo 102 en la red ARA. Los detalles de las funciones de estos módulos se describen a continuación.

Registro de dispositivo ilustrativo

En una implementación, antes de registrarse con el NMS en la oficina central 104 y/o convertirse en un miembro de la red ARA, un dispositivo 102 (por ejemplo, el dispositivo 102-3) se puede acoplar, en primer lugar, a la red ARA. A modo de ejemplo y sin limitación, el dispositivo solicitante 102-3 se puede acoplar, en primer lugar, a la red ARA hasta un punto en que el dispositivo solicitante 102-3 puede enviar una solicitud de unión a la red ARA, por ejemplo, en un nivel o capa de IP. Por ejemplo, el dispositivo solicitante 102-3 se puede acoplar, en primer lugar, a la red ARA en el

nivel MAC (es decir, control de acceso al medio) o capa MAC. En una implementación, el dispositivo solicitante 102-3 puede corresponder a un dispositivo, tal como un contador de servicio público inteligente, recientemente implementado en un área que incluye la red ARA. Como alternativa, el dispositivo solicitante 102-3 puede corresponder a un dispositivo que está intentando migrar a la red ARA desde otra red ARA como se muestra en la figura 1.

En una implementación, el módulo de descubrimiento 212 del dispositivo solicitante 102-3 puede descubrir, de forma activa o pasiva, uno o más dispositivos vecinos 102 (por ejemplo, el dispositivo 102-2) en una proximidad del mismo. Un dispositivo vecino del dispositivo solicitante 102-3 puede incluir, por ejemplo, un dispositivo que está comunicativamente a un salto del dispositivo solicitante 102-3. Es decir, un dispositivo vecino es un dispositivo con el que el dispositivo solicitante puede comunicarse directamente a través de un enlace de comunicación. En una implementación, el dispositivo solicitante 102-3 puede realizar un servicio de descubrimiento vecino en una capa MAC. De forma adicional, o como alternativa, el módulo de descubrimiento 212 puede descubrir el uno o más dispositivos vecinos en la proximidad del mismo a través del examen de señales detectadas o recibidas a una frecuencia o intervalo de frecuencias predeterminado designado para la red ARA a la que desea unirse el dispositivo solicitante 102-3.

De forma adicional, o como alternativa, en algunas implementaciones, el dispositivo solicitante 102-3 puede transmitir la solicitud para unirse a la red ARA usando el módulo de radiodifusión 214 con o sin, en primer lugar, conocer o descubrir dispositivo alguno en la proximidad del mismo, en un intento de que uno o más dispositivos que están dentro de su proximidad puedan recibir la solicitud, y puedan procesar la solicitud en nombre del dispositivo solicitante 102-3, y/o establecer una conexión con el dispositivo solicitante 102-3.

De forma adicional, o como alternativa, en una implementación, el módulo de radiodifusión 214 puede transmitir una presencia del dispositivo solicitante 102-3, y esperar a que uno o más dispositivos en la red ARA que observen la presencia del dispositivo solicitante 102-3 se comuniquen con el dispositivo solicitante 102-3. En una implementación, el módulo de radiodifusión 214 puede transmitir la presencia del dispositivo solicitante 102-3 usando un código o mensaje predeterminado en una frecuencia o intervalo de frecuencia predeterminado.

Independientemente de si el dispositivo solicitante 102-3 descubre uno o más dispositivos vecinos 102 o el uno o más dispositivos vecinos 102 descubren el dispositivo solicitante 102-3, el dispositivo solicitante 102-3 puede seleccionar un dispositivo vecino 102 (por ejemplo, el dispositivo 102-2), y enviar una solicitud para unirse a la red ARA asociada con el dispositivo vecino 102-2 al dispositivo vecino 102-2. En una implementación, el dispositivo solicitante 102-3 puede enviar una solicitud del Protocolo de Configuración Dinámica de Anfitrión versión 6 (DHCPv6) o DHCPv4 al dispositivo vecino 102-2 a través del módulo de envío 216. Como alternativa, el dispositivo solicitante 102-3 puede incluir la solicitud de unión en un mensaje de baliza y enviar el mensaje de baliza al dispositivo vecino 102-2 a través del módulo de envío 216.

El dispositivo solicitante 102-3 puede, o no, conocer una dirección (por ejemplo, una dirección de Protocolo de Internet (IP)) de un dispositivo de control asociado con la red ARA que es responsable de controlar una admisión o adición de un nuevo dispositivo a la red ARA. El dispositivo de control en este ejemplo puede comprender el dispositivo de borde 102-4, un servidor de DHCP u otro dispositivo fuera del ARA. Específicamente, la solicitud de unión o el mensaje de baliza pueden incluir, o no, una dirección de destino del dispositivo de control asociado con la red ARA a la que necesita dirigirse, por último, la solicitud de unión del dispositivo solicitante 102-3.

En algunas implementaciones, el dispositivo solicitante 102-3 puede cifrar la totalidad o parte de la solicitud de unión o el mensaje de baliza mediante una clave de codificación usando el módulo de cifrado/descifrado 218. La clave de cifrado puede comprender una clave privada o una clave simétrica. En una implementación, cada uno de los dispositivos 102 (ya sea un dispositivo que sea miembro de la red ARA o un dispositivo que se pueda unir a la red ARA) puede compartir el mismo par de claves pública/privada o la misma clave simétrica durante o después de su fabricación. En algunas implementaciones, cada uno de los dispositivos 102 (ya sea un dispositivo que sea miembro de la red ARA o un dispositivo que se pueda unir a la red ARA) puede tener una clave de cifrado/descifrado o clave simétrica seleccionada de un conjunto predeterminado de claves de cifrado/descifrado accesibles por cada uno de los dispositivos 102. En una implementación, cada uno de los dispositivos 102 (ya sea un dispositivo que sea miembro de la red ARA o un dispositivo que se pueda unir a la red ARA) puede tener una clave de cifrado/descifrado o clave simétrica que solo se conoce a sí misma y uno o más dispositivos y/o servidores (tales como la oficina central 104, el servidor de autenticación 120, y/o el dispositivo de control de la red ARA, etc.). En otras implementaciones, el dispositivo solicitante 102 puede enviar la solicitud de combinación o el mensaje de baliza sin cifrado, es decir, en un formato simple.

De forma adicional, o como alternativa, en una implementación, la solicitud de unión puede incluir, pero no se limita a, un identificador del dispositivo solicitante 102-3 y/o información de autenticación, tal como una firma de autenticación, una semilla o un valor arbitrario que está firmado o cifrado usando una clave predeterminada (por ejemplo, la clave de cifrado anterior, clave simétrica o pública) que se ha registrado en el dispositivo solicitante 102-3 y conocida por la red ARA, el dispositivo de control de la red ARA, el NMS en la oficina central 104 y/o el servidor de autenticación 120. En algunas implementaciones, la solicitud de unión puede incluir adicionalmente un mensaje, un código u otro indicador que indique si el dispositivo solicitante 102-3 es un dispositivo aislado. A modo de ejemplo y no de limitación, se puede determinar que el dispositivo solicitante 102-3 está aislado si el dispositivo solicitante 102-3 es incapaz de unirse a

redes (no mostradas) que no sean la red ARA. De forma adicional, o como alternativa, se puede determinar que el dispositivo solicitante 102-3 está aislado si el dispositivo solicitante 102-3 no detecta otras redes que cubren un área en la que está situado el dispositivo solicitante 102-3. De forma adicional, o como alternativa, se puede determinar que el dispositivo solicitante 102-3 está aislado si el dispositivo solicitante 102-3 intenta migrar de otra red (como se muestra en la figura 1) a la red ARA y esta otra red y la red ARA son las únicas redes que cubren el área en la que se encuentra el dispositivo solicitante 102-3. De forma adicional, o como alternativa, se puede determinar que el dispositivo solicitante 102-3 está aislado si el dispositivo solicitante 102-3 ha agotado (es decir, ha intentado y no ha podido unirse) todas las redes detectadas en su área excepto la red ARA. De forma adicional, o como alternativa, el dispositivo solicitante 102-3 (es decir, no se ha podido unir) está aislado si la red ARA es la única red que puede proporcionar conectividad entre el dispositivo solicitante 102-3 y uno o más servidores tales como NMS y Servidores DHCP, por ejemplo.

En algunas implementaciones, tras enviar la solicitud de unión al dispositivo vecino 102-2, el dispositivo solicitante 102-3 espera una respuesta de la red ARA a través del dispositivo vecino 102-2. La respuesta puede indicar si la solicitud de unión del dispositivo solicitante 102-3 para unirse a la red ARA está permitida o rechazada. Si la respuesta indica que la solicitud de unión del dispositivo solicitante 102-3 es rechazada o denegada, el dispositivo solicitante 102-3 puede explorar otra red ARA y enviar una solicitud de unión a la otra red ARA que el dispositivo solicitante 102-3 puede encontrar.

En caso de que se permita la solicitud de unión, la respuesta puede incluir, por ejemplo, una clave de grupo asociada con la red ARA, información de configuración para que el dispositivo solicitante 102-3 se una a la red ARA, y/o una dirección (por ejemplo, una dirección de Protocolo de Internet (IP) que está asignada al dispositivo solicitante 102-3. De forma adicional, o como alternativa, en algunas implementaciones, la respuesta puede incluir información de dirección de uno o más dispositivos 102 dentro de la red ARA, incluyendo, por ejemplo, información de dirección de dispositivos a lo largo de una o más trayectorias designadas por el dispositivo controlador para encaminar paquetes de datos del dispositivo solicitante 102-3 dentro de la red ARA, y/o información de dirección del dispositivo de control asociado con la red ARA. En una implementación, parte o la totalidad de la respuesta (por ejemplo, la clave del grupo, etc.) se puede cifrar usando la clave simétrica del dispositivo solicitante 102-3. De forma adicional o alternativa, parte o la totalidad de la respuesta (como la información de dirección del dispositivo de control, por ejemplo) se puede cifrar usando la clave de grupo asociada a la red ARA.

En algunas implementaciones, el dispositivo solicitante 102-3 solo puede realizar una única toma de contacto o intercambio (es decir, un único mensaje de sentido ascendente para la solicitud de unión y un único mensaje de sentido descendente para responder a la solicitud de unión), usando el protocolo DHCPv6 o DHCPv4, por ejemplo, con la red ARA (por ejemplo, el dispositivo vecino 102-2 de la red ARA) para lograr unirse a la red ARA. En una implementación, el dispositivo solicitante 102-3 y/o la red ARA pueden lograr la autenticación mutua (es decir, la autenticación de una identidad del dispositivo solicitante 102-3 por la red ARA o el servidor de autenticación 120, y la autenticación de una identidad de la red ARA por el dispositivo solicitante 102-3) usando esta única toma de contacto o intercambio.

A modo de ejemplo y no de limitación, si la clave simétrica o asimétrica (por ejemplo, la clave pública/privada) del dispositivo solicitante 102-3 es conocida (o se supone que es conocida) solo para el dispositivo solicitante 102-3 y otros uno o más dispositivos y/o servidores (por ejemplo, el servidor de autenticación 120, la oficina central 104 y/o el dispositivo de control) que están asociados con la red ARA, el dispositivo solicitante 102-3 y la red ARA pueden autenticarse entre sí usando la clave simétrica o asimétrica del dispositivo solicitante 102-3. Por ejemplo, la red ARA puede autenticar una identidad del dispositivo solicitante 102-3 si el servidor de autenticación 120, por ejemplo, puede descifrar con éxito una semilla o una firma (que puede estar incluida en la solicitud de unión) que se ha cifrado usando la tecla simétrica o asimétrica (por ejemplo, la clave pública) del dispositivo solicitante 102-3. Además, el dispositivo solicitante 102-3 puede autenticar la red ARA si, por ejemplo, el dispositivo solicitante 102-3 puede descifrar satisfactoriamente una clave de grupo cifrada (u otra información tal como la semilla o firma enviada previamente o la firma incluida en la respuesta a la solicitud conjunta, por ejemplo) que se ha cifrado usando la clave simétrica o asimétrica (por ejemplo, la clave pública) del dispositivo solicitante 102-3. En algunas implementaciones, si se usa una clave de grupo cifrada como fuente de autentificación de la red ARA, el dispositivo solicitante 102-3 puede determinar adicionalmente una autenticidad de la red ARA si el dispositivo solicitante 102-3 puede comunicarse con éxito con otros dispositivos en la Red ARA usando la clave de grupo descifrada. En una implementación alternativa, el dispositivo solicitante 102-3 puede realizar una pluralidad de tomas de contacto o intercambios con la red ARA, posiblemente usando uno o más protocolos tales como protocolo TCP/IP y/u otros protocolos de Internet, para lograr unirse a la red ARA.

En una implementación, el dispositivo vecino 102-2 puede recibir la solicitud de unión enviada o transmitida desde el dispositivo solicitante 102-3 a través del módulo de recepción 220 del dispositivo vecino 102-2. Si se cifra la solicitud de unión o el mensaje de baliza, el dispositivo vecino 102-2 puede descifrar la solicitud de unión o el mensaje de baliza usando el módulo de cifrado/descifrado 218 del dispositivo vecino 102-2. El dispositivo vecino 102-2 puede analizar la solicitud de combinación (descifrada u originalmente en formato simple si no está cifrada) y determinar a través del módulo de análisis 222 que el dispositivo solicitante 102-3 está solicitando unirse a la red ARA.

En algunas implementaciones, en respuesta a determinar que el dispositivo solicitante 102 solicita unirse a la red ARA

del dispositivo vecino 102-2, el dispositivo vecino 102-2 puede retransmitir la solicitud de unión al dispositivo de control asociado con la red ARA (por ejemplo, el dispositivo 102-4). En una implementación, el dispositivo vecino 102-2 puede conocer una dirección (por ejemplo, una dirección IP) del dispositivo de control y puede retransmitir la solicitud de unión al dispositivo de control a través del módulo de retransmisión 224. A modo de ejemplo y sin limitación, el módulo de retransmisión 224 puede incluir un agente de retransmisión, por ejemplo, un agente de retransmisión DHCPv6, para retransmitir la solicitud de unión (DHCPv6) enviada desde el dispositivo solicitante 102-3 al dispositivo de control. Por ejemplo, el módulo de retransmisión 224 del dispositivo vecino 102-2 puede insertar la dirección IP del dispositivo de control como una dirección de destino de un paquete de datos que incluye la solicitud de unión del dispositivo solicitante 102-3 y retransmitir el paquete de datos al controlador dispositivo directa o indirectamente a través de un dispositivo primario del dispositivo vecino 102-2.

Como alternativa, si el dispositivo vecino 102-2 no conoce la dirección del dispositivo de control, el módulo de retransmisión 224 del dispositivo vecino 102-2 puede retransmitir el paquete de datos (que incluye la solicitud del dispositivo solicitante 102-3) al dispositivo primario del dispositivo vecino 102-2 en la red ARA, por ejemplo, insertando una dirección IP del dispositivo primario, y dirigiendo o permitiendo que el dispositivo primario del dispositivo vecino 102-2 retransmita la solicitud de unión del dispositivo solicitante 102-3 al dispositivo de control.

De forma adicional, o como alternativa, independientemente de si la solicitud de unión se retransmite al dispositivo de control o al dispositivo primario del dispositivo vecino 102-2, el dispositivo vecino 102-2 puede cifrar adicionalmente la solicitud retransmitida usando una clave de cifrado del dispositivo vecino 102-2. En una implementación, esta clave de cifrado puede incluir una clave de grupo asociada a la red ARA y distribuida a cada dispositivo 102 en la red ARA. En algunas implementaciones, esta clave de cifrado puede incluir una clave de cifrado seleccionada del conjunto de claves de cifrado/descifrado accesibles por cada dispositivo 102 de la red ARA y/o asignadas al dispositivo vecino 102-2. En algunas otras implementaciones, el dispositivo vecino 102-2 puede retransmitir la solicitud en un formato simple, es decir, sin cifrado. En una implementación, el dispositivo vecino 102-2 puede usar una dirección del mismo como dirección de origen de la solicitud (o reemplazar la dirección de origen de la solicitud de combinación del dispositivo solicitante 102-3 por la dirección del dispositivo vecino 102-2) que el dispositivo vecino 102-2 va a retransmitir en nombre del dispositivo solicitante 102-3. Esto permite reenviar adecuadamente una respuesta desde otros dispositivos o servidores asociados con la red ARA al dispositivo solicitante 102-3. Por ejemplo, una respuesta o contestación (por ejemplo, para la solicitud de unión) al dispositivo solicitante 102-3 puede usar la dirección del dispositivo vecino 102-2 como la dirección de destino, y solicitar al dispositivo vecino 102-2 que envíe o retransmita la respuesta o contestación al dispositivo solicitante 102-3 en consecuencia.

En algunas implementaciones, el dispositivo vecino 102-2 retransmite la solicitud de unión del dispositivo solicitante 102-3 independientemente de una condición de la red ARA y/o una condición del dispositivo solicitante 102-3. De forma adicional, o como alternativa, en algunas implementaciones, el dispositivo vecino 102-2 puede recibir una instrucción del dispositivo de control 102-4, lo que indica que la red ARA puede no aceptar la admisión de un nuevo dispositivo a la red ARA a menos que se agregue el nuevo dispositivo o unido a la red ARA es un dispositivo aislado. En este último caso, el módulo de análisis 222 del dispositivo vecino 102-2 puede determinar adicionalmente si el dispositivo solicitante 102-3 es un dispositivo aislado basándose, por ejemplo, en la solicitud de unión recibida por el módulo de recepción 220. En respuesta a determinar que el dispositivo solicitante 102-3 no es un dispositivo aislado, el dispositivo vecino 102-2 puede enviar una respuesta o retroalimentación al dispositivo solicitante 102-3 que indique que la solicitud de unirse a la red ARA se rechaza porque, por ejemplo, el dispositivo vecino 102-2 ha recibido previamente del dispositivo de control 102-4 una instrucción para rechazar la admisión de nuevos dispositivos excepto los dispositivos aislados.

En algunas implementaciones, en respuesta a la recepción de la solicitud retransmitida desde el dispositivo vecino 102-2, el dispositivo de control asociado con la red ARA puede determinar si permite o rechaza la solicitud de unión del dispositivo solicitante 102-3 basándose en una condición de la Red ARA. El dispositivo de control puede determinar si permite o rechaza la solicitud de unión del dispositivo solicitante 102-3 usando el módulo de control 226. En una implementación, el dispositivo de control puede desempeñar un papel de autoridad de control de admisión. En una implementación, el dispositivo de control puede comprender un dispositivo raíz o de borde (por ejemplo, el dispositivo 102-4) de la red ARA, un encaminador de la red ARA, o puede estar distribuido en uno o más nodos de las redes ARA. En algunas implementaciones, el dispositivo de control puede estar situado, como alternativa, en un dispositivo de extremo posterior tal como la oficina central 104, una raíz de un árbol de encaminamiento de una o más redes ARA manejable por la oficina central 104, u otro servidor 122 que puede estar afiliado a la oficina central 104. En algunas implementaciones, el dispositivo de control puede incluir un servidor de DHCP o DHCPv6, que puede estar incluido en uno o más de los otros servidores 122. En una implementación, en el caso de que el dispositivo de control no incluya un servidor de DHCP o DHCPv6, o incluya una o más funciones del servidor de DHCP o DHCPv6, el dispositivo controlador puede retransmitir la solicitud de unión al servidor de DHCP o DHCPv6. En algunas implementaciones, el dispositivo de control puede incluir una combinación de uno o más dispositivos que incluyen el servidor de DHCP o DHCPv6, un dispositivo raíz, un dispositivo de borde, un encaminador, un dispositivo de extremo posterior tal como la oficina central 104 u otro servidor 122. Para facilitar la referencia en esta aplicación, se hará referencia al dispositivo 102-4 como el dispositivo de control. El dispositivo 102-4 es representativo de un nodo raíz, encaminador de borde u otro dispositivo de borde de la red ARA, que acopla la red ARA a la oficina central 104 a través de la red de retroceso 106.

En algunas implementaciones, en respuesta a la recepción de la solicitud retransmitida desde el dispositivo vecino 102-2, el dispositivo de control 102-4 puede determinar si permite o rechaza la solicitud del dispositivo solicitante 102-3 basándose en si una carga en la red ARA excede un umbral predeterminado. A modo de ejemplo y sin limitación, el dispositivo de control 102-4 puede determinar si permite o rechaza la solicitud del dispositivo solicitante 102-3 basándose en si la red ARA está sobrecargada (por ejemplo, si el número actual de dispositivos en la red ARA es mayor o igual a un umbral predeterminado para dar cabida). De forma adicional, o como alternativa, el dispositivo de control 102-4 puede determinar si permite o rechaza la solicitud del dispositivo solicitante 102-3 basándose en si las estadísticas (como un uso de ancho de banda actual/promedio, una tasa de colisión actual/promedio, una tasa de caída actual/promedio de paquetes de datos, un tráfico de datos actual/promedio, etc.) de la red ARA es mayor o igual a un umbral predeterminado para las estadísticas.

En una implementación, en respuesta a determinar que la carga en la red ARA excede el umbral predeterminado (por ejemplo, la estadística es mayor o igual que el umbral predeterminado para las estadísticas), el dispositivo de control 102-4 puede rechazar la (DHCP o DHCPv6) solicitud de unión del dispositivo solicitante 102-3. Como alternativa, en algunas implementaciones, el dispositivo de control 102-4 puede determinar adicionalmente si el dispositivo solicitante 102-4 es un dispositivo aislado basándose, por ejemplo, en información en la solicitud recibida. La información en la solicitud recibida puede incluir, por ejemplo, un indicador que indique que el dispositivo solicitante 102-3 es un dispositivo aislado. En respuesta a determinar que el dispositivo solicitante 102-3 es un dispositivo aislado, el dispositivo de control 102-4 puede permitir que el dispositivo solicitante 102-3 se una a la red ARA independientemente de la condición de la red ARA (es decir, independientemente de si la carga en la red ARA excede el umbral predeterminado).

En algunas implementaciones, el dispositivo de control 102-4 puede determinar adicionalmente una autenticidad del dispositivo solicitante 102-3 usando el módulo de autenticación 228. Por ejemplo, el módulo de autenticación 228 del dispositivo de control 102-4 puede determinar una autenticidad del dispositivo solicitante 102-3 basándose en el identificador del dispositivo solicitante 102-3 o la firma de autenticación incluida en la solicitud recibida. De forma adicional, o como alternativa, el dispositivo de control 102-4 puede analizar la solicitud y enviar el identificador y/o la firma de autenticación del dispositivo solicitante 102-3 a un servidor de autenticación tal como un servidor de seguridad o servidor de Autenticación, Autorización y Contabilidad (AAA) 120. El servidor de seguridad o el servidor de AAA 120 es responsable de autenticar las identidades de los dispositivos que unen una o más redes ARA (incluida la red ARA actual) que son administradas por la oficina central 104, por ejemplo. En una implementación, el servidor de seguridad o el servidor de AAA 120 pueden estar ubicados fuera de la red ARA. En algunas implementaciones, el servidor de seguridad o el servidor de AAA 120 puede ser otro nodo o dispositivo (por ejemplo, el dispositivo 102-1) dentro de la misma red ARA del dispositivo de control 102-4. El dispositivo de control 102-4 puede enviar información que incluye el identificador y/o la firma de autenticación del dispositivo solicitante 102-3 al servidor de seguridad o al servidor de AAA 120 usando un protocolo de red como RADIUS (es decir, servicio de usuario de marcado de autenticación remota), por ejemplo. Para facilitar la referencia en esta aplicación, el servidor de AAA se usa como ejemplo para describir operaciones de autenticación de identidades de dispositivos que unen una o más redes ARA.

En una implementación, tras autenticar con éxito la identidad del dispositivo solicitante 102-3 basándose en el identificador y/o la firma de autenticación del dispositivo solicitante 102-3, por ejemplo, el servidor de AAA 120 puede enviar un mensaje al dispositivo de control 102-4 o el servidor de DHCP asociado o conectado con el dispositivo de control 102-4, que indica que la identidad del dispositivo solicitante 102-3 se ha autenticado satisfactoriamente. De forma adicional, o como alternativa, en algunas implementaciones, el servidor de AAA 120 puede enviar adicionalmente una clave de grupo (por ejemplo, una clave de capa de enlace de grupo) asociada con la red ARA al dispositivo de control 102-4 o el servidor de DHCP del dispositivo de control 102-4. De forma adicional, o como alternativa, el servidor de AAA 120 puede enviar el mensaje firmado o cifrado por la clave de grupo (por ejemplo, una clave de capa de enlace de grupo) asociada con la red ARA al dispositivo de control 102-4 o el servidor de DHCP asociado con el dispositivo de control 102-4. En una implementación, el dispositivo de control 102-4 puede haber almacenado previamente la clave de grupo asociada con la red ARA, y por lo tanto puede descifrar el mensaje cifrado usando la clave de grupo. En una implementación, el dispositivo de control 102-4 puede no tener información de la clave pública o simétrica del dispositivo solicitante 102-3. En ese caso, el servidor de AAA 120 puede cifrar la clave de grupo usando una clave pública o simétrica del dispositivo solicitante 102-3, y cifrar el mensaje (incluyendo la clave de grupo cifrada) usando la clave de grupo asociada con la red ARA al dispositivo de control 102-4, que puede reenviar la clave de grupo que se ha cifrado usando la clave pública o simétrica del dispositivo solicitante 102-3 al dispositivo solicitante 102-3.

En una implementación, si el dispositivo de control 102-4 y el servidor de DHCP son dispositivos separados, el servidor de AAA 120 puede enviar el mensaje al servidor de DHCP asociado con el dispositivo de control 120-4 (por ejemplo, después de que se haya enviado la solicitud de autenticación desde el servidor de DHCP o desde el dispositivo de control 102-4 a través del servidor de DHCP). En respuesta a la recepción del mensaje, el servidor de DHCP puede analizar el mensaje y determinar si la identidad del dispositivo solicitante 102-3 está autenticada. De forma adicional, o como alternativa, el servidor de DHCP puede retransmitir el mensaje al dispositivo de control 102-4. En algunas implementaciones, el servidor de AAA 120 puede enviar el mensaje al dispositivo de control 102-4 directamente si la solicitud de autenticación fue enviada desde el dispositivo de control 102-4 (o desde el dispositivo de control 102-4 a

través del servidor de DHCP si el dispositivo de control 102-4 y el servidor de DHCP son dispositivos separados). Independientemente de si el mensaje se retransmite desde el servidor de DHCP o se envía directamente desde el servidor de AAA 120, en una implementación, en respuesta a la recepción del mensaje del servidor de AAA 120, el dispositivo de control 102-4 puede analizar el mensaje y determinar si la identidad del dispositivo solicitante 102-3 está autenticada. En respuesta a la determinación de que la identidad del dispositivo solicitante 102-3 está autenticada, el dispositivo de control 102-4 puede enviar un mensaje, que se puede cifrar, o no, usando una clave pública o clave simétrica del dispositivo solicitante 102-3 (que puede depender de si el dispositivo de control 102-4 tiene la clave pública o simétrica del dispositivo solicitante 102-3, por ejemplo) como se describe en las implementaciones anteriores, al dispositivo solicitante 102-3 que indica que la identidad del dispositivo solicitante 102-3 está autenticada y/o que se permite al dispositivo solicitante 102-3 unirse a la red ARA. De forma adicional, o como alternativa, en algunas implementaciones, el dispositivo de control 102-4 puede cifrar el mensaje usando la clave de grupo asociada con la red ARA, que posteriormente puede ser descifrada y analizada por el dispositivo vecino 102-2 al dispositivo solicitante 102-3. En una implementación, el mensaje puede incluir adicionalmente, por ejemplo, una clave de grupo asociada con la red ARA y otra información que se puede cifrar, o no, usando la clave pública o simétrica del dispositivo solicitante 102-3, tal como la clave de grupo cifrada recibida del servidor de AAA 120, por ejemplo. En algunas implementaciones, en respuesta a la recepción del mensaje, el dispositivo solicitante 102-3 puede descifrar el mensaje si está cifrado (por ejemplo, usando la clave pública o simétrica del dispositivo solicitante 102-3) y recuperar la clave de grupo asociada con la red ARA. De forma adicional, o como alternativa, el dispositivo solicitante 102-3 puede descifrar la clave de grupo cifrada (tal como la clave de grupo cifrada en el servidor de AAA 120 usando la clave pública o simétrica del dispositivo solicitante 102-3) para recuperar la clave de grupo. El dispositivo solicitante 102-3 puede entonces enviar y/o recibir datos (por ejemplo, datos cifrados usando la clave de grupo, etc.) con otros dispositivos de la red ARA.

En algunas implementaciones, el dispositivo de control 102-4 (o el servidor de DHCP asociado con el dispositivo de control 102-4) puede enviar adicionalmente una solicitud de registro al NMS usando el módulo de envío 216. La solicitud de registro puede incluir, por ejemplo, el identificador del dispositivo solicitante 102-3, que puede estar firmado o cifrado usando una clave privada (de claves públicas/privadas) asociada con el dispositivo de control 102-4, la clave de grupo asociada con la red ARA, y/o la clave asociada con el dispositivo solicitante 102-3. En una implementación, el dispositivo de control 102-4 puede enviar la solicitud de registro al NMS en un formato simple, no cifrado.

Tras recibir la solicitud de registro del dispositivo de control 102-4, el NMS puede descifrar el mensaje si el mensaje está cifrado, analizar el mensaje y obtener el identificador del dispositivo solicitante 102-3. En algunas implementaciones, el NMS puede recuperar adicionalmente información asociada con el dispositivo solicitante 102-3 y/o información asociada con la red ARA. En una implementación, el NMS puede determinar información de configuración o parámetros utilizables para que el dispositivo solicitante 102-3 se una o configure con la red ARA basándose en la información recuperada. La información recuperada puede incluir, pero no se limita a, un tipo de modelo o tipo de dispositivo del dispositivo solicitante 102-3, un tipo de red ARA al que el dispositivo solicitante 102-3 solicita unirse, etc. De forma adicional, o como alternativa, el NMS puede enviar la información de configuración o parámetros al dispositivo de control 102-4 o al servidor de DHCP del dispositivo de control 102-4.

En una implementación, en respuesta a la recepción de la información de configuración o parámetros del NMS, el módulo de asignación de direcciones 230 del dispositivo de control 102-4 (o el servidor de DHCP) puede determinar una nueva dirección (por ejemplo, una nueva dirección IP tal como dirección IPv6) para el dispositivo solicitante 102-3. En una implementación, el dispositivo de control 102-4 (o el servidor de DHCP) puede determinar la nueva dirección basándose en un prefijo asignado a un agente de retransmisión que el dispositivo de control 102-4 (o el servidor de DHCP) puede emplear, por ejemplo. De forma adicional, o como alternativa, el dispositivo de control 102-4 (o el servidor de DHCP) puede determinar la nueva dirección basándose en un prefijo designado o compartido por dispositivos en la red ARA del dispositivo de control 102-4. En una implementación, la nueva dirección que está asignada al dispositivo solicitante 102-3 puede incluir el prefijo que está asignado al agente de retransmisión del dispositivo de control 102-4 (o el servidor de DHCP), o designado o compartido por cada dispositivo en la red ARA. En algunas implementaciones, el dispositivo de control 102-4 (o el servidor de DHCP) puede generar adicionalmente un número aleatorio y usar este número aleatorio para el resto de la nueva dirección. De forma adicional, o como alternativa, el dispositivo de control 102-4 (o el servidor de DHCP) puede haber reservado y almacenado previamente una pluralidad de direcciones (por ejemplo, direcciones de IPv6) que se usarán para los dispositivos que se suman a la red de ARA. El dispositivo de control 102-4 (o el servidor de DHCP) puede entonces seleccionar aleatoria o secuencialmente una dirección de la pluralidad de direcciones para asignar al dispositivo solicitante 102-3.

De forma adicional, o como alternativa, en algunas implementaciones, tras determinar la nueva dirección a asignar al dispositivo solicitante 102-3, el dispositivo de control 102-4 (o el servidor de DHCP) puede verificar adicionalmente esta nueva dirección con un servidor de DNS (es decir, Sistema de Nombres de Dominio) para determinar si esta nueva dirección está actualmente asignada a cualquier otro dispositivo. En una implementación, el dispositivo de control 102-4 (o el servidor de DHCP) puede enviar la nueva dirección y el identificador del dispositivo solicitante 102-3 al servidor de DNS. Si el dispositivo de control 102-4 (o el servidor de DHCP) recibe una respuesta del servidor de DNS, que indica que la nueva dirección está actualmente asignada a otro dispositivo, el dispositivo de control puede volver a determinar otra nueva dirección para el dispositivo solicitante 102-3 y verificar la nueva dirección redeterminada con el servidor de DNS para garantizar la disponibilidad de la nueva dirección redeterminada. Si la

nueva dirección o la nueva dirección redeterminada está disponible, el servidor de DNS puede registrar la nueva dirección o la nueva dirección redeterminada con el identificador del dispositivo solicitante 102-3 y reservar la nueva dirección o la nueva dirección redeterminada para el dispositivo solicitante 102-3.

En una implementación, tras confirmar la nueva dirección que se asignará al dispositivo solicitante 102-3, el dispositivo de control 102-4 puede proporcionar una respuesta (por ejemplo, una respuesta de DHCP) al dispositivo solicitante 102-3. A modo de ejemplo y sin limitación, la respuesta puede incluir, entre otras, la dirección asignada (por ejemplo, la dirección global IPv6 asignada), la clave de grupo (por ejemplo, la clave de capa de enlace de grupo) asociada a la red ARA, y/o la información de configuración o parámetros utilizables para que el dispositivo solicitante 102-3 se una o configure con la red ARA. En una implementación, el dispositivo de control 102-4 (o el servidor de DHCP) puede enviar la respuesta al dispositivo solicitante 102-3. En algunas implementaciones, con o sin el conocimiento de una dirección global del dispositivo solicitante 102-3 (por ejemplo, debido a que la nueva dirección no se ha asignado aún al dispositivo solicitante 102-3), el dispositivo de control 102-4 (o el servidor de DHCP) puede enviar la respuesta al dispositivo solicitante 102-3 a través del dispositivo vecino 102-2 (y el encaminador dirigiendo la red ARA si el dispositivo de control 102-4 está situado fuera de la red ARA). Por ejemplo, el dispositivo de control 102-4 (o el servidor de DHCP) puede enviar la respuesta al dispositivo vecino 102-2 y solicitar que el dispositivo vecino 102-2 retransmita la respuesta al dispositivo solicitante 102-3. El dispositivo vecino 102-2, que ha establecido comunicación con el dispositivo solicitante 102-3, puede retransmitir la respuesta al dispositivo solicitante 102-3 a través de un mensaje usando el protocolo DHCPv6 o un mensaje de baliza. De forma adicional, o como alternativa, el dispositivo vecino 102-2 puede transmitir la respuesta en una proximidad del mismo, y el dispositivo solicitante 102-3, que está cerca del dispositivo vecino 102-2, puede recibir la respuesta emitida y analizar la respuesta para obtener tal información como la nueva dirección asignada, etc., para unirse a la red ARA.

Tras recibir la respuesta a la solicitud de unión, el dispositivo solicitante 102-3 puede configurar parámetros de configuración para la comunicación dentro de la red ARA basándose, por ejemplo, en la información de configuración o los parámetros incluidos en la respuesta. Por ejemplo, el dispositivo solicitante 102-3 se puede acoplar a una topología de encaminamiento en la red ARA al decidir qué trayectoria de encaminamiento y/o dispositivo vecino usar si hay más de una trayectoria de encaminamiento y/o dispositivos vecinos disponibles. De forma adicional, o como alternativa, el dispositivo solicitante 102-3 puede enviar un mensaje al nodo raíz de la red ARA para notificar su llegada a la red ARA, por ejemplo. El dispositivo solicitante 102-3 puede, o no, solicitar o necesitar un acuse de recibo desde el nodo raíz. En el caso de que se solicite o necesite un acuse de recibo desde el nodo raíz, el dispositivo solicitante 102-3 puede esperar un acuse de recibo enviado desde el nodo raíz. En una implementación, si no se recibe acuse de recibo desde el nodo raíz durante un período de tiempo predeterminado, el dispositivo solicitante 102-3 puede reenviar el mensaje al nodo raíz. El dispositivo solicitante 102-3 puede reenviar el mensaje para un número predeterminado de fallos de recepción de acuse de recibo. De forma adicional, o como alternativa, el dispositivo solicitante 102-3 puede seleccionar una trayectoria de encaminamiento diferente y/o un dispositivo vecino 102 para enviar o retransmitir el mensaje al nodo raíz. Tras recibir un acuse de recibo del nodo raíz, el dispositivo solicitante 102-3 puede comenzar a realizar operaciones normales en la red ARA, que incluyen, por ejemplo, encaminamiento y/o reenvío de paquetes que no están destinados al dispositivo solicitante 102-3, procesamiento de paquetes dirigido al dispositivo solicitante 102-3, respondiendo por paquetes (si se solicitan) que están destinados al nodo solicitante 102-3, etc. Si no se recibe acuse de recibo desde el nodo raíz para un número predeterminado de reintentos, el dispositivo solicitante 102-3 puede comenzar a realizar operaciones normales como si se hubiera recibido un acuse de recibo desde el nodo raíz, reenviando nuevamente el mensaje de llegada después de un intervalo de tiempo predeterminado o decidir migrar a otra red ARA adyacente, si está disponible, etc.

Migración de dispositivo ilustrativa

En algunas implementaciones, un dispositivo 102 dentro de una red ARA puede decidir o iniciar el abandono o la migración desde la red ARA a otra red ARA. A modo de ejemplo y sin limitación, el dispositivo 102 puede decidir o iniciar la partida o migración desde una red ARA (en donde está actualmente acoplado el dispositivo 102) a otra red ARA basándose en una o más condiciones de red asociadas con el dispositivo 102 y/o la red ARA. Por ejemplo, el dispositivo 102 puede iniciar la migración desde la red ARA a otra red ARA si una calidad de comunicación (por ejemplo, calidad de comunicación de capa de enlace) con el dispositivo 102 es pobre o está degradada, por ejemplo, por debajo de un umbral de calidad predeterminado. De forma adicional, o como alternativa, el dispositivo 102 puede migrar de la red ARA a otra red ARA si falla el encaminador de la red ARA. De forma adicional, o como alternativa, el dispositivo 102 puede, mientras está acoplado a la red ARA actual, escuchar la en un entorno de la misma, y detectar o descubrir la existencia de otras redes ARA adyacentes. El dispositivo 102 puede aprender acerca del rendimiento tal como calidad de servicio (QoS) ofrecido por estas redes adyacentes. El dispositivo 102 puede migrar de la red ARA a otra red ARA si la otra red ARA ofrece un mejor rendimiento, tal como calidad de servicio, que la red ARA a la que está actualmente acoplado el dispositivo 102. En una implementación, el dispositivo 102 puede seleccionar una red ARA adyacente para la migración basándose en una o más políticas o criterios. Los ejemplos de estas políticas o criterios pueden incluir, pero no se limitan a, seleccionar una red que ofrezca al menos una cantidad predeterminada o porcentaje de mejora sobre el rendimiento, tal como QoS, tiempo o latencia de respuesta, rendimiento, tasa de caída de paquetes, etc., en comparación con la red ARA a la que está actualmente acoplado el dispositivo 102.

De forma adicional, o como alternativa, el dispositivo 102 puede ser forzado por el dispositivo de control 102-4 (o un

dispositivo 102 en la red ARA, tal como el encaminador que dirige la red ARA) a migrar de la red ARA a otra red ARA por razones administrativas asociadas con la red ARA tal como saturación o sobrecarga de dispositivos en la red ARA, degradación del rendimiento (por ejemplo, mayor tasa de caída de paquetes, menor ancho de banda disponible, mayor tasa de colisión, etc.) asociada a la red ARA, equilibrado de carga entre la red ARA y la otra red, etc. De forma adicional, o como alternativa, el dispositivo de control 102-4 puede forzar que el dispositivo 102 migre de la red ARA a otra red ARA si la red ARA está llena (por ejemplo, una carga actual en la red ARA es mayor o igual a un umbral predeterminado) y un dispositivo nuevo que solicita unirse a la red ARA es un dispositivo aislado.

En una implementación, en un evento en que el dispositivo de control 102-4 puede necesitar forzar que algún dispositivo 102 abandone la red ARA o migre a otra red ARA, el dispositivo de control 102-4 puede determinar que uno o más dispositivos 102 en la red ARA salgan o migren seleccionando aleatoriamente un dispositivo 102 de la red ARA. En algunas implementaciones, el dispositivo de control 102-4 puede seleccionar uno o más dispositivos para salir o migrar basándose en información asociada con cada dispositivo en la red ARA. En una implementación, el dispositivo de control 102-4 puede almacenar la información asociada con cada dispositivo 102 en la red ARA cuando el dispositivo respectivo 102 se une a la red ARA.

De forma adicional, o como alternativa, el dispositivo de control 102-4 puede inspeccionar cada dispositivo en la red ARA en respuesta a la decisión de forzar que uno o más dispositivos 102 en la red ARA abandonen o migren a otra red ARA. De forma adicional, o como alternativa, el dispositivo de control 102-4 puede consultar los dispositivos 102 en la red ARA para determinar cuál de ellos es capaz de abandonar o migrar de la red ARA. De forma adicional, o como alternativa, el dispositivo de control 102-4 puede recuperar la información de topología asociada con cada dispositivo 102 en la red ARA desde la oficina central 104 o cualquier dispositivo o nodo que esté jerárquicamente aguas arriba del dispositivo de control 102-4. En una implementación, la información asociada con cada dispositivo 102 puede incluir, aunque no de forma limitativa, si el dispositivo 102 respectivo es un dispositivo aislado, si el dispositivo 102 respectivo tiene un dispositivo secundario (es decir, un dispositivo que está jerárquicamente aguas abajo del dispositivo respectivo 102), cuántos dispositivos secundarios tiene el dispositivo respectivo 102, etc.

En respuesta a la recuperación de la información asociada con cada dispositivo 102 en la red ARA o la recepción de respuestas desde dispositivos en la red ARA, el dispositivo de control 102-4 puede seleccionar uno o más dispositivos 102 en la red ARA para abandonar o migrar basándose en una o más estrategias heurísticas. A modo de ejemplo y no de limitación, el dispositivo de control 102-4 puede seleccionar uno o más dispositivos 102 que no están aislados como se indica en la información. De forma adicional, o como alternativa, el dispositivo de control 102-4 puede seleccionar uno o más dispositivos 102 que tienen menos dispositivos secundarios, por ejemplo, menos de un número umbral predeterminado. De forma adicional, o como alternativa, el dispositivo de control 102-4 puede seleccionar un número predeterminado (por ejemplo, uno, dos, etc.) de los primeros pocos dispositivos 102 que tienen menos de un número umbral de dispositivos secundarios. De forma adicional, o como alternativa, el dispositivo de control 102-4 puede seleccionar uno o más dispositivos que están más alejados del dispositivo de control 102-4 basándose en la información de encaminamiento, por ejemplo.

Tras seleccionar el uno o más dispositivos 102 para salir o migrar de la red ARA, el dispositivo de control 102-4 puede enviar una instrucción o solicitud al uno o más dispositivos 102 para abandonar o migrar de la red ARA. En una implementación, el dispositivo de control 102-4 puede enviar la instrucción o solicitud a un dispositivo 102 y enviar la instrucción o solicitud a otro dispositivo 102 si el dispositivo 102 anterior no puede salir o migrar de la red ARA por alguna razón (por ejemplo, el primer dispositivo quedaría aislado si fuera forzado a abandonar la red ARA actual). En algunas implementaciones, el dispositivo de control 102-4 puede enviar la instrucción o solicitud a más de un (o un número predeterminado de) dispositivos 102 para evitar el problema de reenviar la instrucción o solicitud a otros dispositivos 102 en el caso en que la instrucción o solicitud previamente enviada pueda no ser cumplida por un dispositivo previamente instruido o solicitado.

En un ejemplo específico, el dispositivo de control 102-4 puede seleccionar el dispositivo 102-5 para abandonar o migrar de la red ARA. En respuesta a la recepción de la instrucción o solicitud de migración, el dispositivo 102-5 puede determinar si hay una o más redes ARA adicionales a las que puede migrar el dispositivo 102-5. Por ejemplo, el dispositivo 102-5 puede usar el módulo de descubrimiento 212 y el módulo de radiodifusión 214 para determinar si hay dispositivos vecinos que pertenecen a otras redes ARA. Si el dispositivo 102-5 no puede encontrar otras redes ARA a las que migrar, el dispositivo 102-5 puede enviar un mensaje al dispositivo de control 102-4, rechazando abandonar la red ARA del dispositivo de control 102-4, ya que hacer esto daría como resultado que el dispositivo 102-5 quedara aislado.

Como alternativa, el dispositivo 102-5 puede detectar otra red ARA, pero determina que la calidad de la comunicación con esta otra red ARA es pobre o esporádica. En ese caso, el dispositivo 102-5 puede enviar un mensaje al dispositivo de control 102-4 que indica que el dispositivo 102-5 no puede abandonar o migrar de la red ARA. De forma adicional, o como alternativa, en el momento de recibir la instrucción o solicitud de migración, el dispositivo 102-5 puede determinar que el dispositivo 102-5 está ocupado procesando, recibiendo y/o transmitiendo datos que pueden necesitar un cierto período de tiempo mayor o igual a un umbral de tiempo predeterminado. En respuesta a esto, el dispositivo 102-5 puede enviar un mensaje al dispositivo de control 102-4 de que el dispositivo 102-5 no puede salir o migrar de la red ARA. En una implementación, el dispositivo 102-5 puede ser forzado a abandonar o migrar de la red

ARA independientemente de las consecuencias de tal migración, excepto por que el dispositivo 102-5 no será forzado a abandonar o migrar de la red ARA si obrar de este modo diera como resultado que el dispositivo 102-5 quedara aislado.

En una implementación, si el dispositivo 102-5 detecta otra red ARA y determina que el dispositivo 102-5 puede salir o migrar de la red ARA, el dispositivo 102-5 puede comenzar a unirse a la otra red ARA como se describe en el ejemplo de la sección de registro del dispositivo arriba. Por ejemplo, el dispositivo 102-5 puede enviar una solicitud (que se puede cifrar, o no, usando una clave y/o algoritmo de cifrado como se describe en las implementaciones anteriores) a un dispositivo vecino 102 que pertenece a una red ARA adyacente para solicitar la unión a la red adyacente. Además, el dispositivo 102-5 puede transmitir adicionalmente un mensaje a los dispositivos 102 en la red de los que el dispositivo 102-5 se está yendo o migrando, lo que indica que el dispositivo 102-5 está saliendo de la red. En algunas implementaciones, debido a que el dispositivo 102-5 se ha registrado con éxito con el NMS previamente cuando se une a la red ARA del dispositivo de control 102-4, se puede eximir al dispositivo 102-5 de la totalidad o parte de un proceso de autenticación como se ha descrito anteriormente (al proporcionar una clave de grupo asociada con la red ARA y/o un identificador de dispositivo del dispositivo 102-5 a un dispositivo de control de la otra red ARA, por ejemplo) cuando se une a una nueva red ARA.

En una implementación, el dispositivo 102-5 puede recibir una nueva dirección que incluye un prefijo específico (por ejemplo, un prefijo de IPv6) designado a la otra red ARA. Tras recibir la nueva dirección, el dispositivo 102-5 puede actualizar su dirección antigua (es decir, una dirección previamente asignada al dispositivo 102-5 por el dispositivo de control 102-4) con la nueva dirección en un nivel de aplicación tal como en la norma C12.22 del Instituto Nacional Estadounidense de Normas (ANSI), DNS, etc.

En una implementación, durante un período de tiempo de la migración y antes de la compleción de la migración, el dispositivo 102-5 puede mantener la conexión o el acoplamiento a la red ARA a la que este está actual u originalmente acoplado. Por ejemplo, el dispositivo 102-5 puede seguir realizando operaciones normales en la red ARA actual, incluyendo encaminamiento y reenvío de paquetes no destinados al dispositivo 102-5, procesamiento de paquetes dirigidos al dispositivo 102-5, respondiendo por los paquetes destinados al dispositivo 102-5 - si así se solicita - a través de la red ARA actual, etc. De forma adicional, o como alternativa, el dispositivo 102-5 puede seleccionar un dispositivo vecino 102 de la nueva red ARA y emplear este dispositivo vecino 102 como un dispositivo de retransmisión y/o reenvío para paquetes de datos. De forma adicional, o como alternativa, el dispositivo 102-5 puede seguir recibiendo paquetes de datos destinados a su dirección antigua desde otros dispositivos 102 en la red ARA. En algunas implementaciones, durante el período de tiempo de la migración, el dispositivo 102-5 puede guardar o almacenar su dirección antigua y continuar procesando datos o paquetes de datos dirigidos a su dirección antigua como es habitual, manteniendo de este modo una conectividad con la red ARA que está migrando durante este período de tiempo de la migración. En una implementación, si el dispositivo 102-5 ha perdido la conexión con sus dispositivos primarios de la red ARA de la que está migrando, el dispositivo 102-5 puede, por ejemplo eliminar de su memoria intermedia todos los paquetes de sentido ascendente (paquetes de datos transmitidos a dispositivos en un nivel jerárquico superior de la red ARA). En algunas implementaciones, el dispositivo 102-5 puede reenviar los paquetes de datos recibidos a la red ARA de la que está migrando (si sigue acoplado) durante el período de tiempo de la migración. En una implementación, si el dispositivo 102-5 recibe su nueva dirección y está acoplado ahora a la otra red ARA (es decir, la nueva red ARA), el dispositivo 102-5 puede "tunelizar" los paquetes de datos almacenados en memoria intermedia, es decir, paquetes de datos proveniente de su red ARA "antigua", y enviar los paquetes de datos recibidos (que están incluidos o encapsulados en paquetes nuevos, por ejemplo) usando su nueva dirección a través de la nueva red ARA, por ejemplo.

En una implementación, tras acoplarse o migrar con éxito a la nueva red ARA, el dispositivo 102-5 se separa o abandona la red ARA antigua. En una implementación, el dispositivo 102-5 puede enviar un mensaje al nodo raíz de la red ARA antigua para notificar o anunciar su salida de la red ARA antigua. De forma adicional, o como alternativa, el dispositivo 102-5 puede enviar mensajes (que indican su salida de la red ARA antigua) a uno o más dispositivos 102 en la red ARA antigua que reenvían y/o encaminan sus paquetes de datos a través del dispositivo 102-5. Estos mensajes (es decir, mensajes al nodo raíz y/o a los otros dispositivos 102 en la red ARA antigua) pueden, o no, solicitar un acuse de recibo desde el nodo raíz y/o los otros dispositivos 102 en la red ARA antigua. Además, en algunas implementaciones, el dispositivo 102-5 puede enviar repetidamente los mensajes al nodo raíz y/o a los otros dispositivos 102 en la red ARA antigua para aumentar o asegurar la probabilidad de que el nodo raíz y/o los otros dispositivos 102 reciban los mensajes.

De forma adicional, o como alternativa, el dispositivo 102-5 puede detener el procesamiento de cualquier paquete de datos que no esté destinado a su dirección antigua. En una implementación, el dispositivo 102-5 puede elegir procesar un paquete de datos si el paquete de datos es un paquete de datos destinado a la dirección antigua del dispositivo 102-5, y/o un paquete de datos (que puede, o no, estar destinado a la dirección antigua del dispositivo 102-5) que indica un alto grado de urgencia o importancia (como lo indica un momento en el que se necesita una respuesta, etc.), por ejemplo. De forma adicional, o como alternativa, el dispositivo 102-5 puede elegir responder a ciertos tipos de paquetes de datos que tienen alcances o propósitos específicos si los paquetes de datos están destinados a la dirección antigua del dispositivo 102-5. A modo de ejemplo y no de limitación, el dispositivo 102-5 puede procesar un paquete de datos que transporta datos destinados a un conjunto predefinido de aplicaciones y requiere una respuesta

del dispositivo 102-5. El dispositivo 102-5 puede enviar una respuesta a través de la nueva red ARA y usar una nueva dirección del dispositivo 102-5 en la nueva red ARA como dirección de origen de la respuesta. De forma adicional, o como alternativa, el dispositivo 102-5 puede ignorar o eliminar paquetes de datos que no son uno de los ámbitos específicos o destinados al conjunto de aplicaciones predefinido. En algunas implementaciones, después de que el dispositivo 102-5 se haya separado de la red ARA antigua y esté realizando operaciones normales en la nueva red ARA, el dispositivo 102-5 puede seguir aceptando paquetes destinados a la dirección antigua durante un período de tiempo predeterminado que pueden estar por omisión en la red ARA antigua o nueva, o puede ser predefinido por un administrador de la red ARA antigua o nueva. El dispositivo 102-5 puede procesar paquetes de datos destinados a su dirección antigua (y/o paquetes de datos no destinados a su dirección antigua) de acuerdo con las implementaciones anteriores como se describió anteriormente.

En algunas implementaciones, la dirección antigua del dispositivo 102-5 no se redistribuirá a otro dispositivo durante un cierto período de tiempo, llamado como un período de tiempo de migración. Este período de migración se establece para que sea lo suficientemente largo como para abarcar todo el proceso de conmutación de ARA hasta que todo un sistema (incluidos, por ejemplo, los nodos raíz de las redes ARA antiguas y nuevas, servidor de DNS, etc.) se actualice para reflejar la migración del dispositivo 102-5.

Implementaciones alternativas

Aunque las implementaciones anteriores describen aplicaciones en una red de área de encaminamiento autónoma de una infraestructura de medición avanzada (AMI), la presente divulgación no se limita a esto. En una implementación, la presente divulgación se puede aplicar a redes tales como redes celulares, redes domésticas, redes de oficinas, etc. Por ejemplo, en un evento que una estación celular determina que una carga en una red celular controlada excede un umbral predeterminado, la estación celular puede seleccionar y forzar que algunos de los dispositivos móviles conectados a su red abandonen o migren a otra red celular, por lo tanto, realizando equilibrado de carga para su red controlada.

Métodos ilustrativos

La figura 3 es un diagrama de flujo que representa un ejemplo de método 300 de registro de dispositivo en una red. La figura 4 es un diagrama de flujo que representa un método 400 ilustrativo de determinación de si permitir o rechazar un dispositivo para unirse a una red. La figura 5 es un diagrama de flujo que representa un método 500 ilustrativo de migración de dispositivo desde una red. Los métodos de la figura 3, la figura 4 y la figura 5 pueden, pero no necesitan, implementarse en el entorno de la figura 1 y usar el dispositivo de la figura 2. Para facilitar la explicación, los métodos 300, 400 y 500 se describen con referencia a las figuras 1 y 2. Sin embargo, los métodos 300, 400 y 500 pueden, como alternativa, implementarse en otros entornos y/o usar otros sistemas.

Los métodos 300, 400 y 500 se describen en el contexto general de instrucciones ejecutables por ordenador. En general, las instrucciones ejecutables por ordenador pueden incluir rutinas, programas, objetos, componentes, estructuras de datos, procedimientos, módulos, funciones y similares que realizan funciones particulares o implementan tipos de datos abstractos particulares. Los métodos se pueden poner en práctica también en un entorno informático distribuido en donde las funciones son realizadas por dispositivos de procesamiento remotos que están vinculados a través de una red de comunicación. En un entorno de compilación distribuido, las instrucciones ejecutables por ordenador pueden ubicarse en medios de almacenamiento informático local y/o remoto, incluidos los dispositivos de almacenamiento de memoria.

Los métodos ilustrativos se ilustran como una colección de bloques en un gráfico de flujo lógico que representa una secuencia de operaciones que se puede implementar en hardware, software, firmware o una combinación de los mismos. El orden en que se describen los métodos no se interpreta como una limitación, y se puede combinar un número de los bloques de métodos descritos en un orden nuevo para implementar el método o métodos alternativos. Además, algunos bloques individuales se pueden omitir del método sin apartarse del espíritu y alcance de la materia objeto descrita en el presente documento. En el contexto del software, los bloques representan instrucciones de computadora que, cuando son ejecutadas por uno o más procesadores, realizan las operaciones recitadas.

Con referencia de nuevo a la figura 3, en el bloque 302, el dispositivo solicitante 102-3 puede desear unirse a una red que cubre un área en donde se encuentra el dispositivo solicitante 102-3. El dispositivo solicitante 102-3 puede descubrir el dispositivo vecino 102-2 y envía una solicitud de unión (por ejemplo, una solicitud de DHCPv6 o un mensaje de baliza que incluye la solicitud de unión) al dispositivo vecino 102-2.

En el bloque 304, en respuesta a la recepción de la solicitud de unión, el dispositivo vecino 102-2 puede analizar la solicitud y determinar que el dispositivo solicitante 102-3 solicita unirse a una red de la que el dispositivo vecino 102-2 es miembro.

En el bloque 306, en respuesta a determinar que el dispositivo solicitante 102-3 solicita unirse a la red, el dispositivo vecino 102-2 puede opcionalmente filtrar la solicitud de unión. En una implementación, el dispositivo vecino 102-2 puede determinar si retransmitir la solicitud de unión a otros dispositivos de la red. Por ejemplo, el dispositivo vecino

102-2 puede haber recibido una instrucción o solicitud del dispositivo de control 102-4 de que no se pueden aceptar dispositivos a excepción de los dispositivos aislados en la red por razones administrativas o de red tales como saturación o sobrecarga de la red. En este caso, el dispositivo vecino 102-2 puede determinar si el dispositivo solicitante 102-3 es un dispositivo aislado basándose en, por ejemplo, información incluida en la solicitud de unión. En una implementación, si el dispositivo vecino 102-2 ha recibido la instrucción o solicitud de que no se acepten dispositivos a excepción de dispositivos aislados en la red y el dispositivo solicitante 102-3 no es un dispositivo aislado, el dispositivo vecino 102-2 puede enviar una respuesta al dispositivo solicitante 102-3, que indica que la solicitud de unión es rechazada. De lo contrario, el dispositivo vecino 102-2 puede prepararse para retransmitir la solicitud de unión del dispositivo solicitante 102-3 a otros dispositivos de la red.

En el bloque 308, el dispositivo solicitante 102-3 recibe la respuesta del dispositivo vecino 102-2 que indica que la solicitud de combinación de la misma es rechazada.

En el bloque 310, el dispositivo vecino 102-2 puede retransmitir la solicitud de unión al dispositivo de control 102-4 o al dispositivo primario del dispositivo vecino 102-2 basándose en si el dispositivo vecino 102-2 conoce la dirección del dispositivo de control 102-4.

En el bloque 312, en respuesta a la recepción de la solicitud de unión retransmitida desde el dispositivo vecino 102-2, el dispositivo de control 102-4 puede determinar si permite o rechaza la solicitud de unión del dispositivo solicitante 102-3. En una implementación, el dispositivo de control 102-4 puede determinar si permite la solicitud de unión basándose en una condición de la red y/o una condición del dispositivo solicitante 102-3. Si el dispositivo de control 102-4 determina rechazar la solicitud de unión del dispositivo solicitante 102-3, el dispositivo de control 102-4 puede enviar una respuesta al dispositivo solicitante 102-3 a través del dispositivo vecino 102-2, lo que indica que el dispositivo de control 102-4 o la red no puede permitir que el dispositivo solicitante 102-3 se una.

En el bloque 314, en respuesta a la determinación de permitir la solicitud del dispositivo solicitante 102-3, el dispositivo de control 102-4 puede enviar un mensaje que incluye un identificador y/o una firma de autenticación del dispositivo solicitante 102-3 incluida en la solicitud de unión del dispositivo solicitante 102-3 a un servidor de autenticación (por ejemplo, servidor de AAA 120). En una implementación, el dispositivo de control 102-4 puede firmar o cifrar adicionalmente el mensaje usando una clave de grupo asociada con la red o una clave de cifrado asociada con el dispositivo de control 102-4.

En el bloque 316, tras recibir el mensaje, el servidor de autenticación 120 puede descifrar el mensaje si está cifrado, y analizar el mensaje para obtener el identificador y/o la firma de autenticación del dispositivo solicitante 102-3. El servidor de autenticación 120 puede entonces realizar la autenticación basándose en el identificador obtenido y/o la firma de autenticación obtenida del dispositivo solicitante 102-3. En respuesta a la autenticación con éxito de una identidad del dispositivo solicitante 102-3, el servidor de autenticación 120 puede enviar un mensaje de autenticación con éxito que posiblemente incluya una clave de grupo asociada con la red (que se puede cifrar, o no, usando una clave pública o simétrica del dispositivo solicitante 102-4) al dispositivo de control 102-4. En una implementación, la clave pública o simétrica del dispositivo solicitante 102-4 puede ser conocida solo por el dispositivo solicitante 102-4 y el servidor de autenticación 120. En algunas implementaciones, la clave pública o simétrica del dispositivo solicitante 102-4 puede ser conocida adicionalmente por otros dispositivos o servidores (tales como la oficina central 104 y/o el dispositivo de control 102-4, por ejemplo) de la red ARA que son responsables de la gestión o el control de la red. Por ejemplo, el servidor de autenticación 120 puede enviar el mensaje de autenticación con éxito que incluye adicionalmente la clave pública o simétrica del dispositivo solicitante 102-4 que ha sido cifrada usando la clave de grupo asociada con la red ARA. Como alternativa, si el servidor de autenticación 120 no puede autenticar la identidad del dispositivo solicitante 102-3, el servidor de autenticación 120 puede enviar un mensaje de autenticación fallido al dispositivo de control 102-4, lo que indica que la autenticación ha fallado.

En el bloque 318, en respuesta a la recepción de un mensaje del servidor de autenticación 120, el dispositivo de control 102-4 puede determinar si la autenticación de la identidad del dispositivo solicitante 102-3 tiene éxito. Si falla, el dispositivo de control 102-4 puede enviar una respuesta al dispositivo solicitante 102-3 a través del dispositivo vecino 102-2, indicando que la solicitud de unión del dispositivo solicitante 102-3 es denegada. En respuesta a la determinación de que la identidad del dispositivo solicitante 102-3 se autentica con éxito, el dispositivo de control 102-4 puede enviar una respuesta de admisión al dispositivo solicitante 102-3 a través del dispositivo vecino 102-2 que incluye un mensaje que indica que se permite la solicitud de unión del dispositivo solicitante 102-3. En una implementación, la respuesta puede incluir, además, pero no se limita a, una clave de grupo asociada con la red que se puede cifrar, o no, en el servidor de autenticación usando la clave pública o simétrica del dispositivo solicitante 102-3. De forma adicional, o como alternativa, en algunas implementaciones, el dispositivo de control 102-4 puede cifrar la respuesta usando una clave pública o simétrica del dispositivo solicitante 102-3 si el dispositivo de control 102-4 conoce la clave pública o simétrica del dispositivo solicitante 102-3, por ejemplo, desde el servidor de autenticación 120. De forma adicional, o como alternativa, en una implementación, el dispositivo de control 102-4 puede cifrar la clave de grupo (y/u otra información relacionada para unirse a la red) usando la clave pública o simétrica del dispositivo solicitante 102-3 (si esta clave pública o simétrica es conocida por el dispositivo de control 102-4) y cifra la clave de grupo cifrada y/o el mensaje usando la clave de grupo asociada con la red. En alguna implementación, el dispositivo de control 102-4 puede cifrar la clave de grupo y el mensaje usando la clave pública o simétrica del dispositivo

solicitante 102-3, y cifrar adicionalmente la clave de grupo cifrada, el mensaje cifrado y/u otra información (tal como información que permite encaminar la respuesta al dispositivo solicitante 102-3, por ejemplo, una dirección del dispositivo vecino 102-2 y/o una identidad del dispositivo solicitante 102-3, etc.) usando la clave de grupo.

En algunas implementaciones, el dispositivo de control 102-4 puede no enviar una respuesta de admisión al dispositivo solicitante 102-3 tras recibir una autenticación de identidad con éxito del dispositivo solicitante 102-3 desde el servidor de autenticación 120 (es decir, después de determinar que la identidad del dispositivo solicitante 102-3 está autenticada con éxito). En estas implementaciones alternativas, el dispositivo de control 102-4 puede enviar opcionalmente una solicitud de registro al NMS para registrar el dispositivo solicitante 102-3 con el NMS o la oficina central 104 como se describe en el bloque 324 a continuación.

En el bloque 320, el dispositivo vecino 102-2 puede recibir y analizar la respuesta de admisión enviada desde el dispositivo de control 102-4. En una implementación, si la respuesta se cifra usando la clave de grupo asociada a la red, el dispositivo vecino 102-2 puede descifrar la respuesta cifrada. En una implementación, en respuesta a determinar que la respuesta de admisión es una respuesta relacionada con la solicitud de unión del dispositivo solicitante 102-3, el dispositivo vecino 102-2 puede transmitir parte o la totalidad de la respuesta al dispositivo solicitante 102-2. Por ejemplo, el dispositivo vecino 102-2 puede transmitir parte de la respuesta que se cifra usando la clave pública o simétrica del dispositivo solicitante 102-3 al dispositivo solicitante 102-3.

En el bloque 322, el dispositivo solicitante 102-3 recibe la respuesta retransmitida desde el dispositivo vecino 102-2 y analiza la respuesta para recuperar un resultado de la solicitud de combinación y/o la clave de grupo de la red (si está incluida). El dispositivo solicitante 102-3 puede comenzar a recibir datos desde y/o enviar datos a otros dispositivos de la red usando la clave de grupo.

En el bloque 324, el dispositivo de control 102-4 puede enviar opcionalmente una solicitud de registro al NMS para registrar el dispositivo solicitante 102-3 con el NMS o la oficina central 104. La solicitud de registro puede incluir, pero no se limita a, un identificador del dispositivo solicitante 102-3.

En el bloque 326, en respuesta a la recepción de la solicitud de registro desde el dispositivo de control 102-4, el NMS puede obtener información asociada con la red y la información asociada con el dispositivo solicitante 102-3 en la misma o desde otros dispositivos. El NMS puede determinar información de configuración o parámetros utilizables para el dispositivo solicitante 102-3 basándose en la información obtenida. Por ejemplo, el NMS puede determinar información de configuración o parámetros utilizables para el dispositivo solicitante 102-3 basándose en un tipo del dispositivo solicitante 102-3, un tipo de la red, etc. Tras determinar la información de configuración o los parámetros, el NMS puede enviar la información de configuración o los parámetros al dispositivo de control 102-4.

En el bloque 328, en respuesta a la obtención de la información de configuración o parámetros del NMS, el dispositivo de control 102-4 puede asignar una nueva dirección al dispositivo solicitante 102-3. En una implementación, el dispositivo de control 102-4 puede asignar una nueva dirección que incluye un prefijo especificado o designado a la red. El dispositivo de control 32 puede preparar adicionalmente una respuesta (por ejemplo, una respuesta de DHCP) al dispositivo solicitante 102-3. En una implementación, la respuesta puede incluir, entre otras, la nueva dirección asignada, la información o parámetros de configuración y/o la clave de grupo asociada a la red. En una implementación, si el dispositivo de control 102-4 no ha enviado una respuesta de admisión al dispositivo solicitante 102-3 inmediatamente después de determinar que la identidad del dispositivo solicitante 102-3 está autenticada con éxito, enviando esta respuesta desde el dispositivo de control 102-4 puede indicar la autenticación con éxito de la identidad del dispositivo solicitante 102-3. En algunas implementaciones, el dispositivo de control 102-4 puede fusionar adicionalmente la información recibida del servidor de autenticación 120 relacionada con la autenticación de la identidad del dispositivo solicitante 102-3 en la respuesta. En una implementación, el dispositivo de control 102-4 puede enviar la respuesta al dispositivo solicitante 102-3 a través del dispositivo vecino 102-2 (y un encaminador que dirige la red si el dispositivo de control se encuentra fuera de la red).

En el bloque 330, el dispositivo vecino 102-2 retransmite la respuesta desde el dispositivo de control 102-4 al dispositivo solicitante 102-3.

En el bloque 332, el dispositivo solicitante 102-3 se une a y se registra con éxito con la red usando información (por ejemplo, la clave de grupo, la dirección asignada, y/o la información o parámetros de configuración) recibidos en la respuesta. En una implementación, el dispositivo solicitante 102-3 puede autentificar adicionalmente la red si la clave simétrica o asimétrica del dispositivo solicitante 102-3 es conocida solamente a sí misma y a uno o más dispositivos y/o servidores autorizados (por ejemplo, el servidor de autenticación 120, la oficina central 104 y/o el dispositivo de control 102-4). Por ejemplo, la clave de grupo que se incluye en la respuesta puede cifrarse usando la clave simétrica o asimétrica (por ejemplo, la clave pública) del dispositivo solicitante 102-3. El dispositivo solicitante 102-3 puede por lo tanto autenticar la red si el dispositivo solicitante 102-3 puede descifrar la clave de grupo cifrada usando su clave simétrica o asimétrica (por ejemplo, la clave privada), y puede comunicarse con éxito con otros dispositivos de la red ARA usando esa clave de grupo descifrada. Sin embargo, si el dispositivo solicitante 102-3 no puede comunicar datos con otros dispositivos usando la clave de grupo descifrada, el dispositivo solicitante 102-3 puede determinar que la autenticación de la red falla, y abandonar (o desconectarse de) la red en consecuencia.

Con referencia de nuevo a la figura 4, en el bloque 402, el dispositivo de control 102-4 puede recibir una solicitud del dispositivo solicitante 102-3 a través del dispositivo vecino 102-2. El dispositivo solicitante 102-3 puede incluir un dispositivo recientemente implementado dentro de la red o un dispositivo que intenta migrar a la red desde otra red. En una implementación, el dispositivo de control 102-4 puede determinar que la solicitud del dispositivo solicitante 102-3 es una solicitud de unión, solicitando unirse a la red asociada con el dispositivo de control 102-4. La solicitud de unión puede incluir al menos información acerca de si el dispositivo solicitante 102-3 es un dispositivo aislado. En algunas implementaciones, la solicitud de unión puede incluir, además, pero no se limita a, una identidad del dispositivo solicitante 102-3, etc. En una implementación, la solicitud de unión puede estar cifrada o firmada por una clave privada o simétrica del dispositivo solicitante 102-3. El dispositivo de control 102-4 puede descifrar la solicitud usando la clave pública o simétrica del dispositivo solicitante 102-3 si la solicitud ha sido cifrada.

En el bloque 404, en respuesta a determinar que la solicitud es una solicitud de unión, el dispositivo de control 102-4 puede determinar si la red tiene capacidad para dar cabida a dispositivos adicionales. Por ejemplo, el dispositivo de control 102-4 puede determinar si una carga asociada con la red es mayor o igual a un umbral predeterminado. Una carga asociada a la red puede incluir, pero no se limita a, una cantidad actual de dispositivos, un tráfico actual, una tasa de caída de paquetes actual o promedio, un uso de ancho de banda actual o promedio, etc.

En el bloque 406, si el dispositivo de control 102-4 determina que la red puede dar cabida a dispositivos adicionales, por ejemplo, la carga es menor que el umbral predeterminado, el dispositivo de control 102-4 puede proceder a procesar la solicitud de unión del dispositivo solicitante 102-3 como se describe en las realizaciones anteriores, por ejemplo, la figura 3, con otros dispositivos y/o servidores.

En el bloque 408, si el dispositivo de control 102-4 determina que la red no puede dar cabida a dispositivos adicionales, por ejemplo, la carga ha excedido el umbral predeterminado, el dispositivo de control 102-4 puede determinar si el dispositivo solicitante 102-3 es un dispositivo aislado basándose, por ejemplo, en información incluida en la solicitud de unión.

En el bloque 410, si el dispositivo de control 102-4 determina que el dispositivo solicitante 102-3 no es un dispositivo aislado, el dispositivo de control 102-4 puede rechazar la solicitud de unión del dispositivo solicitante 102-3 y enviar una respuesta de rechazo al dispositivo solicitante 102-3 a través del dispositivo vecino 102-2.

En el bloque 412, si el dispositivo de control 102-4 determina que el dispositivo solicitante 102-3 es un dispositivo aislado, el dispositivo de control 102-4 puede proceder a procesar la solicitud de conexión del dispositivo solicitante 102-3 como se describe en las implementaciones anteriores, por ejemplo, la figura 3, con otros dispositivos y/o servidores. Además, el dispositivo de control 102-4 puede forzar que uno o más dispositivos de la red abandonen o migren de la red como se describe en las realizaciones anteriores y se describirá en la figura 5 y las descripciones adjuntas posteriormente.

Con referencia de nuevo a la figura 5, en el bloque 502, el dispositivo de control 102-4 decide forzar que uno o más dispositivos 102 abandonen o migren de la red. El dispositivo de control 102-4 puede tomar esta decisión basándose en una o más razones tales como el equilibrado de carga de la red, la solicitud de un dispositivo aislado para unirse a una red ya sobrecargada, etc.

En el bloque 504, el dispositivo de control 102-4 puede seleccionar uno o más dispositivos 102 en la red para salir o migrar basándose en una o más estrategias heurísticas. La una o más estrategias heurísticas pueden incluir, pero no se limitan a, la selección de dispositivos que no están aislados, la selección de dispositivos que no tienen o tienen un número menor de dispositivos secundarios, la selección de dispositivos que están comunicativamente más alejados del dispositivo de control.

En el bloque 506, tras seleccionar el uno o más dispositivos para salir o migrar, el dispositivo de control 102-4 puede enviar una instrucción o solicitud al uno o más dispositivos, forzando o solicitando que uno o más dispositivos abandonen o migren desde la red.

En el bloque 508, en respuesta a la recepción de la instrucción o solicitud de migración, el uno o más dispositivos, por ejemplo, el dispositivo 102-5, pueden determinar que el dispositivo 102-5 pueda salir o migrar de la red. En una implementación, el dispositivo 102-5 puede determinar si el dispositivo 102-5 es actualmente un dispositivo aislado detectando o descubriendo si existen una o más redes (que no sean la red de la que dispositivo 102-5 es actualmente miembro) en un área en la que se encuentra el dispositivo 102-5. El dispositivo 102-5 puede enviar un mensaje al dispositivo de control 102-4 en respuesta a la determinación de que el dispositivo 102-5 es incapaz de abandonar o migrar a otra red.

En el bloque 510, en respuesta a determinar que existen una o más redes (que no sean la red de la que el dispositivo 102-5 es actualmente un miembro), el dispositivo 102-5 puede comenzar a unirse a una de las una o más redes como se ha descrito anteriormente con respecto a la figura 3, por ejemplo. Además, el dispositivo 102-5 puede transmitir adicionalmente un mensaje a los dispositivos 102 en la red que el dispositivo 102-5 está saliendo o migrando de la

red.

En el bloque 512, durante un período de tiempo de migración y antes de la compleción de la migración, en respuesta a recibir paquetes de datos destinados a una dirección "antigua" (es decir, una dirección asignada al dispositivo 102-5 por la red desde la cual el dispositivo 102-5 se está yendo o migrando) del dispositivo 102-5, el dispositivo 102-5 puede eliminar los paquetes de datos, o enviar los paquetes de datos a otros dispositivos en la red a los que sigue conectado el dispositivo 102-5.

En el bloque 514, tras obtener con éxito la nueva dirección y acoplarse a la nueva red, el dispositivo 102-5 puede comenzar a realizar sus operaciones o funciones normales o asignadas en la nueva red.

Aunque la figura 5 describe que el dispositivo 102-5 puede ser forzado, o recibir instrucciones, para que abandone o migre de la red ARA por el dispositivo de control 102-4, en algunas implementaciones, el dispositivo 102-5 en realidad comienza por sí solo a abandonar o migrar de la red ARA a otra red ARA. A modo de ejemplo y sin limitación, el dispositivo 102-5 puede decidir o iniciar el abandono o la migración desde la red ARA a otra red ARA basándose en una o más condiciones de red asociadas con el dispositivo 102-5 y/o la red ARA. Por ejemplo, el dispositivo 102-5 puede iniciar la migración desde la red ARA a otra red ARA si una calidad de comunicación (por ejemplo, una calidad de comunicación de capa de enlace) con el dispositivo 102-5 es pobre o está degradada, por ejemplo, por debajo de un umbral de calidad predeterminado. De forma adicional, o como alternativa, el dispositivo 102-5 puede migrar de la red ARA a otra red ARA si falla el encaminador de la red ARA. De forma adicional, o como alternativa, el dispositivo 102-5 puede, mientras esté acoplado a la red ARA actual, escuchar la en un entorno de la misma, y detectar o descubrir la existencia de otras redes ARA adyacentes. El dispositivo 102-5 puede aprender acerca del rendimiento/calidad del servicio ofrecido por estas redes adyacentes. El dispositivo 102-5 puede migrar de la red ARA a otra red ARA si la otra red ARA ofrece un mejor rendimiento/calidad de servicio que la red ARA a la que está acoplado actualmente el dispositivo 102-5.

Cualquiera de los actos de cualquiera de los métodos descritos en el presente documento se puede implementar al menos parcialmente por un procesador u otro dispositivo electrónico basándose en las instrucciones almacenadas en uno o más medios legibles por ordenador. A modo de ejemplo y no de limitación, cualquiera de los actos de cualquiera de los métodos descritos en el presente documento se puede implementar bajo el control de uno o más procesadores configurados con instrucciones ejecutables que pueden almacenarse en uno o más medios legibles por ordenador, tales como uno o más medios de almacenamiento informático.

Conclusión

Aunque la invención se ha descrito en un lenguaje específico de características estructurales y/o actos metodológicos, se ha de entender que la invención no se limita necesariamente a las características o actos específicos descritos. Más bien, las características y actos específicos se divulgan como formas ilustrativas de implementación de la invención.

REIVINDICACIONES

1. Un método que comprende:

recibir, en un dispositivo (102-5), un mensaje de un dispositivo de control (102-4) de una red actual para solicitar o forzar que el dispositivo (102-5) abandone la red actual a la que está actualmente conectado el dispositivo (102-5);
en respuesta a recibir la solicitud, determinar si existen otras una o más redes a las que el dispositivo (102-5) es capaz de unirse (508); y
si existen otras una o más redes a las que el dispositivo (102-5) es capaz de unirse, seleccionar una red de entre las otras una o más redes y enviar una solicitud de unirse a la red seleccionada; si no
si no existe ninguna otra red, enviar una respuesta a la red actual para rechazar abandonar la red actual;
recibir una respuesta de la red seleccionada que indica que se permite al dispositivo (102-5) unirse a la red seleccionada; migrar (510) de la red actual a la red seleccionada basándose en información proporcionada en la respuesta recibida (510); y
antes de una compleción de la migración, y en respuesta a recibir un paquete en una dirección antigua del dispositivo (102-5), estando relacionada la dirección antigua con la red actual: reenviar el paquete recibido a la red actual si sigue existiendo una conexión entre el dispositivo y la red actual, no estando destinado el paquete al dispositivo (102-5); o
incluir el paquete recibido en un nuevo paquete y enviar el nuevo paquete usando una nueva dirección del dispositivo (102-5) tras recibir la nueva dirección asignada al dispositivo (102-5), estando relacionada la nueva dirección con la red seleccionada.

2. El método según la reivindicación 1, comprendiendo la información una clave de grupo asociada con la red seleccionada, información de configuración para que el dispositivo se una a la red seleccionada y la nueva dirección asignada al dispositivo.

3. El método según la reivindicación 2, que comprende adicionalmente: actualizar la dirección antigua del dispositivo (102-5) con la dirección nueva y recibir paquetes destinados a la dirección nueva tras la migración.

4. Uno o más medios legibles por ordenador que tienen instrucciones almacenadas en los mismos que, cuando son ejecutadas por uno o más procesadores, realizan el método de cualquiera de las reivindicaciones precedentes.

5. Un dispositivo (102-5) que comprende:

una unidad de procesamiento (108) configurada para realizar actos que comprenden:

recibir un mensaje de un dispositivo de control (102-4) de una red actual para solicitar o forzar que el dispositivo (102-5) abandone la red actual a la que está actualmente conectado el dispositivo (102-5);
en respuesta a recibir la solicitud, determinar si existen otras una o más redes a las que el dispositivo (102-5) es capaz de unirse (508); y
si existen otras una o más redes a las que el dispositivo (102-5) es capaz de unirse, seleccionar una red de entre las otras una o más redes y enviar una solicitud de unirse a la red seleccionada; si no

si no existe ninguna otra red, enviar una respuesta a la red actual para rechazar abandonar la red actual; y

estando la unidad de procesamiento (108) configurada adicionalmente para realizar actos que comprenden:

recibir una respuesta de la red seleccionada que indica que se permite al dispositivo (102-5) unirse a la red seleccionada;
migrar (510), de la red actual a la red seleccionada, basándose en información proporcionada en la respuesta recibida (510); y
antes de una compleción de la migración, y en respuesta a recibir un paquete en una dirección antigua del dispositivo (102-5), estando relacionada la dirección antigua con la red actual:

reenviar el paquete recibido a la red actual si sigue existiendo una conexión entre el dispositivo (102-5) y la red actual, no estando destinado el paquete al dispositivo (102-5); o
incluir el paquete recibido en un nuevo paquete y enviar el nuevo paquete usando una nueva dirección del dispositivo (102-5) tras recibir la nueva dirección asignada al dispositivo (102-5), estando relacionada la nueva dirección con la red seleccionada.

6. El dispositivo (102-5) de la reivindicación 5, en donde la información comprende una clave de grupo asociada con la red seleccionada, información de configuración para que el dispositivo (102-5) se una a la red seleccionada y la nueva dirección asignada al dispositivo (102-5).

7. El dispositivo (102-5) de la reivindicación 6, comprendiendo adicionalmente los actos:

actualizar la dirección antigua del dispositivo (102-5) con la dirección nueva y recibir paquetes destinados a la dirección nueva tras la migración.

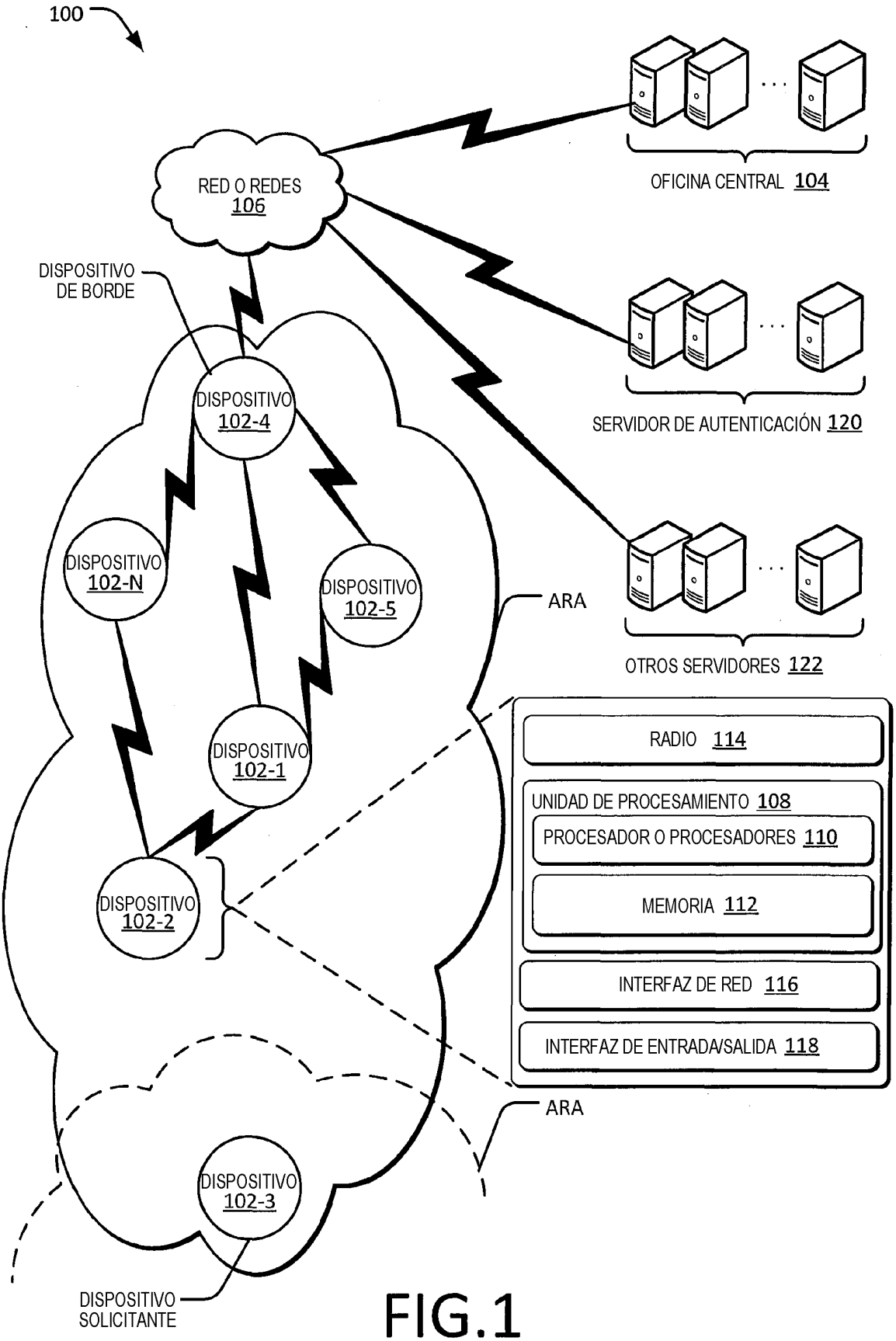
100
RED O REDES 106
OFICINA CENTRAL 104
DISPOSITIVO DE BORDE
DISPOSITIVO 102-4
SERVIDOR DE AUTENTICACIÓN 120
DISPOSITIVO 102-N
DISPOSITIVO 102-5
ARA
OTROS SERVIDORES 122
DISPOSITIVO 102-1
RADIO 114
UNIDAD DE PROCESAMIENTO 108
PROCESADOR O PROCESADORES 110
DISPOSITIVO 102-2
MEMORIA 112
INTERFAZ DE RED 116
INTERFAZ DE ENTRADA/SALIDA 118
ARA
DISPOSITIVO 102-3
DISPOSITIVO SOLICITANTE

FIG.1

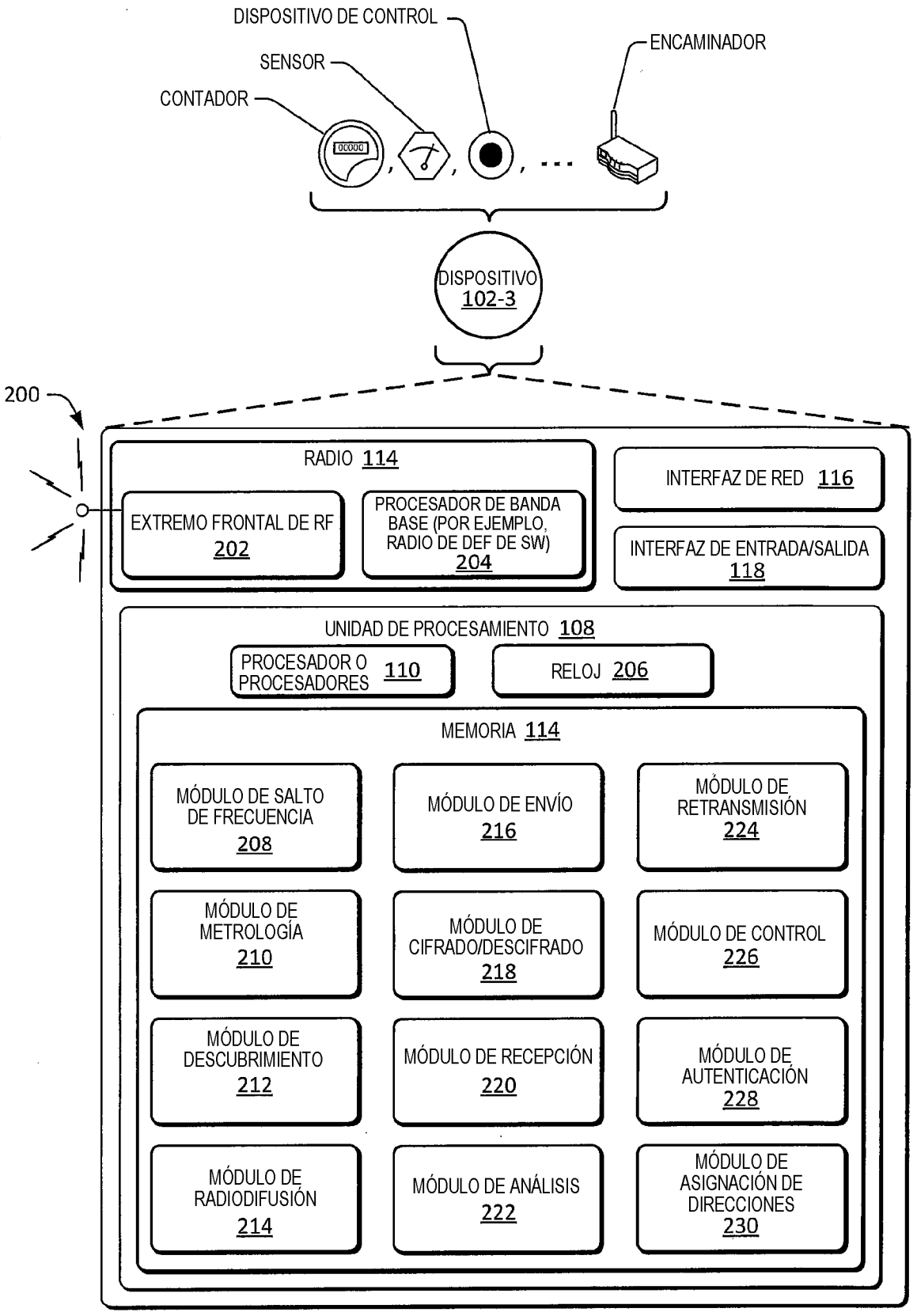
DISPOSITIVO DE CONTROL
SENSOR
CONTADOR
ENCAMINADOR
DISPOSITIVO 102-3
200
RADIO 114
EXTREMO FRONTAL DE RF 202
PROCESADOR DE BANDA BASE (POR EJEMPLO, RADIO DE DEF DE SW) 204
INTERFAZ DE RED 116
INTERFAZ DE ENTRADA/SALIDA 118
UNIDAD DE PROCESAMIENTO 108
PROCESADOR O PROCESADORES 110
RELOJ 206
MEMORIA 114
MÓDULO DE SALTO DE FRECUENCIA 208
MÓDULO DE ENVÍO 216
MÓDULO DE RETRANSMISIÓN 224
MÓDULO DE METROLOGÍA 210
MÓDULO DE CIFRADO/DESCIFRADO 218
MÓDULO DE CONTROL 226
MÓDULO DE DESCUBRIMIENTO 212
MÓDULO DE RECEPCIÓN 220
MÓDULO DE AUTENTICACIÓN 228
MÓDULO DE RADIODIFUSIÓN 214
MÓDULO DE ANÁLISIS 222
MÓDULO DE ASIGNACIÓN DE DIRECCIONES 230

FIG.2

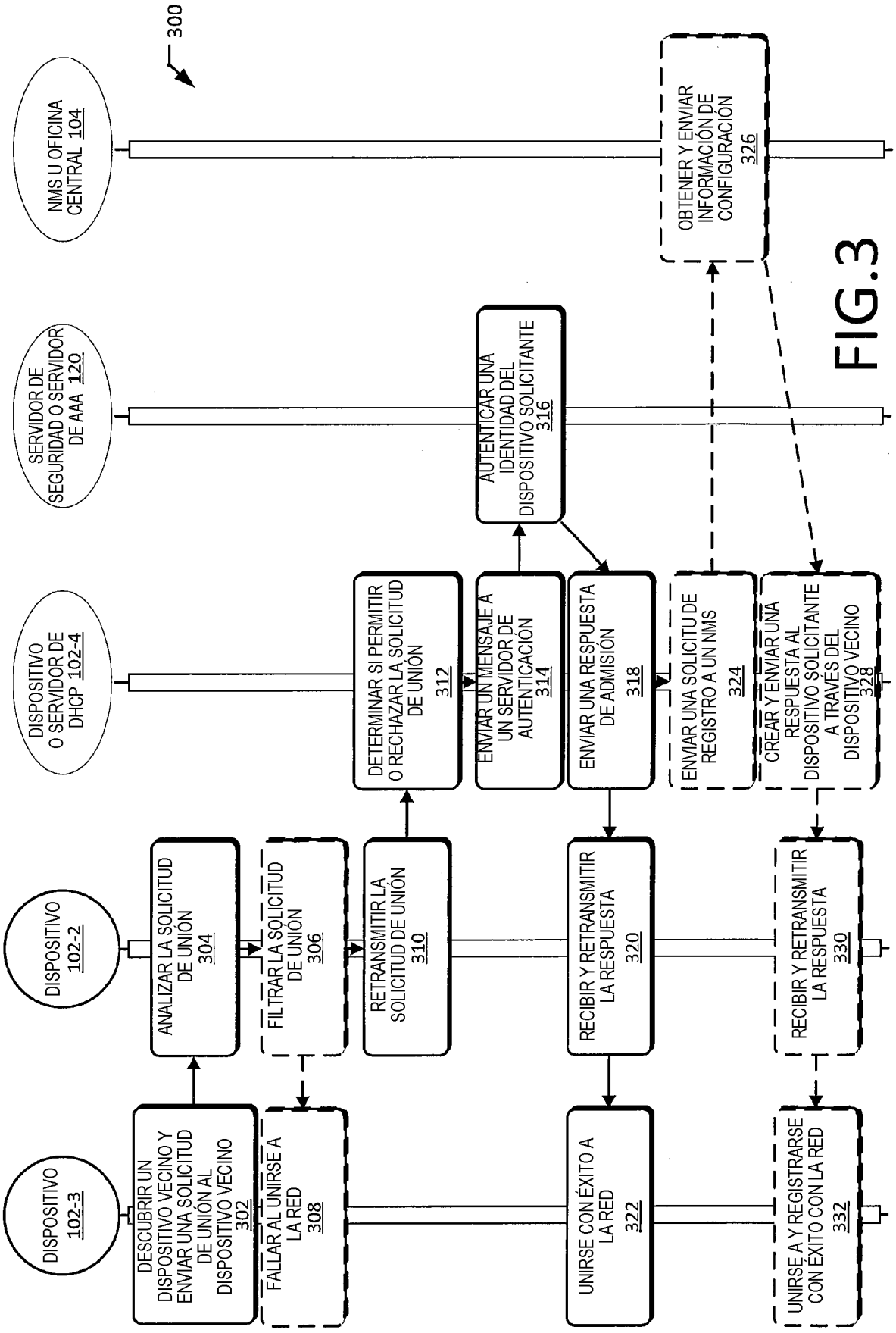
300
DISPOSITIVO 102-3
DISPOSITIVO 102-2
DISPOSITIVO O SERVIDOR DE DHCP 102-4
SERVIDOR DE SEGURIDAD O SERVIDOR DE AAA 120
NMS U OFICINA CENTRAL 104
DESCUBRIR UN DISPOSITIVO VECINO Y ENVIAR UNA SOLICITUD DE UNIÓN AL DISPOSITIVO VECINO 302
ANALIZAR LA SOLICITUD DE UNIÓN 304
FALLAR AL UNIRSE A LA RED 308
FILTRAR LA SOLICITUD DE UNIÓN 306
RETRANSMITIR LA SOLICITUD DE UNIÓN 310
DETERMINAR SI PERMITIR O RECHAZAR LA SOLICITUD DE UNIÓN 312
ENVIAR UN MENSAJE A UN SERVIDOR DE AUTENTICACIÓN 314
AUTENTICAR UNA IDENTIDAD DEL DISPOSITIVO SOLICITANTE 316
ENVIAR UNA RESPUESTA DE ADMISIÓN 318
UNIRSE CON ÉXITO A LA RED 322
RECIBIR Y RETRANSMITIR LA RESPUESTA 320
ENVIAR UNA SOLICITU DE REGISTRO A UN NMS 324
OBTENER Y ENVIAR INFORMACIÓN DE CONFIGURACIÓN 326
CREAR Y ENVIAR UNA RESPUESTA AL DISPOSITIVO SOLICITANTE A TRAVÉS DEL DISPOSITIVO VECINO 328
UNIRSE A Y REGISTRARSE CON ÉXITO CON LA RED 332
RECIBIR Y RETRANSMITIR LA RESPUESTA 330

FIG.3

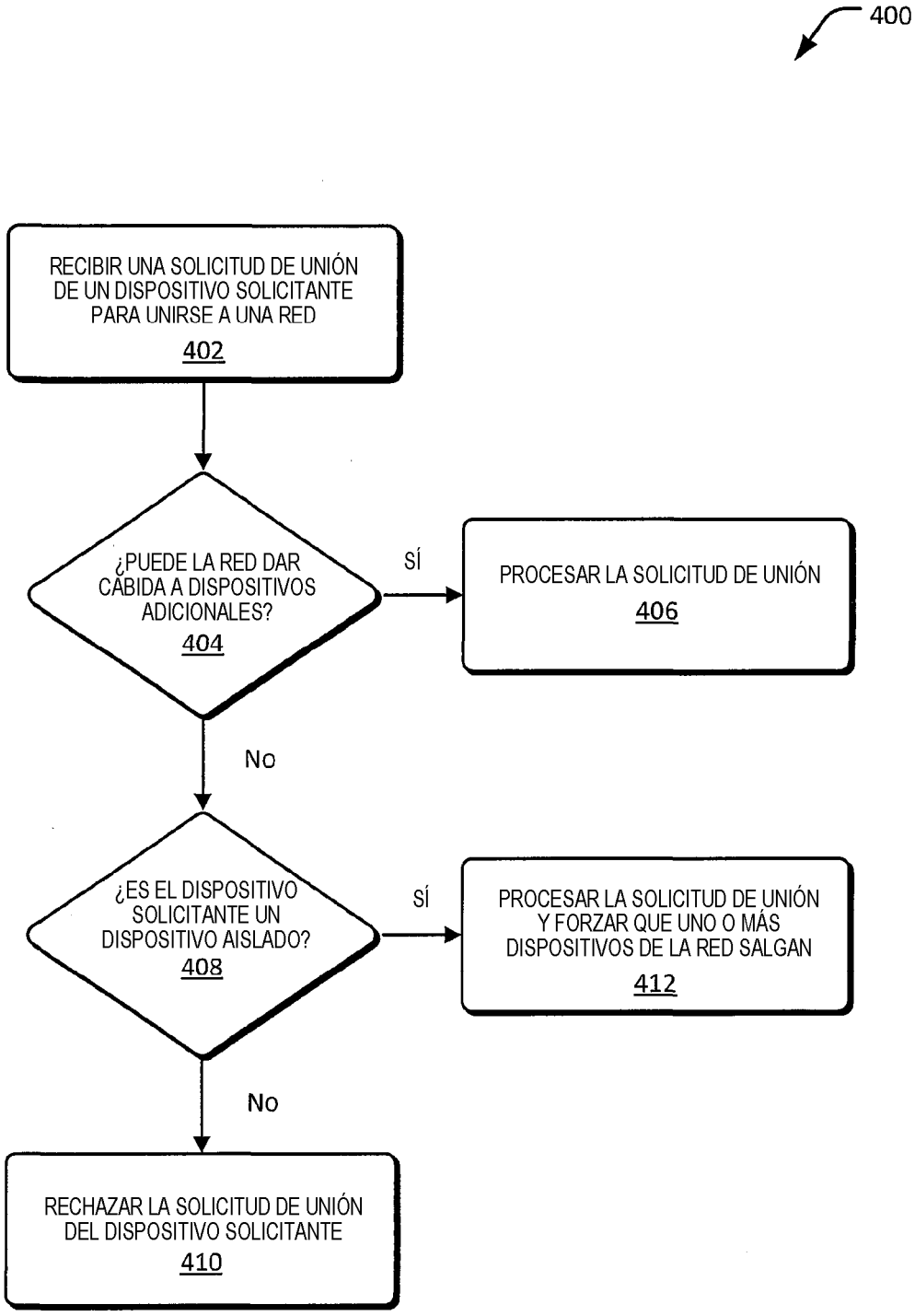
400
RECIBIR UNA SOLICITUD DE UNIÓN DE UN DISPOSITIVO SOLICITANTE PARA UNIRSE A UNA RED
402
¿PUEDE LA RED DAR CABIDA A DISPOSITIVOS ADICIONALES?
404
SÍ
PROCESAR LA SOLICITUD DE UNIÓN
406
No
¿ES EL DISPOSITIVO SOLICITANTE UN DISPOSITIVO AISLADO?
408
SÍ
PROCESAR LA SOLICITUD DE UNIÓN Y FORZAR QUE UNO O MÁS DISPOSITIVOS DE LA RED SALGAN
412
No
RECHAZAR LA SOLICITUD DE UNIÓN DEL DISPOSITIVO SOLICITANTE
410

FIG. 4

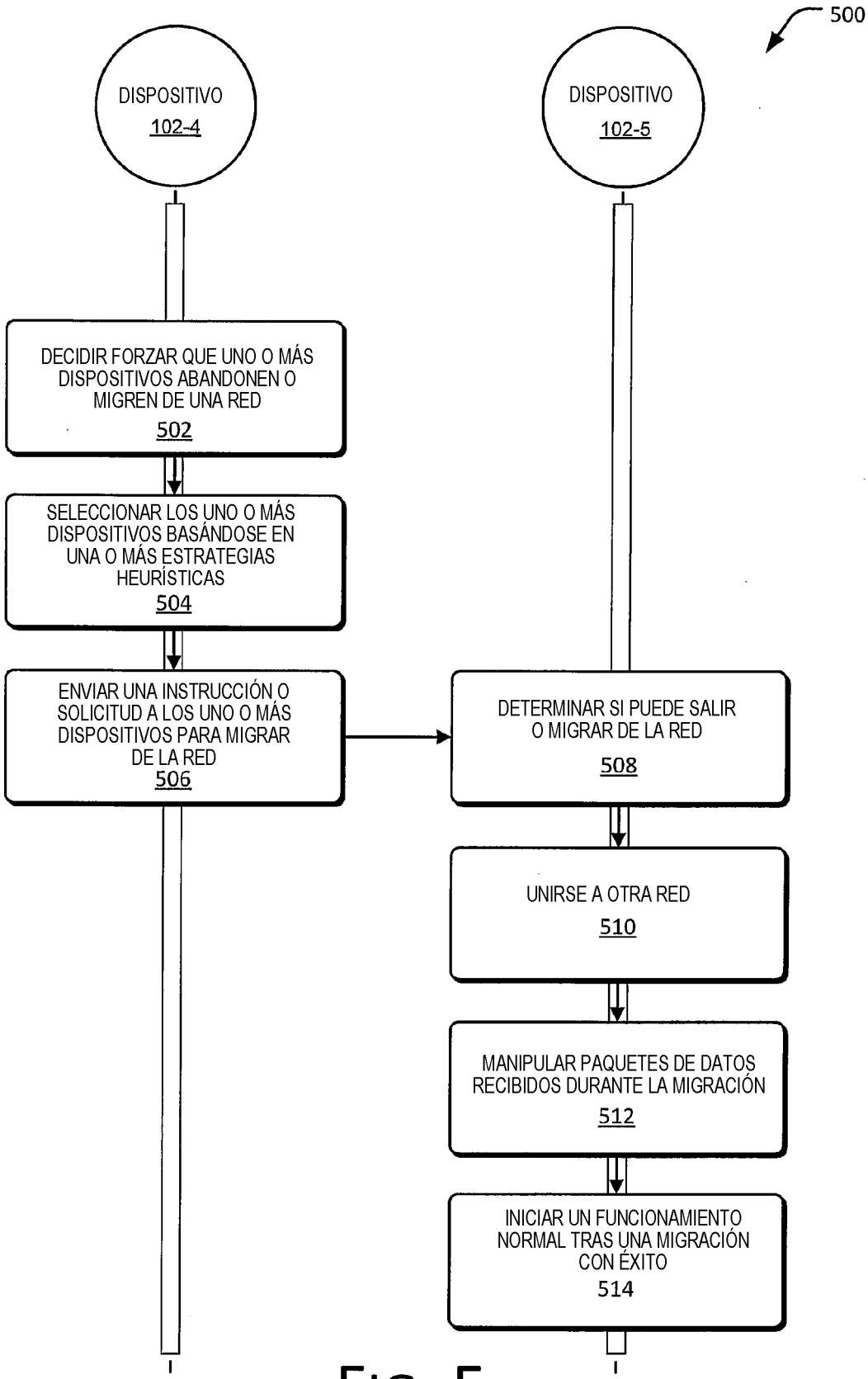
500
DISPOSITIVO
102-4
DISPOSITIVO
102-5
DECIDIR FORZAR QUE UNO O MÁS DISPOSITIVOS ABANDONEN O MIGREN DE UNA RED
502
SELECCIONAR LOS UNO O MÁS DISPOSITIVOS BASÁNDOSE EN UNA O MÁS ESTRATEGIAS HEURÍSTICAS
504
ENVIAR UNA INSTRUCCIÓN O SOLICITUD A LOS UNO O MÁS DISPOSITIVOS PARA MIGRAR DE LA RED
506
DETERMINAR SI PUEDE SALIR O MIGRAR DE LA RED
508
UNIRSE A OTRA RED
510
MANIPULAR PAQUETES DE DATOS RECIBIDOS DURANTE LA MIGRACIÓN
512
INICIAR UN FUNCIONAMIENTO NORMAL TRAS UNA MIGRACIÓN CON ÉXITO
514

FIG. 5