(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 690 470**

(51) Int. CI.:

H04W 40/24 (2009.01)
H04W 40/32 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.05.2012 E 12166697 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.08.2018 EP 2661127**

(54) Título: **Migración eficiente de dispositivo en redes de malla**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2018

(73) Titular/es:

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

(72) Inventor/es:

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

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Migración eficiente de dispositivo en redes de malla

Antecedentes

Con el advenimiento de la tecnología de dispositivos inteligentes, se ha implementado un número cada vez mayor de dispositivos inteligentes para usos residenciales, comerciales y militares en la actualidad. Ejemplos de estos dispositivos incluyen medidores de servicios inteligentes, sensores, dispositivos de control, enrutadores, reguladores, etc. En general, cuando se despliega un nuevo dispositivo, un técnico irá a un campo donde se desplegará el nuevo dispositivo y configurará manualmente el nuevo dispositivo en el campo. 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 estándar 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 estándar para unirse a una red inalámbrica consta de tres pasos: primero un nodo de unión debe completar la autenticación 802.1x, luego el nodo se comunica con un servidor de protocolo de configuración dinámica de “host” (DHCP) para adquirir una dirección de protocolo de Internet (IP) y finalmente el nodo contacta con un servidor de gestión de red (NMS) para obtener la información de configuración requerida. Estos tres pasos exigen un intenso intercambio de paquetes de extremo a extremo, que proporciona una carga considerable para las redes de comunicación inalámbricas desafiadas.

El documento US2010/0150063A1 describe que se proporciona un método para que un nuevo nodo se una a una red ad-hoc. El método incluye dos funciones básicas. Cuando el nuevo nodo puede unirse a la red, el dispositivo indicador del nodo que se está uniendo genera una indicación. Cuando el nuevo nodo se une a la red, el dispositivo indicador del nuevo nodo también genera una indicación.

Wanshi Qiu et al: “An efficient self-healing process for ZigBee sensor networks”, Tecnologías de las comunicaciones y de la información, 2007. ISCIT '07. Simposio internacional sobre, IEEE, PI, 1 de octubre de 2007, páginas 1389-1394, XP031166678, DOI: 10.1109/ISCIT.2007.4392233, ISBN: 978-1-4244-0976-1, describe que la autocuración es una característica importante de las redes de sensores inalámbricos robustas y confiables, y que ZigBee es un estándar industrial ampliamente adoptado para redes de sensores inalámbricos. Se propone un proceso eficiente para que una red ZigBee se repare después de una falla de nodo o ruptura de comunicación, permitiendo que una subred desconectada se reincorpore a la red con un mínimo intercambio de mensajes y, por lo tanto, ahorre tiempo y energía.

DHARIA S I ET AL: “A novel distributed resource-aware scalable scheme for Scatternet formation”, NETWORKS, 2003. ICON2003. LA XI CONFERENCIA INTERNACIONAL DE IEEE EL SEPT. 28-OCT. 1, 2003, PISCATAWAY, NJ, EE. UU., IEEE, 28 de septiembre de 2003 (2003-09-28), páginas 659-664, XP010683578, DOI: 10.1109/ICON.2003.1266266, ISBN: 978-0-7803-7788-2, describe que Bluetooth es un sistema de comunicación inalámbrico de corto alcance de baja potencia y bajo coste. En una red ad hoc Bluetooth, hasta ocho dispositivos Bluetooth pueden comunicarse entre sí en una red especial llamada Piconet. Scatternet se puede formar interconectando Piconets. En el documento de DHARIA, se presenta un algoritmo de formación de Scatternet escalable de recursos distribuidos. Aunque el algoritmo propuesto tiene dos fases, no es necesario que todos los nodos estén en la misma fase en un momento dado. El Scatternet formado tiene las siguientes propiedades: 1. Todos los dispositivos pueden no estar necesariamente en el rango de transmisión del otro. 2. Cualquier dispositivo será miembro de como máximo dos Piconets. 3. Se prefieren los dispositivos de mayor ponderación de recursos sobre los dispositivos de menor ponderación de recursos para realizar el papel de un maestro y/o un puente. 4. Los puentes esclavo/esclavo son preferibles a los puentes maestro/esclavo. Extensas simulaciones han demostrado que el número de mensajes transmitidos por dispositivos ponderados de bajo recurso es significativamente menor que el número de mensajes intercambiados por dispositivos ponderados de alto recurso, y el número de puentes maestro/esclavo es notablemente menor en comparación con el número de puentes esclavo/esclavo.

Breve descripción de los dibujos

La invención se presenta en la reivindicación independiente. La descripción detallada se establece con referencia a las figuras que la acompañan. En las figuras, los dígitos más a la izquierda de un número de referencia identifican la figura en la que aparece primero el número de referencia. El uso de los mismos números de referencia en diferentes figuras indica ítems similares o idénticos.

La Fig. 1 ilustra un entorno de ejemplo utilizable para implementar el registro y/o la migración de un dispositivo en una red.

La Fig. 2 ilustra el dispositivo de ejemplo de la FIG. 1 en más detalle.

La Fig. 3 ilustra un método de ejemplo de registro de dispositivo en una red.

La Fig. 4 ilustra un método de ejemplo para determinar si se permite o rechaza una solicitud de un dispositivo para unirse a una red.

La Fig. 5 ilustra un método de ejemplo de migración de dispositivo de una red a otra.

Descripción detallada

Perspectiva general

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

Esta divulgación describe métodos para el registro automático de dispositivos y la migración de dispositivos en una red de enrutamiento 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 implementará 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 la dirección o el control de 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 escuchada por dispositivos vecinos (es decir, dispositivos que están dentro del alcance de transmisión del dispositivo solicitante). Adicional o alternativamente, 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. Alternativamente, el dispositivo vecino puede retransmitir la solicitud a un dispositivo en la red que sea uno de los padres del dispositivo vecino, dirigiendo el dispositivo principal para retransmitir la solicitud al dispositivo de control u otro dispositivo que esté jerárquicamente más cerca del dispositivo de control que el dispositivo principal. En una implementación, el dispositivo vecino puede retransmitir la solicitud a su dispositivo principal 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 principal, el dispositivo vecino puede insertar una dirección de destino (por ejemplo, una dirección IP del dispositivo de control o el dispositivo principal) 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 se permite o rechaza la solicitud del dispositivo solicitante en función de 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 en función de la 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 unir redes que no sean la red del dispositivo de control. Adicional o alternativamente, se puede determinar que el dispositivo solicitante esté aislado si el dispositivo solicitante no detecta ninguna otra red que cubra el área donde se encuentra el dispositivo solicitante. Adicional o alternativamente, se puede determinar que el dispositivo solicitante está aislado si el dispositivo solicitante no detecta otras redes o se ve forzado a migrar desde 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. Adicional o alternativamente, 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. Adicional o alternativamente, 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

Adicional o alternativamente, el dispositivo de control puede determinar si permite o rechaza la solicitud del dispositivo solicitante de unirse a la red en función de 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. Adicional o alternativamente, 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.) sobre 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.

Con base 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 además que la carga (o las estadísticas) en la red, por ejemplo, el uso de ancho de banda actual es/son mayor o igual que los umbrales respectivos, el dispositivo de control puede forzar uno o más dispositivos en la red para abandonar la red o migrar 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 además 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 un único apretón de manos con la red para unirse a la red. En algunas implementaciones, el dispositivo vecino, que está ubicado en un vecindario 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 así el dispositivo solicitante de forma aleatoria o sin rumbo enviando la solicitud a la red. Los métodos descritos permiten además una migración fluida de un dispositivo existente en la red a otra red, evitando así que la red sobrecargue, atempere 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(los) respectivo(s) umbral(es) predeterminado(s). Esto facilita que el administrador decida si agrega nuevo hardware de soporte para mejorar el ancho de banda de la red y/o rearreglar físicamente o reubicar algunos de los dispositivos en la red.

En el ejemplo presentado aquí, el dispositivo de control recibe la solicitud, determina si permite o rechaza la solicitud, determina si obliga a uno o más dispositivos de la red a abandonar la red y prepara información relacionada para habilitar el dispositivo solicitante para unirse a la red. Sin embargo, en otras implementaciones, uno o más de otros dispositivos o servicios pueden realizar algunas o todas estas funciones. Por ejemplo, el dispositivo de control puede enviar o difundir 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 se permite o rechaza la solicitud del dispositivo solicitante para que se conecte a la red, mientras que otro dispositivo o servicio puede determinar si se fuerza o no uno o más dispositivos en la red para abandonar la red, y aún otro dispositivo o servicio 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 de ejemplo que es adecuado para practicar diversas implementaciones. A continuación, la aplicación describe ejemplos de sistemas, dispositivos y procesos para implementar el registro del dispositivo y la migración del dispositivo.

Ambiente de ejemplo

La Fig. 1 es un diagrama esquemático de una arquitectura 100 de ejemplo utilizable para implementar el registro del dispositivo y la migración del dispositivo. La arquitectura 100 incluye una pluralidad de nodos o dispositivos 102-1, 102-2, 102-3, 102-4, 102-5, ..., 102-N (referidos colectivamente como dispositivos 102) acoplados comunicativamente entre sí a través de rutas de comunicación directa o “enlaces”. En este ejemplo, N representa una cantidad de dispositivos dispuestos en un área de enrutamiento autónomo (ARA), tal como una red de área amplia (WAN), red de área metropolitana (MAN), red de área local (LAN), red de área vecina (NAN), red de área personal (PAN), o similar. Mientras que solo se muestra un ARA en la FIG. 1, en la práctica, pueden existir múltiples ARA y pueden definir colectivamente una red más grande, como una red de infraestructura de medición avanzada (AMI). En cualquier momento dado, cada dispositivo individual puede ser miembro de un ARA en particular. Con el tiempo, sin embargo,

los dispositivos pueden migrar de un ARA a otro ARA geográficamente próximo o superpuesto en función de una variedad de factores, tales como cargas respectivas en los ARA, interferencia o similares.

Como se discutió anteriormente, el término “enlace” se refiere a una ruta de comunicación directa entre dos dispositivos (sin pasar o propagarse por otro dispositivo). El enlace puede estar sobre una ruta de comunicación por cable 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 puede definirse por un rango 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 variedad de dispositivos tales como, por ejemplo, medidores de servicios inteligentes (por ejemplo, medidores de electricidad, gas y agua), sensores (por ejemplo, sensores de temperatura), estaciones meteorológicas, sensores de frecuencia, etc.), dispositivos de control, transformadores, enrutadores, 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.

En algunas implementaciones, algunos o todos los dispositivos 102 pueden implementarse adicional o alternativamente como cualquiera de una variedad de dispositivos informáticos convencionales que incluyen, por ejemplo, un portátil u ordenador portátil, un dispositivo de mano, una netbook, un dispositivo de Internet, un dispositivo de lectura portátil, un dispositivo lector de libros electrónicos, una tableta o un ordenador de 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 pueden configurarse además para comunicarse con una oficina 104 central a través de un dispositivo periférico (por ejemplo, el dispositivo 102-4) que sirve como punto de conexión del ARA a una o más redes de retorno 106, tales como el Internet. En una implementación, el dispositivo periférico puede incluir, pero no se limita a, un repetidor celular, un enrutador celular, un enrutador periférico, una raíz DODAG (Gráfico acíclico dirigido orientado a destino), un dispositivo raíz o nodo 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 104 central a través de la o la(s) red(es) 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 procesadores 110 acoplados de forma comunicativa a la memoria 112. La memoria 112 puede estar configurada para almacenar uno o más módulos de software y/o firmware, que son ejecutables en el o los procesadores 110 para implementar diversas funciones. Si bien los módulos se describen en este 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 ASIC, 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 memoria 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, 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. 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, memoria de solo lectura de disco compacto (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 aquí, 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 puede estar configurada además 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.

Adicional o alternativamente, en algunas implementaciones, algunos o todos los dispositivos 102 pueden incluir una interfaz de red 116, y/o una interfaz 118 de entrada/salida. La unidad de procesamiento 108 puede estar configurada además para recibir y actuar sobre datos desde la interfaz 116 de red, recibida desde la interfaz 118 de entrada/salida, y/o almacenada en la memoria 112.

La(s) red(es) 106, mientras tanto, representan una red de retorno, que puede comprender una red inalámbrica o por cable, o una combinación de las mismas. La(s) red(es) 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 por cable, o una combinación de las mismas.

La oficina 104 central puede implementarse por uno o más dispositivos informáticos, tales como servidores, ordenadores personales, ordenadores portátiles, enrutadores, conmutadores, etc. El uno o más dispositivos informáticos pueden estar equipados con uno o más procesadores conectados de forma comunicativa a la memoria. En algunos ejemplos, la oficina 104 central incluye un sistema centralizado de gestión de datos de medidor que realiza el procesamiento, análisis, almacenamiento y/o gestión de datos recibidos desde uno o más de los dispositivos 102. Por ejemplo, la oficina 104 central puede procesar, analizar, almacenar y/o gestionar datos obtenidos a partir de un medidor, sensor, dispositivo de control, enrutador, regulador, servidor, relé, interruptor, válvula y/u otros dispositivos inteligentes. La oficina 104 central puede incluir adicional o alternativamente 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 FIG. 1 ilustra la oficina 104 central en una única ubicación, en algunos ejemplos la oficina central puede distribuirse entre múltiples ubicaciones y/o puede eliminarse por completo (por ejemplo, en el caso de una plataforma informática distribuida altamente descentralizada).

En una implementación, la arquitectura puede incluir además un servidor 120 de autenticación responsable de autenticar identidades de los dispositivos 102 en la red ARA. En algunas implementaciones, la arquitectura 100 puede incluir además 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 de ejemplo

La Fig. 2 es un diagrama esquemático que muestra detalles adicionales del dispositivo 102 (por ejemplo, dispositivo representativo 102-2) de la FIG. 1. En este ejemplo, la radio 114 incluye una antena 200 acoplada a un extremo 202 frontal de RF y un procesador 204 de banda de base. El extremo 202 de RF puede proporcionar funciones de transmisión y/o recepción. El extremo 202 frontal de RF 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 202 de RF puede proporcionar una señal al procesador 204 de banda de base.

En un ejemplo, todo o parte del procesador 204 de banda base puede configurarse como una radio definida por software (SW). En un ejemplo, el procesador 204 de banda base proporciona funcionalidad de selección de frecuencia y/o canal a la radio 114. Por ejemplo, la radio definida por SW puede incluir mezcladores, filtros, amplificadores, moduladores y/o demoduladores, detectores, etc., implementados en software ejecutado por un procesador o circuito integrado específico de aplicación (ASIC) u otro dispositivo informático integrado. La radio definida por SW puede utilizar procesador(es) 110 y software definido o almacenado en la memoria 112. Alternativamente, la radio 114 puede implementarse al menos en parte utilizando componentes analógicos.

La unidad de procesamiento 108 puede incluir además un reloj 206 configurado para mantener un tiempo. El reloj 206 puede configurarse además para proporcionar uno o más temporizadores de cuenta adelante o de cuenta atrás. Dichos temporizadores pueden usarse en salto de frecuencia entre múltiples canales de comunicación.

Un módulo 208 de salto de frecuencia puede configurarse para comunicarse con el procesador 204 de banda base 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 208 de salto de frecuencia cuándo “saltar” o sintonizar un canal o frecuencia diferente. Adicionalmente, el módulo 208 de salto de frecuencia puede configurarse 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 208 de salto de frecuencia puede desplazarse repetidamente entre frecuencias acordadas, en momentos acordados y comunicarse con otro(s) dispositivo(s) durante períodos de tiempo acordados y en protocolos acordados.

En algunas implementaciones (por ejemplo, cuando el dispositivo es un contador de servicios), 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 luego puede transmitirse a uno o más dispositivos 102 para su eventual propagación a la oficina 104 central u otro destino.

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

Registro de dispositivo de ejemplo

En una implementación, antes de registrarse con el NMS en la oficina 104 central y/o convertirse en un miembro de la red ARA, un dispositivo 102 (por ejemplo, el dispositivo 102-3) puede conectarse primero a la red ARA. A modo de ejemplo y sin limitación, el dispositivo 102-3 solicitante puede conectarse primero a la red ARA hasta un punto en que el dispositivo 102-3 solicitante puede enviar una solicitud de unión a la red ARA, por ejemplo, en un nivel o capa de IP. Por ejemplo, el dispositivo 102-3 solicitante puede conectarse primero a la red ARA en el nivel MAC (es decir, control de acceso al medio) o capa MAC. En una implementación, el dispositivo (102-3) solicitante puede corresponder a un dispositivo, tal como un contador de servicios inteligentes, recientemente desplegado en un área que incluye la red ARA. Alternativamente, el dispositivo 102-3 solicitante puede corresponder a un dispositivo que está intentando migrar a la red ARA desde otra red ARA como se muestra en la FIG. 1.

En una implementación, el módulo 212 de descubrimiento del dispositivo 102-3 solicitante puede descubrir activa o pasivamente uno o más dispositivos 102 vecinos (por ejemplo, el dispositivo 102-2) en una vecindad del mismo. Un dispositivo vecino del dispositivo 102-3 solicitante puede incluir, por ejemplo, un dispositivo comunicativamente a un salto del dispositivo 102-3 solicitante. 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 102-3 solicitante puede realizar un servicio de descubrimiento vecino en una capa MAC. Adicional o alternativamente, el módulo 212 de descubrimiento puede descubrir el uno o más dispositivos vecinos en la vecindad del mismo a través del examen de señales detectadas o recibidas a una frecuencia predeterminada o rango de frecuencias designado para la red ARA que el dispositivo 102-3 solicitante desea unirse.

Adicional o alternativamente, en algunas implementaciones, el dispositivo 102-3 solicitante puede transmitir la solicitud para unirse a la red ARA usando el módulo 214 de radiodifusión con o sin primero conocer o descubrir cualquier dispositivo en la vecindad del mismo, en un intento de que uno o más dispositivos que están dentro de su vecindario pueden recibir la solicitud, y pueden procesar la solicitud en nombre del dispositivo 102-3 solicitante, y/o establecer una conexión con el dispositivo 102-3 solicitante.

Adicional o alternativamente, en una implementación, el módulo 214 de radiodifusión puede transmitir una presencia del dispositivo 102-3 solicitante, y esperar a que uno o más dispositivos en la red ARA que observen la presencia del dispositivo 102-3 solicitante se comuniquen con el dispositivo 102-3 solicitante solicitando el dispositivo 102-3. En una implementación, el módulo 214 de radiodifusión puede transmitir la presencia del dispositivo 102-3 solicitante usando un código o mensaje predeterminado en una frecuencia o rango de frecuencia predeterminados.

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

El dispositivo 102-3 solicitante 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 102-4 periférico, 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 finalmente la solicitud de unión del dispositivo 102-3 solicitante.

En algunas implementaciones, el dispositivo 102-3 solicitante puede cifrar la totalidad o parte de la solicitud de unión o el mensaje de baliza mediante una clave de codificación que utiliza el módulo 218 de cifrado/descifrado. 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 104 central, el servidor 120 de autenticación, y/o el dispositivo de control de la red ARA, etc.). En otras implementaciones, el dispositivo 102 solicitante puede enviar la solicitud de combinación o el mensaje de baliza sin cifrado, es decir, en un formato simple.

Adicional o alternativamente, en una implementación, la solicitud de unión puede incluir, pero no se limita a, un identificador del dispositivo 102-3 solicitante 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 102-3 solicitante y conocida por la red ARA, el dispositivo de control de la red ARA, el NMS en la oficina 104 central y/o el servidor 120 de autenticación. En algunas implementaciones, la solicitud de unión puede incluir además un mensaje, un código u otro indicador que indique si el dispositivo 102-3 solicitante es un dispositivo aislado. A modo de ejemplo y no de limitación, se puede determinar que el dispositivo 102-3 solicitante está aislado si el dispositivo 102-3 solicitante es incapaz de unir redes (no mostradas) distintas de la red ARA. Adicional o alternativamente, se puede determinar que el dispositivo 102-3 solicitante está aislado si el dispositivo 102-3 solicitante no detecta otras redes que cubren un área en la que está situado el dispositivo 102-3 solicitante. Adicional o alternativamente, se puede determinar que el dispositivo (102-3) solicitante está aislado si el dispositivo (102-3) solicitante intenta migrar desde otra red (como se muestra en la Fig. 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 102-3 solicitante. Adicional o alternativamente, se puede determinar que el dispositivo 102-3 solicitante está aislado si el dispositivo 102-3 solicitante ha agotado (es decir, ha intentado y no ha podido unirse) todas las redes detectadas en su área excepto la red ARA. Adicional o alternativamente, el dispositivo 102-3 solicitante (es decir, no se ha podido unir) está aislado si la red ARA es la única red que puede proporcionar conectividad entre el dispositivo 102-3 solicitante y uno o más servidores tales como NMS y Servidores DHCP, por ejemplo.

En algunas implementaciones, al enviar la solicitud de unión al dispositivo 102-2 vecino, el dispositivo 102-3 solicitante espera una respuesta de la red ARA a través del dispositivo 102-2 vecino. La respuesta puede indicar si la solicitud de unión del dispositivo 102-3 solicitante para unirse a la red ARA está permitida o rechazada. Si la respuesta indica que la solicitud de unión del dispositivo 102-3 solicitante es rechazada o denegada, el dispositivo 102-3 solicitante puede explorar otra red ARA y enviar una solicitud de unión a la otra red ARA que el dispositivo 102-3 solicitante 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 102-3 solicitante se una a la red ARA, y/o una dirección (por ejemplo, una dirección de Protocolo de Internet (IP) que está asignada al dispositivo 102-3 solicitante. Adicional o alternativamente, 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 rutas designadas por el dispositivo controlador para enrutar paquetes de datos del dispositivo 102-3 solicitante 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 utilizando la clave simétrica del dispositivo 102-3 solicitante. 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 utilizando la clave de grupo asociada a la red ARA.

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

A modo de ejemplo y no de limitación, si la clave simétrica o asimétrica (por ejemplo, la clave pública/privada) del dispositivo 102-3 solicitante es conocida (o se supone que es conocida) solo para el dispositivo 102-3 solicitante y uno o más de otros dispositivos y/o servidores (por ejemplo, el servidor 120 de autenticación, la oficina 104 central y/o el dispositivo de control) que están asociados con la red ARA, el dispositivo 102-3 solicitante y la red ARA pueden autenticarse entre sí utilizando la clave simétrica o asimétrica del dispositivo 102-3 solicitante. Por ejemplo, la red ARA puede autenticar una identidad del dispositivo 102-3 solicitante si el servidor 120 de autenticación, por ejemplo, puede descifrar con éxito una semilla o una firma (que puede estar incluida en la solicitud de unión) que se ha cifrado utilizando la tecla simétrica o asimétrica (por ejemplo, la clave pública) del dispositivo 102-3 solicitante. Además, el dispositivo 102-3 solicitante puede autenticar la red ARA si, por ejemplo, el dispositivo 102-3 solicitante 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 utilizando la clave simétrica o asimétrica (por ejemplo, la clave pública) del dispositivo 102-3 solicitante. En algunas implementaciones, si se utiliza una clave de grupo cifrada como fuente de autentificación de la red ARA, el dispositivo 102-3 solicitante puede determinar además una autenticidad de la red ARA si el dispositivo 102-3 solicitante puede comunicarse con éxito con otros dispositivos en la Red ARA usando la clave de grupo descifrada. En una implementación alternativa, el dispositivo 102-3 solicitante puede realizar una pluralidad de apretones de manos 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 102-2 vecino puede recibir la solicitud de unión enviada o transmitida desde el dispositivo 102-3 solicitante a través del módulo 220 de recepción del dispositivo 102-2 vecino. Si la solicitud de unión o el mensaje de baliza se cifra, el dispositivo 102-2 vecino puede descifrar la solicitud de unión o el mensaje de baliza utilizando el módulo 218 de cifrado/descifrado del dispositivo 102-2 vecino. El dispositivo 102-2 vecino puede analizar la solicitud de combinación (descifrada u originalmente simple si no está cifrada) y determinar a través del módulo 222 de análisis que el dispositivo 102-3 solicitante está solicitando unirse a la red ARA.

En algunas implementaciones, en respuesta a determinar que el dispositivo 102 solicitante solicita unirse a la red ARA del dispositivo 102-2 vecino, el dispositivo 102-2 vecino 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 102-2 vecino 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 224 de retransmisión. A modo de ejemplo y sin limitación, el módulo 224 de retransmisión puede incluir un agente de retransmisión, por ejemplo, un agente de retransmisión DHCPv6, para retransmitir la solicitud de unión (DHCPv6) enviada desde el dispositivo 102-3 solicitante al dispositivo de control. Por ejemplo, el módulo 224 de retransmisión del dispositivo 102-2 vecino 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 102-3 solicitante y retransmitir el paquete de datos al controlador dispositivo directa o indirectamente a través de un dispositivo principal del dispositivo 102-2 vecino.

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

Adicional o alternativamente, independientemente de si la solicitud de unión se retransmite al dispositivo de control o al dispositivo principal del dispositivo 102-2 vecino, el dispositivo 102-2 vecino puede cifrar adicionalmente la solicitud retransmitida utilizando una clave de cifrado del dispositivo 102-2 vecino. 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 102-2 vecino. En algunas otras implementaciones, el dispositivo 102-2 vecino puede retransmitir la solicitud en un formato simple, es decir, sin cifrado. En una implementación, el dispositivo 102-2 vecino 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 102-3 solicitante por la dirección del dispositivo 102-2 vecino) que el dispositivo 102-2 vecino va a retransmitir en nombre del dispositivo 102-3 solicitante. Esto permite reenviar adecuadamente una respuesta desde otros dispositivos o servidores asociados con la red ARA al dispositivo 102-3 solicitante. Por ejemplo, una respuesta o contestación (por ejemplo, para la solicitud de unión) al dispositivo 102-3 solicitante puede usar la dirección del dispositivo 102-2 vecino como la dirección de destino, y solicitar al dispositivo 102-2 vecino que envíe o retransmita la respuesta o contestación al dispositivo 102-3 solicitante en consecuencia.

En algunas implementaciones, el dispositivo 102-2 vecino retransmite la solicitud de unión del dispositivo 102-3 solicitante independientemente de una condición de la red ARA y/o una condición del dispositivo 102-3 solicitante. Adicional o alternativamente, en algunas implementaciones, el dispositivo 102-2 vecino puede recibir una instrucción del dispositivo 102-4 de control, 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 222 de análisis del dispositivo 102-2 vecino puede determinar además si el dispositivo 102-3 solicitante es un dispositivo aislado en función de, por ejemplo, la solicitud de unión recibida por el módulo 220 de recepción. En respuesta a determinar que el dispositivo 102-3 solicitante no es un dispositivo aislado, el dispositivo 102-2 vecino puede enviar una respuesta o retroalimentación al dispositivo 102-3 solicitante que indique que la solicitud de unirse a la red ARA se rechaza porque, por ejemplo, el dispositivo 102-2 vecino ha recibido previamente del dispositivo 102-4 de control 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 102-2 vecino, el dispositivo de control asociado con la red ARA puede determinar si permite o rechaza la solicitud de unión del dispositivo 102-3 solicitante basándose en una condición de la Red ARA. El dispositivo de control puede determinar si permite o rechaza la solicitud de unión del dispositivo 102-3 solicitante usando el módulo 226 de control. 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 periférico (por ejemplo, el dispositivo 102-4) de la red ARA, un enrutador 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 alternativamente en un dispositivo extremo de retorno tal como la oficina 104 central, una raíz de un árbol de enrutamiento de una o más redes ARA manejable por la oficina 104 central, u otro servidor 122 que puede estar afiliado a la oficina 104 central. En algunas implementaciones, el dispositivo de control puede incluir un servidor 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 DHCP o DHCPv6, o incluya una o más funciones del servidor DHCP o DHCPv6, el dispositivo controlador puede retransmitir la solicitud de unión al servidor DHCP o DHCPv6. En algunas implementaciones, el dispositivo de control puede incluir una combinación de uno o más dispositivos que incluyen el servidor DHCP o DHCPv6, un dispositivo raíz, un dispositivo periférico, un enrutador, un dispositivo extremo de retorno como la oficina 104 central 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, enrutador de borde u otro dispositivo de borde de la red ARA, que acopla la red ARA a la oficina 104 central a través de la red de retorno 106.

En algunas implementaciones, en respuesta a la recepción de la solicitud retransmitida desde el dispositivo 102-2 vecino, el dispositivo 102-4 de control puede determinar si permite o rechaza la solicitud del dispositivo 102-3 solicitante en función de si una carga en la red ARA excede un umbral predeterminado. A modo de ejemplo y sin limitación, el dispositivo 102-4 de control puede determinar si permite o rechaza la solicitud del dispositivo 102-3 solicitante en función de 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 el alojamiento). Adicional o alternativamente, el dispositivo 102-4 de control puede determinar si permite o rechaza la solicitud del dispositivo 102-3 solicitante en función de 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 102-4 de control puede rechazar la (DHCP o DHCPv6) solicitud de unión del dispositivo 102-3 solicitante. Alternativamente, en algunas implementaciones, el dispositivo 102-4 de control puede determinar además si el dispositivo 102-4 solicitante es un dispositivo aislado en función de, por ejemplo, información en la solicitud recibida. La información en la solicitud recibida puede incluir, por ejemplo, un indicador que indique que el dispositivo 102-3 solicitante es un dispositivo aislado. En respuesta a determinar que el dispositivo 102-3 solicitante es un dispositivo aislado, el dispositivo 102-4 de control puede permitir que el dispositivo 102-3 solicitante 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 102-4 de control puede determinar además una autenticidad del dispositivo 102-3 solicitante usando el módulo 228 de autenticación. Por ejemplo, el módulo 228 de autenticación del dispositivo 102-4 de control puede determinar una autenticidad del dispositivo 102-3 solicitante en base al identificador del dispositivo 102-3 solicitante o la firma de autenticación incluida en la solicitud recibida. Adicional o alternativamente, el dispositivo 102-4 de control puede analizar la solicitud y enviar el identificador y/o la firma de autenticación del dispositivo 102-3 solicitante 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 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 104 central, por ejemplo. En una implementación, el servidor de seguridad o el servidor AAA 120 pueden estar ubicados fuera de la red ARA. En algunas implementaciones, el servidor de seguridad o el servidor AAA 120 puede ser otro nodo o dispositivo (por ejemplo, el dispositivo 102-1) dentro de la misma red ARA del dispositivo 102-4 de control. El dispositivo 102-4 de control puede enviar información que incluye el identificador y/o la firma de autenticación del dispositivo 102-3 solicitante al servidor de seguridad o al servidor 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 AAA se usa como ejemplo para describir operaciones de autenticación de identidades de dispositivos que unen una o más redes ARA.

En una implementación, al autenticar con éxito la identidad del dispositivo 102-3 solicitante basado en el identificador y/o la firma de autenticación del dispositivo 102-3 solicitante, por ejemplo, el servidor AAA 120 puede enviar un mensaje al dispositivo de control 102-4 o el servidor DHCP asociado o conectado con el dispositivo 102-4 de control, que indica que la identidad del dispositivo 102-3 solicitante se ha autenticado satisfactoriamente. Adicional o alternativamente, en algunas implementaciones, el servidor AAA 120 puede enviar además una clave de grupo (por ejemplo, una clave de capa de enlace de grupo) asociada con la red ARA al dispositivo 102-4 de control o el servidor DHCP del dispositivo de control 102- 4. Adicional o alternativamente, el servidor 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 102-4 de control o el servidor DHCP asociado con el dispositivo 102-4 de control. En una implementación, el dispositivo 102-4 de control 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 102-4 de control puede no tener información de la clave pública o simétrica del dispositivo 102-3 solicitante. En ese caso, el

servidor AAA 120 puede cifrar la clave de grupo usando una clave pública o simétrica del dispositivo 102-3 solicitante, y cifrar el mensaje (incluyendo la clave de grupo cifrada) usando la clave de grupo asociada con la red ARA al dispositivo 102-4 de control, que puede reenviar la clave de grupo que se ha cifrado utilizando la clave pública o simétrica del dispositivo 102-3 solicitante al dispositivo 102-3 solicitante.

En una implementación, si el dispositivo 102-4 de control y el servidor DHCP son dispositivos separados, el servidor AAA 120 puede enviar el mensaje al servidor DHCP asociado con el dispositivo 120-4 de control (por ejemplo, después de que se haya enviado la solicitud de autenticación desde el Servidor DHCP o desde el dispositivo 102-4 de control a través del servidor DHCP). En respuesta a la recepción del mensaje, el servidor DHCP puede analizar el mensaje y determinar si la identidad del dispositivo 102-3 solicitante está autenticada. Adicional o alternativamente, el servidor DHCP puede retransmitir el mensaje al dispositivo 102-4 de control. En algunas implementaciones, el servidor AAA 120 puede enviar el mensaje al dispositivo 102-4 de control directamente si la solicitud de autenticación fue enviada desde el dispositivo 102-4 de control (o desde el dispositivo 102-4 de control a través del servidor DHCP si el dispositivo 102-4 de control y el servidor DHCP son dispositivos separados). Independientemente de si el mensaje se retransmite desde el servidor DHCP o se envía directamente desde el servidor AAA 120, en una implementación, en respuesta a la recepción del mensaje del servidor AAA 120, el dispositivo 102-4 de control puede analizar el mensaje y determinar si la identidad del dispositivo 102-3 solicitante está autenticada. En respuesta a la determinación de que la identidad del dispositivo 102-3 solicitante está autenticada, el dispositivo 102-4 de control puede enviar un mensaje, que puede o no cifrarse utilizando una clave pública o clave simétrica del dispositivo 102-3 solicitante (que puede depender de si el dispositivo 102-4 de control tiene la clave pública o simétrica del dispositivo 102-3 solicitante, por ejemplo) como se describe en las implementaciones anteriores, al dispositivo 102-3 solicitante que indica que la identidad del dispositivo 102-3 solicitante está autenticado y/o el dispositivo 102-3 solicitante puede unirse a la red ARA. Adicional o alternativamente, en algunas implementaciones, el dispositivo 102-4 de control puede cifrar el mensaje usando la clave de grupo asociada con la red ARA, que posteriormente puede ser descifrada y analizada por el dispositivo 102-2 vecino al dispositivo 102-3 solicitante. En una implementación, el mensaje puede incluir además, por ejemplo, una clave de grupo asociada con la red ARA y otra información que puede o no cifrarse usando la clave pública o simétrica del dispositivo 102-3 solicitante, tal como la clave de grupo cifrada recibida del servidor AAA 120, por ejemplo. En algunas implementaciones, en respuesta a la recepción del mensaje, el dispositivo 102-3 solicitante puede descifrar el mensaje si está cifrado (por ejemplo, usando la clave pública o simétrica del dispositivo 102-3 solicitante) y recuperar la clave de grupo asociada con la red ARA. Adicional o alternativamente, el dispositivo 102-3 solicitante puede descifrar la clave de grupo cifrada (tal como la clave de grupo cifrada en el servidor AAA 120 usando la clave pública o simétrica del dispositivo 102-3 solicitante) para recuperar la clave de grupo. El dispositivo 102-3 solicitante 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 102-4 de control (o el servidor de DHCP asociado con el dispositivo 102-4 de control) puede enviar además una solicitud de registro al NMS utilizando el módulo 216 de envío. La solicitud de registro puede incluir, por ejemplo, el identificador del dispositivo 102-3 solicitante, que puede estar firmado o cifrado usando una clave privada (de claves públicas/privadas) asociada con el dispositivo 102-4 de control, la clave de grupo asociada con la red ARA, y/o la clave asociada con el dispositivo 102-3 solicitante. En una implementación, el dispositivo 102-4 de control puede enviar la solicitud de registro al NMS en un formato simple, no cifrado.

Tras recibir la solicitud de registro del dispositivo 102-4 de control, el NMS puede descifrar el mensaje si el mensaje está cifrado, analizar el mensaje y obtener el identificador del dispositivo 102-3 solicitante. En algunas implementaciones, el NMS puede recuperar adicionalmente información asociada con el dispositivo 102-3 solicitante 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 102-3 solicitante 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 102-3 solicitante, un tipo de red ARA al que el dispositivo 102-3 solicitante solicita unirse, etc. Adicional o alternativamente, el NMS puede enviar la información de configuración o parámetros al dispositivo 102-4 de control o al servidor de DHCP del dispositivo 102-4 de control.

En una implementación, en respuesta a la recepción de la información de configuración o parámetros del NMS, el módulo 230 de asignación de direcciones del dispositivo 102-4 de control (o el servidor DHCP) puede determinar una nueva dirección (por ejemplo, una nueva dirección IP tal como dirección IPv6) para el dispositivo 102-3 solicitante. En una implementación, el dispositivo 102-4 de control (o el servidor DHCP) puede determinar la nueva dirección basándose en un prefijo asignado a un agente de retransmisión que el dispositivo 102-4 de control (o el servidor DHCP) puede emplear, por ejemplo. Adicional o alternativamente, el dispositivo 102-4 de control (o el servidor DHCP) puede determinar la nueva dirección basándose en un prefijo designado o compartido por dispositivos en la red ARA del dispositivo 102-4 de control. En una implementación, la nueva dirección que está asignada al dispositivo 102-3 solicitante puede incluir el prefijo que está asignado al agente de retransmisión del dispositivo 102-4 de control (o el servidor DHCP), o designado o compartido por cada dispositivo en la red ARA. En algunas implementaciones, el dispositivo 102-4 de control (o el servidor DHCP) puede generar adicionalmente un número aleatorio y usar este número aleatorio para el resto de la nueva dirección. Adicional o alternativamente, el dispositivo 102-4 de control (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 102-4 de control

(o el servidor de DHCP) puede entonces seleccionar aleatoria o secuencialmente una dirección de la pluralidad de direcciones para asignar al dispositivo 102-3 solicitante.

Adicional o alternativamente, en algunas implementaciones, al determinar la nueva dirección a asignar al dispositivo 102-3 solicitante, el dispositivo 102-4 de control (o el servidor DHCP) puede verificar adicionalmente esta nueva dirección con un servidor DNS (es decir, Nombre de Sistema de nombre de dominio) para determinar si esta nueva dirección está actualmente asignada a cualquier otro dispositivo. En una implementación, el dispositivo 102-4 de control (o el servidor DHCP) puede enviar la nueva dirección y el identificador del dispositivo 102-3 solicitante al servidor DNS. Si el dispositivo 102-4 de control (o el servidor DHCP) recibe una respuesta del servidor 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 102-3 solicitante y verificar la nueva dirección redeterminada con el servidor DNS para garantizar la disponibilidad de la nueva dirección redeterminada. Si la nueva dirección o la nueva dirección redeterminada está disponible, el servidor DNS puede registrar la nueva dirección o la nueva dirección redeterminada con el identificador del dispositivo 102-3 solicitante y reservar la nueva dirección o la nueva dirección redeterminada para el dispositivo 102-3 solicitante.

En una implementación, al confirmar la nueva dirección que se asignará al dispositivo 102-3 solicitante, el dispositivo 102-4 de control puede proporcionar una respuesta (por ejemplo, una respuesta DHCP) al dispositivo 102-3 solicitante. 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 102-3 solicitante se una o configure con la red ARA. En una implementación, el dispositivo 102-4 de control (o el servidor DHCP) puede enviar la respuesta al dispositivo 102-3 solicitante. En algunas implementaciones, con o sin el conocimiento de una dirección global del dispositivo 102-3 solicitante (por ejemplo, dado que la nueva dirección todavía no se ha asignado al dispositivo 102-3 solicitante), el dispositivo 102-4 de control (o el Servidor DHCP) puede enviar la respuesta al dispositivo 102-3 solicitante a través del dispositivo 102-2 vecino (y el enrutador dirigiendo la red ARA si el dispositivo 102-4 de control está situado fuera de la red ARA). Por ejemplo, el dispositivo 102-4 de control (o el servidor DHCP) puede enviar la respuesta al dispositivo 102-2 vecino y solicitar que el dispositivo 102-2 vecino retransmita la respuesta al dispositivo 102-3 solicitante. El dispositivo 102-2 vecino, que ha establecido comunicación con el dispositivo 102-3 solicitante, puede retransmitir la respuesta al dispositivo 102-3 solicitante a través de un mensaje que utiliza el protocolo DHCPv6 o un mensaje de baliza. Adicional o alternativamente, el dispositivo 102-2 vecino puede transmitir la respuesta en una vecindad de la misma, y el dispositivo 102-3 solicitante, que está cerca del dispositivo 102-2 vecino, 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 102-3 solicitante 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 102-3 solicitante puede unirse a una topología de enrutamiento en la red ARA al decidir qué ruta de enrutamiento y/o dispositivo vecino usar si hay más de una ruta de enrutamiento y/o dispositivos vecinos disponibles. Adicional o alternativamente, el dispositivo 102-3 solicitante puede enviar un mensaje al nodo raíz de la red ARA para notificar su llegada a la red ARA, por ejemplo. El dispositivo 102-3 solicitante 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 102-3 solicitante 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 102-3 solicitante puede reenviar el mensaje al nodo raíz. El dispositivo 102-3 solicitante puede reenviar el mensaje para un número predeterminado de fallas de recepción de acuse de recibo. Adicional o alternativamente, el dispositivo 102-3 solicitante puede seleccionar una ruta de enrutamiento diferente y/o un dispositivo 102 vecino para enviar o retransmitir el mensaje al nodo raíz. Tras recibir un acuse de recibo del nodo raíz, el dispositivo 102-3 solicitante puede comenzar a realizar operaciones normales en la red ARA, que incluyen, por ejemplo, enrutamiento y/o reenvío de paquetes que no están destinados al dispositivo 102-3 solicitante, procesamiento de paquetes dirigido al dispositivo 102-3 solicitante, respondiendo por paquetes (si se solicitan) que están destinados al nodo 102-3 solicitante, etc. Si no se recibe acuse de recibo desde el nodo raíz para un número predeterminado de reintentos, el dispositivo 102-3 solicitante 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 del dispositivo de ejemplo

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 (donde el dispositivo 102 está actualmente conectado) a otra red ARA en base a 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 degradada, por ejemplo, por debajo de un umbral de calidad predeterminado. Adicional o alternativamente, el dispositivo 102 puede migrar de la

red ARA a otra red ARA si falla el enrutador de la red ARA. Adicional o alternativamente, el dispositivo 102 puede, mientras está conectado a la red ARA actual, escucharlo en un entorno del mismo, y detectar o descubrir la existencia de otras redes ARA adyacentes. El dispositivo 102 puede aprender sobre el rendimiento tal como calidad de servicio (QoS) ofrecido por estas redes adyacentes. El dispositivo 102 puede migrar desde 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 el dispositivo 102 está actualmente conectado. En una implementación, el dispositivo 102 puede seleccionar una red ARA adyacente para la migración en base a una o más políticas o criterios. 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, como QoS, tiempo o latencia de respuesta, rendimiento, tasa de caída de paquetes, etc., como en comparación con la red ARA a la que el dispositivo 102 está actualmente conectado.

Adicional o alternativamente, el dispositivo 102 puede ser forzado por el dispositivo 102-4 de control (o un dispositivo 102 en la red ARA, como el enrutador 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, balanceo de carga entre la red ARA y la otra red, etc. Adicional o alternativamente, el dispositivo 102-4 de control puede forzar al dispositivo 102 a migrar desde 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 102-4 de control puede necesitar forzar a algún dispositivo 102 a abandonar la red ARA o migrar a otra red ARA, el dispositivo 102-4 de control puede determinar qué 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 102-4 de control puede seleccionar uno o más dispositivos para salir o migrar en función de la información asociada con cada dispositivo en la red ARA. En una implementación, el dispositivo 102-4 de control puede almacenar la información asociada con cada dispositivo 102 en la red ARA cuando el dispositivo respectivo 102 se une a la red ARA.

Adicional o alternativamente, el dispositivo 102-4 de control puede inspeccionar cada dispositivo en la red ARA en respuesta a la decisión de forzar a uno o más dispositivos 102 en la red ARA a abandonar o migrar a otra red ARA. Adicional o alternativamente, el dispositivo 102-4 de control puede consultar los dispositivos 102 en la red ARA para determinar cuál de ellos es capaz de abandonar o migrar desde la red ARA. Adicional o alternativamente, el dispositivo 102-4 de control puede recuperar la información de topología asociada con cada dispositivo 102 en la red ARA desde la oficina 104 central o cualquier dispositivo o nodo que esté jerárquicamente en perspectiva desde el dispositivo 102-4 de control. 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 hijo (es decir, dispositivo que es jerárquicamente descendente; desde el dispositivo respectivo 102), cuántos dispositivos hijo 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 102-4 de control 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 102-4 de control puede seleccionar uno o más dispositivos 102 que no están aislados como se indica en la información. Adicional o alternativamente, el dispositivo 102-4 de control puede seleccionar uno o más dispositivos 102 que tienen menos dispositivos hijos, por ejemplo, menos de un número de umbral predeterminado. Adicional o alternativamente, el dispositivo 102-4 de control puede seleccionar un número predeterminado (por ejemplo, uno, dos, etc.) de los primeros pocos dispositivos 102 que tienen menos de un número de umbral de dispositivos hijo. Adicional o alternativamente, el dispositivo 102-4 de control puede seleccionar uno o más dispositivos que están más alejados del dispositivo 102-4 de control basándose en la información de enrutamiento, por ejemplo.

Después de seleccionar el uno o más dispositivos 102 para salir o migrar de la red ARA, el dispositivo 102-4 de control puede enviar una instrucción o solicitud al uno o más dispositivos 102 para abandonar o migrar desde la red ARA. En una implementación, el dispositivo 102-4 de control 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 se aislaría si se viera obligado a abandonar la red ARA actual). En algunas implementaciones, el dispositivo 102-4 de control 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 102-4 de control puede seleccionar el dispositivo 102-5 para abandonar o migrar desde 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 el dispositivo 102-5 puede migrar. Por ejemplo, el dispositivo 102-5 puede usar el módulo 212 de descubrimiento y el módulo 214 de difusión 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 102-4 de control, rechazando abandonar la red ARA del dispositivo 102-4 de control, ya que hacerlo así, resultaría en que el dispositivo 102-5 se convirtiera en aislado.

Alternativamente, 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 102-4 de control que indica que el dispositivo 102-5 no puede abandonar o migrar desde la red ARA. Adicional o alternativamente, 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 102-4 de control de que el dispositivo 102-5 no puede salir o migrar de la red ARA. En una implementación, el dispositivo 102-5 puede verse obligado a abandonar o migrar desde la red ARA independientemente de las consecuencias de dicha migración, excepto que el dispositivo 102-5 no se verá obligado a abandonar o migrar de la red ARA si haciéndolo así, el dispositivo 102-5 se aislara.

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 puede o no cifrarse utilizando 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, dado que el dispositivo 102-5 se ha registrado con éxito con el NMS previamente cuando se une a la red ARA del dispositivo 102-4 de control, el dispositivo 102-5 puede estar exento de todo o parte de un proceso de autenticación como se describe anteriormente (proporcionando 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 IPv6) designado a la otra red ARA. Tras recibir la nueva dirección, el dispositivo 102-5 puede actualizar su dirección anterior (es decir, una dirección previamente asignada al dispositivo 102-5 por el dispositivo 102-4 de control) con la nueva dirección en un nivel de aplicación tal como en el Instituto Nacional de Estándares Americanos (ANSI) C12.22, DNS, etc.

En una implementación, durante un período de tiempo de la migración y antes de que se complete la migración, el dispositivo 102-5 puede mantener la conexión o la unión a la red ARA a la que está conectado actualmente u originalmente. Por ejemplo, el dispositivo 102-5 todavía puede realizar operaciones normales en la red ARA actual, incluyendo enrutamiento y reenvío de paquetes no destinados al dispositivo 102-5, procesamiento de paquetes dirigidos al dispositivo 102-5, respondiendo por los paquetes destinados a el dispositivo 102-5 - si se solicita - a través de la red ARA actual, etc. Adicional o alternativamente, el dispositivo 102-5 puede seleccionar un dispositivo 102 vecino de la nueva red ARA y emplear este dispositivo 102 vecino como un dispositivo de retransmisión y/o reenvío para paquetes de datos. Adicional o alternativamente, el dispositivo 102-5 aún puede recibir paquetes de datos destinados a su dirección anterior 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 anterior y continuar procesando datos o paquetes de datos dirigidos a su dirección anterior como es habitual, manteniendo así 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 principales de la red ARA de la que está migrando, el dispositivo 102-5 puede desconectar todos los paquetes ascendentes (paquetes de datos transmitidos a dispositivos en un nivel jerárquico superior de la red ARA) desde su búfer, por ejemplo. En algunas implementaciones, el dispositivo 102-5 puede reenviar los paquetes de datos recibidos a la red ARA de la que está migrando (si aún está conectado) durante el período de tiempo de la migración. En una implementación, si el dispositivo 102-5 recibe su nueva dirección y ahora está conectado a la otra red ARA (es decir, la nueva red ARA), el dispositivo 102-5 puede “tunelizar” los paquetes de datos almacenados, es decir, paquetes de datos proveniente de su “antigua” red ARA, 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, al conectarse o migrar con éxito a la nueva red ARA, el dispositivo 102-5 se separa o abandona la antigua red ARA. En una implementación, el dispositivo 102-5 puede enviar un mensaje al nodo raíz de la antigua red ARA para notificar o anunciar su salida de la antigua red ARA. Adicional o alternativamente, el dispositivo 102-5 puede enviar mensajes (que indican su salida de la antigua red ARA) a uno o más dispositivos 102 en la antigua red ARA que reenvían y/o enrutan 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 antigua red ARA) pueden o no solicitar un acuse de recibo desde el nodo raíz y/o los otros dispositivos 102 en la antigua red ARA. 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 antigua red ARA para aumentar o asegurar la probabilidad de que el nodo raíz y/o los otros dispositivos 102 reciban los mensajes.

Adicional o alternativamente, el dispositivo 102-5 puede detener el procesamiento de cualquier paquete de datos que no esté destinado a su dirección anterior. 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 anterior del dispositivo 102-5, y/o un paquete de datos (que puede o no estar destinado) a la dirección anterior 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. Adicional o alternativamente, 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 anterior 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. Adicional o alternativamente, 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 antigua red ARA y esté realizando operaciones normales en la nueva red ARA, el dispositivo 102-5 todavía puede aceptar paquetes destinados a la dirección anterior durante un período de tiempo predeterminado que pueden estar por omisión en la red ARA vieja o nueva, o puede ser predefinido por un administrador de la red ARA vieja o nueva. El dispositivo 102-5 puede procesar paquetes de datos destinados a su dirección anterior (y/o paquetes de datos no destinados a su dirección anterior) de acuerdo con las implementaciones anteriores como se describió anteriormente.

En algunas implementaciones, la dirección anterior 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 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 enrutamiento autónoma de una infraestructura de medición avanzada (AMI), la presente divulgación no está limitada 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 a algunos de los dispositivos móviles conectados a su red a abandonar o migrar a otra red celular, por lo tanto, realizando balanceo de carga para su red controlada.

Métodos de ejemplo

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

Los métodos 300, 400 y 500 se describen en el contexto general de instrucciones ejecutables por ordenador. Generalmente, 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 en particular. Los métodos también se pueden practicar en un entorno de cómputo distribuido donde las funciones se realizan mediante dispositivos de procesamiento remoto que están enlazados 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 de ejemplo 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, los bloques individuales pueden omitirse del método. 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 FIG. 3, en el bloque 302, el dispositivo 102-3 solicitante puede desear unirse a una red que cubre un área donde se encuentra el dispositivo 102-3 solicitante. El dispositivo 102-3 solicitante puede descubrir

el dispositivo 102-2 vecino 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 102-2 vecino.

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

En el bloque 306, en respuesta a determinar que el dispositivo 102-3 solicitante solicita unirse a la red, el dispositivo 102-2 vecino puede opcionalmente filtrar la solicitud de unión. En una implementación, el dispositivo 102-2 vecino puede determinar si retransmitir la solicitud de unión a otros dispositivos de la red. Por ejemplo, el dispositivo 102-2 vecino puede haber recibido una instrucción o solicitud del dispositivo 102-4 de control de que no se pueden aceptar dispositivos a excepción de los dispositivos aislados en la red por razones administrativas o de red tales como sobrecarga o sobrecarga de la red. En este caso, el dispositivo 102-2 vecino puede determinar si el dispositivo 102-3 solicitante es un dispositivo aislado basado en, por ejemplo, información incluida en la solicitud de unión. En una implementación, si el dispositivo 102-2 vecino ha recibido la instrucción o solicitud de que no se acepten dispositivos a excepción de dispositivos aislados en la red y el dispositivo 102-3 solicitante no es un dispositivo aislado, el dispositivo 102-2 vecino puede enviar una respuesta al dispositivo 102-3 solicitante, que indica que la solicitud de unión es rechazada. De lo contrario, el dispositivo 102-2 vecino puede prepararse para retransmitir la solicitud de unión del dispositivo 102-3 solicitante a otros dispositivos de la red.

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

En el bloque 310, el dispositivo 102-2 vecino puede retransmitir la solicitud de unión al dispositivo 102-4 de control o al dispositivo principal del dispositivo 102-2 vecino en función de si el dispositivo 102-2 vecino 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 102-2 vecino, el dispositivo 102-4 de control puede determinar si permite o rechaza la solicitud de unión del dispositivo 102-3 solicitante. En una implementación, el dispositivo 102-4 de control puede determinar si permite la solicitud de unión en función de una condición de la red y/o una condición del dispositivo 102-3 solicitante. Si el dispositivo 102-4 de control determina rechazar la solicitud de unión del dispositivo 102-3 solicitante, el dispositivo 102-4 de control puede enviar una respuesta al dispositivo 102-3 solicitante a través del dispositivo 102-2 vecino, lo que indica que el dispositivo 102-4 de control o la red no puede permitir que el dispositivo 102-3 solicitante se una.

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

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

En el bloque 318, en respuesta a la recepción de un mensaje del servidor 120 de autenticación, el dispositivo 102-4 de control puede determinar si la autenticación de la identidad del dispositivo 102-3 solicitante es exitosa. Si falla, el dispositivo 102-4 de control puede enviar una respuesta al dispositivo 102-3 solicitante a través del dispositivo 102-2 vecino, indicando que la solicitud de unión del dispositivo 102-3 solicitante es denegada. En respuesta a la determinación de que la identidad del dispositivo 102-3 solicitante se autentica con éxito, el dispositivo 102-4 de control puede enviar una respuesta de admisión al dispositivo 102-3 solicitante a través del dispositivo 102-2 vecino que incluye un mensaje que indica que se permite la solicitud de unión del dispositivo 102-3 solicitante. En una

implementación, la respuesta puede incluir, además, pero no se limita a, una clave de grupo asociada con la red que puede o no cifrarse en el servidor de autenticación utilizando la clave pública o simétrica del dispositivo 102-3 solicitante. Adicional o alternativamente, en algunas implementaciones, el dispositivo 102-4 de control puede cifrar la respuesta usando una clave pública o simétrica del dispositivo 102-3 solicitante si el dispositivo 102-4 de control conoce la clave pública o simétrica del dispositivo 102- 3 solicitante, por ejemplo, desde el servidor 120 de autenticación. Adicional o alternativamente, en una implementación, el dispositivo 102-4 de control puede cifrar la clave de grupo (y/u otra información relacionada para unirse a la red) usando la clave pública o simétrica del dispositivo 102-3 solicitante (si esta clave pública o simétrica es conocida por el dispositivo 102-4 de control) 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 102-4 de control puede cifrar la clave de grupo y el mensaje usando la clave pública o simétrica del dispositivo 102-3 solicitante, y cifrar adicionalmente la clave de grupo cifrada, el mensaje cifrado y/u otra información (tal como información que permite enrutar la respuesta al dispositivo 102-3 solicitante, por ejemplo, una dirección del dispositivo 102-2 vecino y/o una identidad del dispositivo 102-3 solicitante, etc.) usando la clave de grupo.

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

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

En el bloque 322, el dispositivo 102-3 solicitante recibe la respuesta retransmitida desde el dispositivo 102-2 vecino 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 102-3 solicitante 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 102-4 de control puede enviar opcionalmente una solicitud de registro al NMS para registrar el dispositivo 102-3 solicitante con la NMS o la oficina 104 central. La solicitud de registro puede incluir, pero no está limitada, a un identificador del dispositivo 102-3 solicitante.

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

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

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

En el bloque 332, el dispositivo 102-3 solicitante se une y se registra exitosamente 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 102-3 solicitante puede autentificar adicionalmente la red si la clave simétrica o asimétrica del dispositivo 102-3 solicitante es conocida solamente a sí misma y a uno o más dispositivos y/o servidores autorizados (por ejemplo, el servidor 120 de autenticación, la oficina 104 central, y/o el dispositivo 102-4 de control). 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 102-3 solicitante. El dispositivo 102-3 solicitante puede por lo tanto autenticar la red si el dispositivo 102-3 solicitante 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 102-3 solicitante no puede comunicar datos con otros dispositivos usando la clave de grupo descifrada, el dispositivo 102-3 solicitante puede determinar que la autenticación de la red falla, y abandonar (o desconectarse) de la red en consecuencia.

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

En el bloque 404, en respuesta a determinar que la solicitud es una solicitud de unión, el dispositivo 102-4 de control puede determinar si la red tiene capacidad para alojar dispositivos adicionales. Por ejemplo, el dispositivo 102-4 de control 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 está limitada, 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 102-4 de control determina que la red puede acomodar dispositivos adicionales, por ejemplo, la carga es menor que el umbral predeterminado, el dispositivo 102-4 de control puede proceder a procesar la solicitud de unión del dispositivo 102-3 solicitante como se describe en las realizaciones anteriores, por ejemplo, la FIG. 3, con otros dispositivos y/o servidores.

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

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

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

Con referencia de nuevo a la FIG. 5, en el bloque 502, el dispositivo 102-4 de control decide forzar a uno o más dispositivos 102 a abandonar o migrar desde la red. El dispositivo 102-4 de control puede tomar esta decisión basándose en una o más razones tales como el equilibrio 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 102-4 de control 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 hijo, la selección de dispositivos que están comunicativamente más alejados del dispositivo de control.

En el bloque 506, al seleccionar el uno o más dispositivos para salir o migrar, el dispositivo 102-4 de control 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 una o más redes (otras de las que la red el dispositivo 102-5 es actualmente miembro) existen en un área en la que se encuentra el dispositivo 102-5. El dispositivo 102-5 puede enviar un mensaje al dispositivo 102-4 de control 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 una o más redes (distintas de la red en la que el dispositivo 102-5 es actualmente un miembro) existen, el dispositivo 102-5 puede comenzar a unir una de las una o más redes como se describe anteriormente con respecto a la FIG. 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 finalización de la migración, en respuesta a recibir paquetes de datos destinados a una dirección “anterior” (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 soltar los paquetes de datos, o enviar los paquetes de datos a otros dispositivos en la red a los que el dispositivo 102-5 todavía está conectado.

En el bloque 514, al obtener con éxito la nueva dirección y conectarse 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 FIG. 5 describe que el dispositivo 102-5 puede ser forzado u ordenado a abandonar o migrar desde la red ARA por el dispositivo 102-4 de control; en algunas implementaciones, el dispositivo 102-5 en realidad comienza por sí solo a abandonar o migrar desde 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 en base a 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 degradada, por ejemplo, por debajo de un umbral de calidad predeterminado. Adicional o alternativamente, el dispositivo 102-5 puede migrar de la red ARA a otra red ARA si falla el enrutador de la red ARA. Adicional o alternativamente, el dispositivo 102-5 puede, mientras esté conectado a la red ARA actual, escucharlo en un entorno del mismo, y detectar o descubrir la existencia de otras redes ARA adyacentes. El dispositivo 102-5 puede aprender sobre el rendimiento/calidad del servicio ofrecido por estas redes adyacentes. El dispositivo 102-5 puede migrar desde 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 conectado actualmente el dispositivo 102-5.

Cualquiera de los actos de cualquiera de los métodos descritos en este documento puede implementarse 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 este documento puede implementarse bajo el control de uno o más procesadores configurados con instrucciones ejecutables que pueden almacenarse en uno o más medios legibles por ordenador, como uno o más medios de almacenamiento informático.

Conclusión

Aunque la invención se ha descrito en un lenguaje específico para las características estructurales y/o los actos metodológicos, debe entenderse que la invención no está necesariamente limitada a las características o actos específicos descritos. Por el contrario, las características y actos específicos se divulgan como formas de ejemplo de implementación de la invención.

REIVINDICACIONES

1. Un dispositivo (102-4) de control de una red de área de enrutamiento autónoma, comprendiendo el dispositivo (102-4) de control:

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

recibir una solicitud de un dispositivo (102-3) solicitante para unirse a la red de área de enrutamiento autónomo; y

en respuesta a la recepción de la solicitud:

determinar, en base a la información incluida en la solicitud, si el dispositivo (102-3) solicitante es un dispositivo aislado, en el que el dispositivo (102-3) solicitante es un dispositivo aislado si es incapaz de unir redes que no sean la red de área de enrutamiento autónoma;
controlar un rechazo o la aceptación de la admisión del dispositivo (102-3) solicitante a la red de área de enrutamiento autónoma en función de si el dispositivo (102-3) solicitante es un dispositivo aislado; y
en respuesta a determinar que el dispositivo (102-3) solicitante es un dispositivo aislado:

admitir el dispositivo solicitante a la red independientemente de si una carga en la red es mayor o igual a un umbral predeterminado de acomodación; y
forzar a uno o más dispositivos que están actualmente incluidos en la red a abandonar o migrar desde la red, donde obligar a uno o más dispositivos a abandonar o migrar comprende:

seleccionar uno o más dispositivos basados en una o más estrategias heurísticas; y
enviar una instrucción o solicitud a uno o más dispositivos para que abandonen o migren de la red.

2. El dispositivo (102-4) de control según la reivindicación 1, en el que la solicitud comprende un indicador o un mensaje que indica si el dispositivo (102-3) solicitante es un dispositivo aislado.

3. El dispositivo (102-4) de control según la reivindicación 1, comprendiendo, además, los actos:

determinar si la carga en la red es mayor o igual que el umbral predeterminado para la acomodación; y
en respuesta a determinar que la carga en la red es mayor o igual que el umbral predeterminado de acomodación:

seleccionar un dispositivo que está actualmente incluido en la red para abandonar la red; y
enviar un mensaje al dispositivo seleccionado para solicitar que el dispositivo seleccionado salga de la red.

4. El dispositivo (102-4) de control según la reivindicación 1, comprendiendo, además, los actos:

determinar si la carga en la red es mayor o igual al umbral predeterminado de acomodación; y
en respuesta a determinar que la carga en la red es mayor o igual que el umbral predeterminado de acomodación:

transmitir un mensaje para consultar qué dispositivos que están actualmente incluidos en la red son capaces de migrar a otra red;
recibir una o más respuestas de uno o más dispositivos que indican que uno o más dispositivos son capaces de migrar a otra red;
seleccionar un dispositivo del uno o más dispositivos para salir de la red; y
enviar un mensaje al dispositivo seleccionado para solicitar que el dispositivo seleccionado salga de la red.

5. El dispositivo (102-4) de control según la reivindicación 1, comprendiendo, además, los actos:

determinar si la carga en la red es mayor o igual que el umbral predeterminado de acomodación; y
en respuesta a determinar que la carga en la red es mayor o igual que el umbral predeterminado de acomodación:

determinar una pluralidad de dispositivos incluidos en la red que son capaces de unirse a otras redes en función de la información almacenada asociada a cada dispositivo de la red;
seleccionar un dispositivo de la pluralidad de dispositivos incluidos en la red que son capaces de unirse a las otras redes; y
solicitar u obligar al dispositivo seleccionado a abandonar la red.

6. El dispositivo (102-4) de control según la reivindicación 1, comprendiendo, además, los actos:

permitir que la solicitud del dispositivo (102-3) solicitante se una a la red; y
en respuesta a permitir la solicitud:

enviar: una clave de grupo asociada a la red; información de configuración para que el dispositivo (102-3) solicitante se una a la red; y una dirección global asignada al dispositivo (102-3) solicitante.

7. El dispositivo (102-4) de control de acuerdo con la reivindicación 6, en el que la etapa de recibir comprende recibir la solicitud del dispositivo (102-3) solicitante a través de uno o más dispositivos intermedios en la red; y la etapa de envío comprende enviar al dispositivo (102-3) solicitante a través de uno o más dispositivos intermedios:

la clave de grupo asociada a la red;
la información de configuración para que el dispositivo (102-3) solicitante se una a la red; y
la dirección global asignada al dispositivo (102-3) solicitante.

8. El dispositivo (102-4) de control según la reivindicación 1, comprendiendo, además, los actos:

determinar si una carga en la red es mayor o igual que un umbral predeterminado de acomodación; y
en respuesta a determinar que el dispositivo (102-3) solicitante no es un dispositivo aislado y en respuesta a determinar que la carga en la red es mayor o igual al umbral predeterminado de acomodación:

rechazar la solicitud del dispositivo solicitante (102-3) para unirse a la red.

9. El dispositivo (102-4) de control según la reivindicación 1, comprendiendo, además, los actos:

determinar si una carga en la red es menor que un umbral predeterminado de acomodación; y
en respuesta a determinar que la carga en la red es menor que el umbral predeterminado de acomodación:

admitir que el dispositivo (102-3) solicitante se una a la red independientemente de si el dispositivo (102-3) solicitante es un dispositivo aislado.

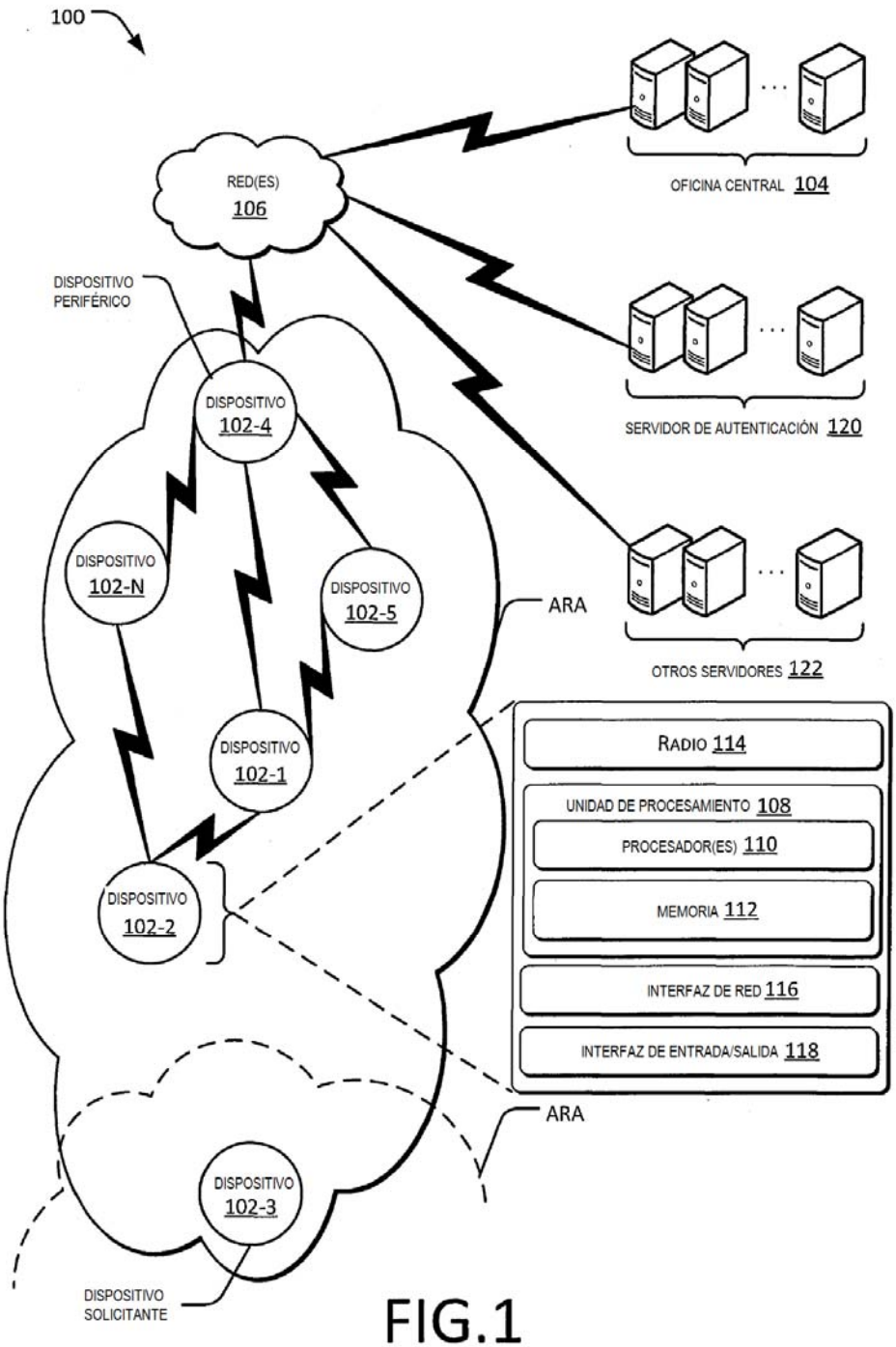
100
RED(ES)
106
OFICINA CENTRAL 104
SERVIDOR DE AUTENTICACIÓN 120
OTROS SERVIDORES 122
DISPOSITIVO PERIFÉRICO
DISPOSITIVO 102-4
DISPOSITIVO 102-N
DISPOSITIVO 102-5
DISPOSITIVO 102-1
DISPOSITIVO 102-2
DISPOSITIVO 102-3
DISPOSITIVO SOLICITANTE
ARA
ARA
RADIO 114
UNIDAD DE PROCESAMIENTO 108
PROCESADOR(ES)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

FIG.1

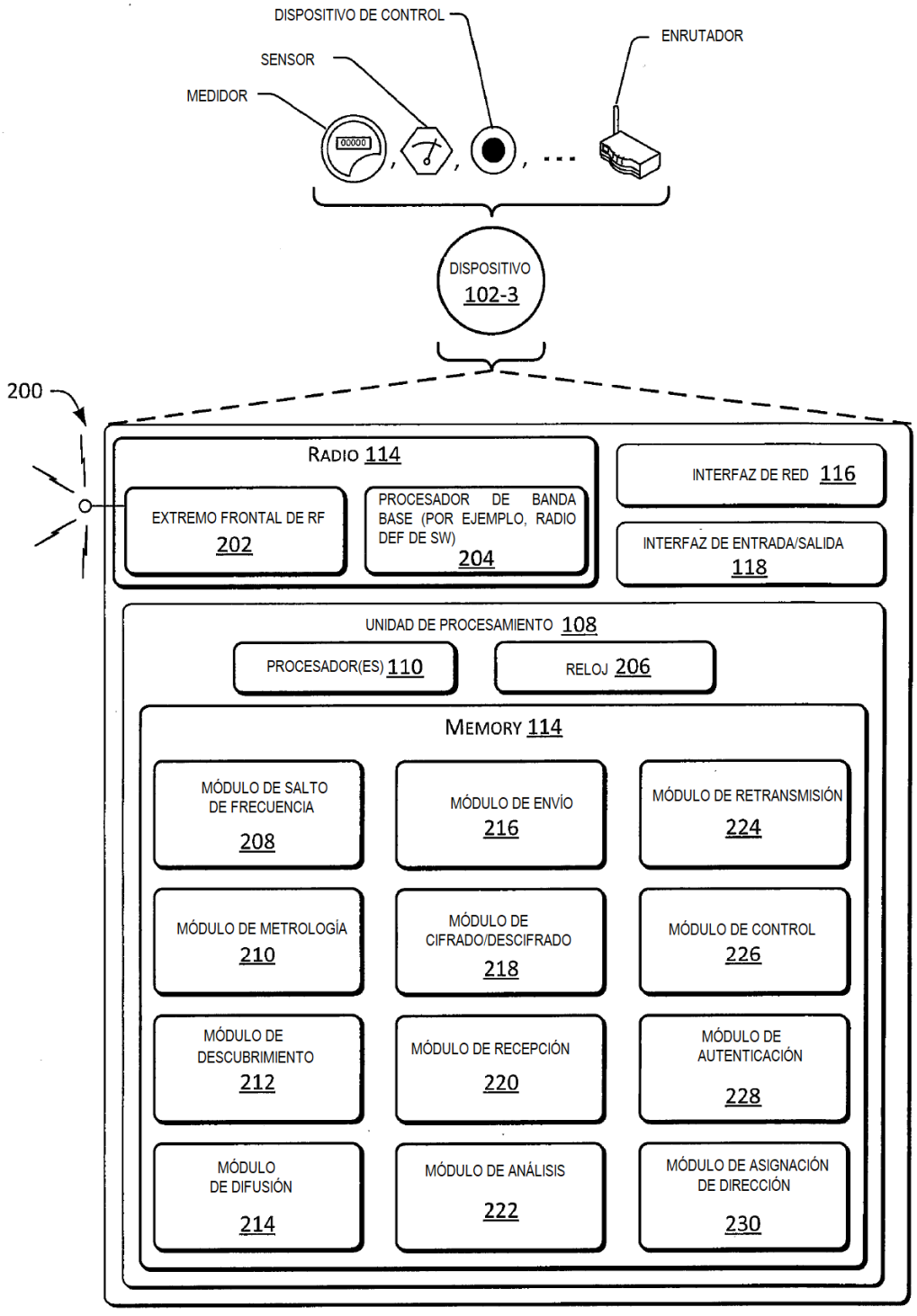
DISPOSITIVO DE CONTROL
SENSOR
MEDIDOR
ENRUTADOR
DISPOSITIVO
102-3
200
RADIO 114
EXTREMO FRONTAL DE RF
202
PROCESADOR DE BANDA BASE (POR EJEMPLO, RADIO DEF DE SW)
204
INTERFAZ DE RED 116
INTERFAZ DE ENTRADA/SALIDA
118
UNIDAD DE PROCESAMIENTO 108
PROCESADOR(ES) 110
RELOJ 206
MEMORY 114
MÓDULO DE SALTO 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 DIFUSIÓN
214
MÓDULO DE ANÁLISIS
222
MÓDULO DE ASIGNACIÓN DE DIRECCIÓN
230

FIG.2

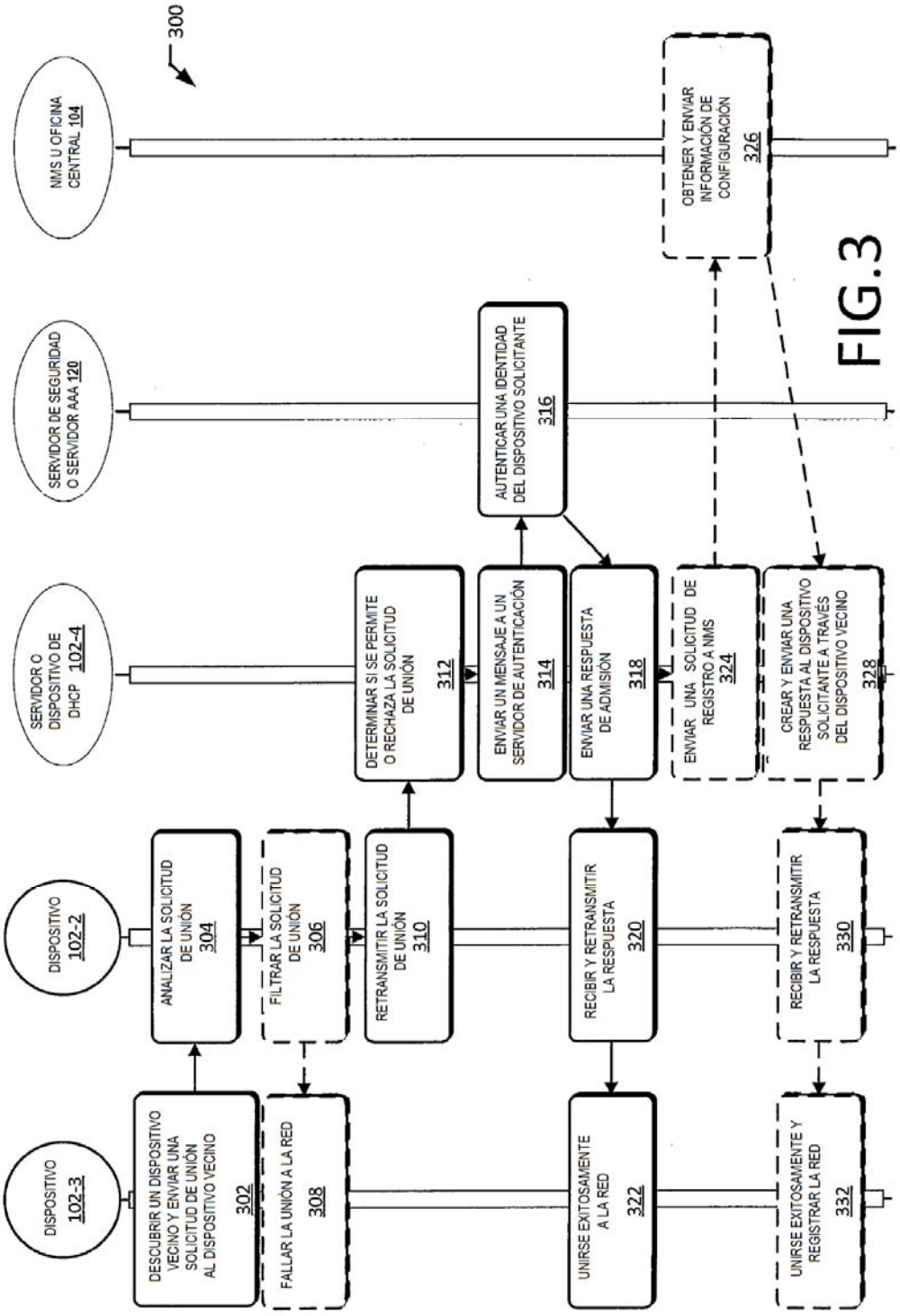
300
NMS U OFICINA CENTRAL 104
SERVIDOR DE SEGURIDAD O SERVIDOR AAA 120
SERVIDOR O DISPOSITIVO DE DHCP 102-4
DISPOSITIVO 102-2
DISPOSITIVO 102-3
DESCUBRIR UN DISPOSITIVO VECINO Y ENVIAR UNA SOLICITUD DE UNIÓN AL DISPOSITIVO VECINO 302
ANALIZAR LA SOLICITUD DE UNIÓN 304
FILTRAR LA SOLICITUD DE UNIÓN 306
FALLAR LA UNIÓN A LA RED 308
RETRANSMITIR LA SOLICITUD DE UNIÓN 310
DETERMINAR SI SE PERMITE O RECHAZA 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
RECIBIR Y RETRANSMITIR LA RESPUESTA 320
UNIRSE EXITOSAMENTE A LA RED 322
ENVIAR UNA SOLICITUD DE REGISTRO A NMS 324
OBTENER Y ENVIAR INFORMACIÓN DE CONFIGURACIÓN 326
CREAR Y ENVIAR UNA RESPUESTA AL DISPOSITIVO SOLICITANTE A TRAVÉS DEL DISPOSITIVO VECINO 328
RECIBIR Y RETRANSMITIR LA RESPUESTA 330
UNIRSE EXITOSAMENTE Y REGISTRAR LA RED 332

FIG.3

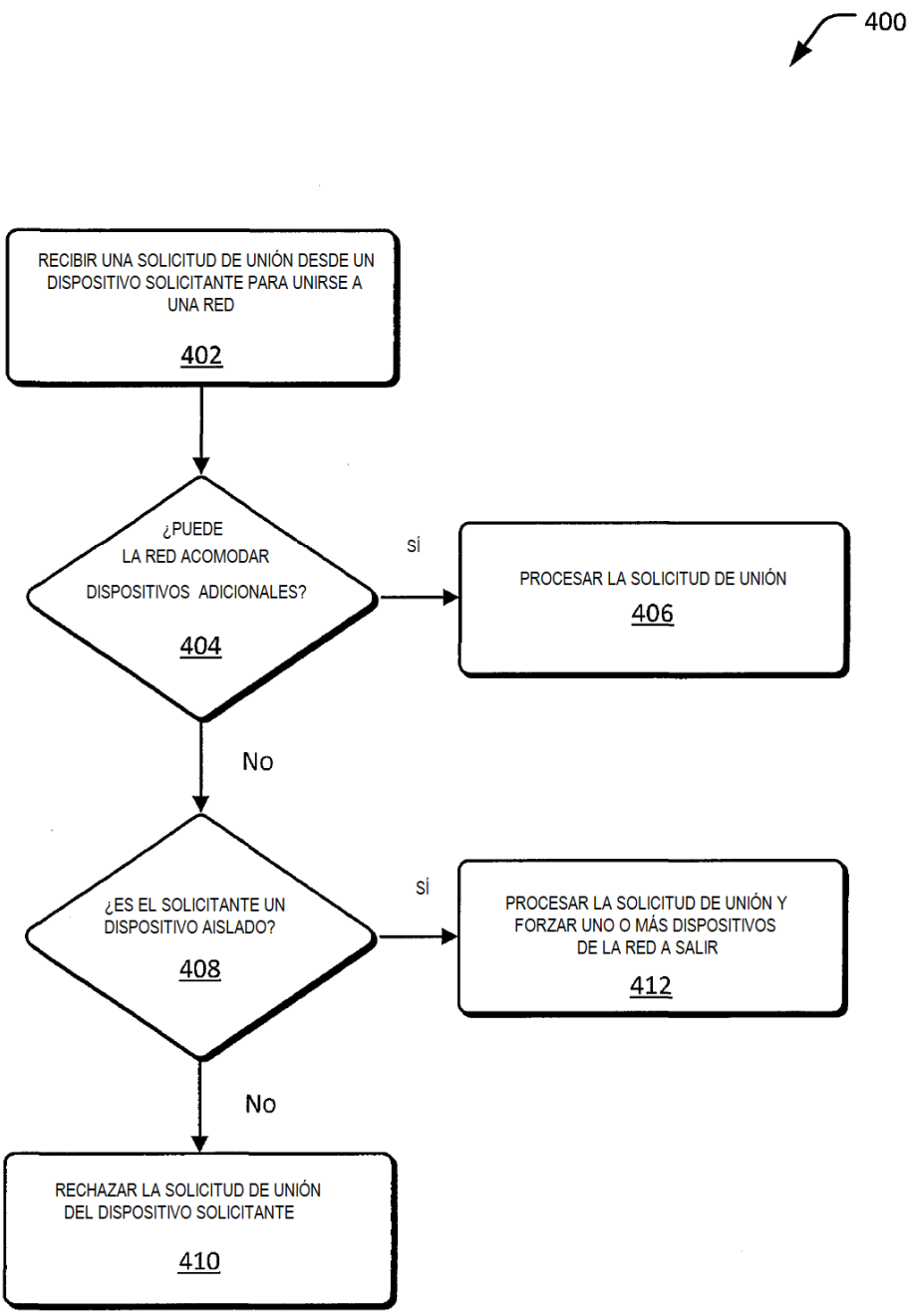
400
RECIBIR UNA SOLICITUD DE UNIÓN DESDE UN DISPOSITIVO SOLICITANTE PARA UNIRSE A UNA RED
402
¿PUEDE LA RED ACOMODAR DISPOSITIVOS ADICIONALES?
404
sí
PROCESAR LA SOLICITUD DE UNIÓN
406
No
¿ES EL SOLICITANTE UN DISPOSITIVO AISLADO?
408
sí
PROCESAR LA SOLICITUD DE UNIÓN Y FORZAR UNO O MÁS DISPOSITIVOS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

FIG. 4

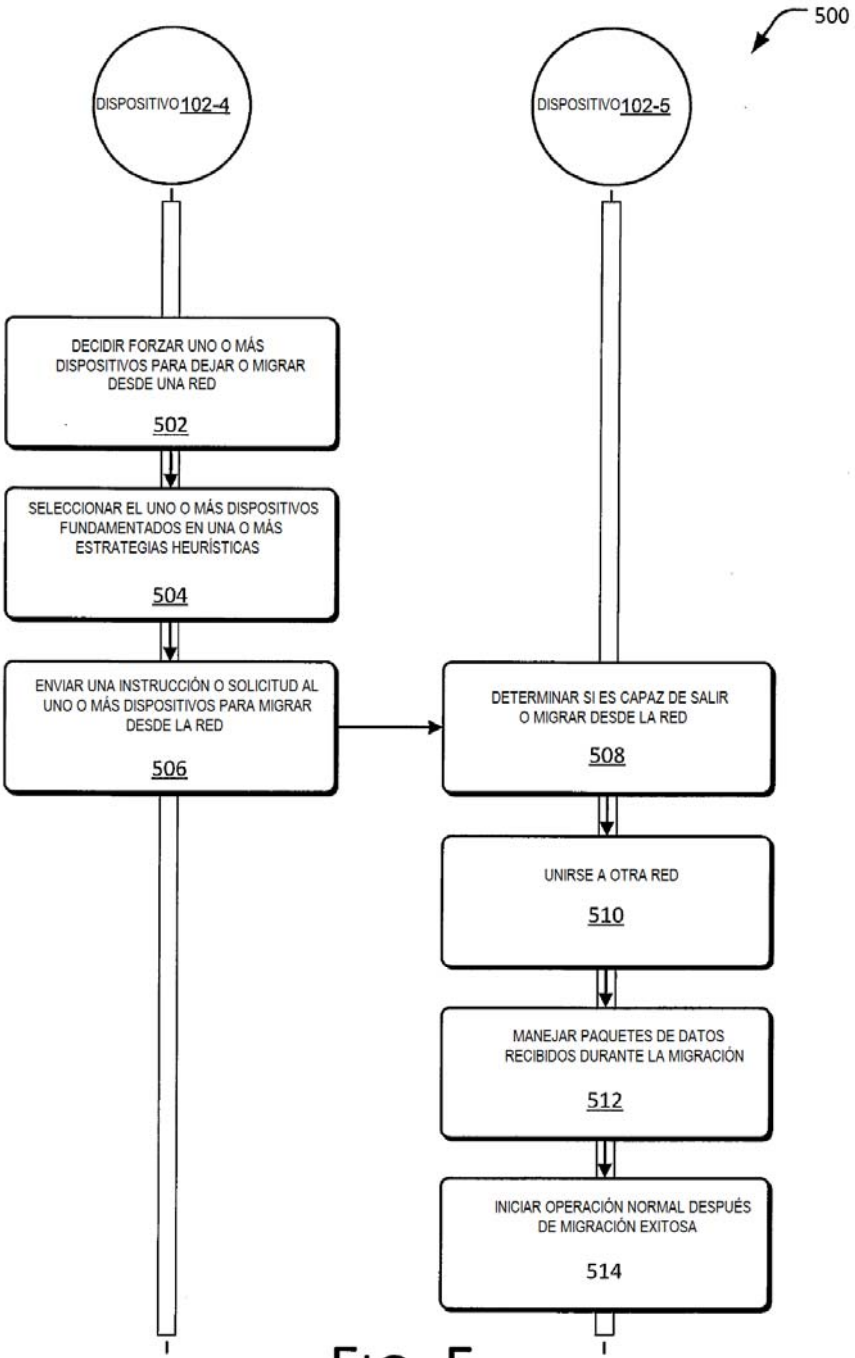
500
DISPOSITIVO 102-4
DISPOSITIVO 102-5
DECIDIR FORZAR UNO O MÁS DISPOSITIVOS PARA DEJAR O MIGRAR DESDE UNA RED
502
SELECCIONAR EL UNO O MÁS DISPOSITIVOS FUNDAMENTADOS EN UNA O MÁS ESTRATEGIAS HEURÍSTICAS
504
ENVIAR UNA INSTRUCCIÓN O SOLICITUD AL UNO O MÁS DISPOSITIVOS PARA MIGRAR DESDE LA RED
506
DETERMINAR SI ES CAPAZ DE SALIR O MIGRAR DESDE LA RED
508
UNIRSE A OTRA RED
510
MANEJAR PAQUETES DE DATOS RECIBIDOS DURANTE LA MIGRACIÓN
512
INICIAR OPERACIÓN NORMAL DESPUÉS DE MIGRACIÓN EXITOSA
514

FIG. 5