(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 015 060**

(51) Int. Cl.:

G06F 21/44 (2013.01)
H04L 69/324 (2012.01)
H04L 69/329 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.09.2018 PCT/JP2018/033887**

(87) Fecha y número de publicación internacional: **15.08.2019 WO19155671**

(96) Fecha de presentación y número de la solicitud europea: **12.09.2018 E 18904797 (0)**

(97) Fecha y número de publicación de la concesión europea: **19.02.2025 EP 3751819**

(54) Título: **Sistema de red**

(30) Prioridad:

06.02.2018 JP 2018018928

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.04.2025

(73) Titular/es:

CONNECTFREE CORPORATION (100.00%)
83,Kankoboko-cho, Shijokarasuma-nishiiru, Shimogyo-ku
Kyoto-shi, Kyoto 600-8009, JP

(72) Inventor/es:

TATE, KRISTOPHER ANDREW

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Sistema de red

Campo técnico

La presente invención se refiere a un sistema de red basado en un nuevo concepto de autenticación de una dirección de red en sí misma.

Antecedentes técnicos

Las tecnologías de la información y la comunicación (TIC) han progresado notablemente en los últimos años y los dispositivos conectados a redes como Internet no se limitan a aparatos de procesamiento de la información como los ordenadores personales convencionales o los teléfonos inteligentes, sino que incluyen diversas cosas. Esta tendencia tecnológica se denomina "Internet de las cosas (IoT, por sus siglas en inglés)" y se han propuesto y puesto en práctica diversas tecnologías y servicios. En el futuro se espera un mundo en el que varios miles de millones de personas y diez mil millones o varios billones de dispositivos de la Tierra estén conectados simultáneamente. Para hacer realidad ese mundo interconectado, debe ofrecerse una solución más sencilla y segura que permita una conexión más libre.

Normalmente en una red, los datos se comunican entre dispositivos utilizando una dirección de red asignada estática o dinámicamente a cada dispositivo. Normalmente, se adopta como dirección de red una dirección de protocolo de Internet (IP, por sus siglas en inglés).

En general, algunas direcciones IP, como las direcciones globales, se establecen de forma única en Internet y otras direcciones IP, como las direcciones privadas, se asignan exclusivamente en una red privada. También existe el esquema de asignación dinámica de una dirección IP basado en un protocolo de configuración dinámica de host (DHCP).

Así, al establecer una dirección IP para la comunicación de datos, se presta atención únicamente a la asignación exclusiva de direcciones IP en la misma red. A saber, la dirección IP es una dirección de red establecida arbitrariamente de acuerdo con una red de interés.

Por ejemplo, la patente japonesa número 2017-059868 (PTL 1), puesta al descubierto, divulga una configuración que reduce las horas-hombre para establecer una dirección IP. Como otro ejemplo, una publicación US 7,249,374 divulga una solución para aplicar selectivamente la política de seguridad de red utilizando identificadores de grupo. Como otro ejemplo, una publicación US 2012/0304259 divulga una Femtocélula que proporciona servicios a un equipo de usuario y autentica un equipo de usuario registrado en un primer dominio operativo, cuando el equipo de usuario solicita el servicio proporcionado por un segundo dominio operativo. Como otro ejemplo, una publicación US 2005/0216587 divulga una solución para establecer la confianza en un cliente de correo electrónico, donde se determina a partir de una lista almacenada de direcciones de red de confianza, si el cliente de correo electrónico es de confianza según la dirección de red del cliente de correo electrónico. La publicación CN106453378A divulga la autenticación de direcciones de red de un dispositivo servidor.

Lista de citas

Literatura de patentes

PTL 1: Patente japonesa número 2017-059868, puesta al descubierto.

Resumen de la invención

Problema técnico

Como se ha descrito anteriormente, una dirección de red ha servido hasta ahora como información de identificación para identificar un destino, sin embargo, no se ha proporcionado fiabilidad a dicha dirección en sí. Por lo tanto, aunque los datos se comunican entre dispositivos utilizando la dirección IP, el procesamiento de autenticación o similar se ha realizado en una capa superior (por ejemplo, una capa de aplicación).

Por lo tanto, con el fin de proporcionar un servicio que requiere varios tipos de procesamiento de autenticación, una aplicación para realizar el procesamiento de autenticación como la base para el servicio debe ser proporcionada por adelantado o cada vez, lo que ha interferido con la prevalencia.

La presente invención proporciona una solución al problema descrito anteriormente.

Solución al problema

La invención se define mediante las reivindicaciones adjuntas.

Un sistema de red según un aspecto de la presente invención incluye al menos un dispositivo servidor y al menos un dispositivo terminal que accede a cualquiera del al menos un dispositivo servidor. El dispositivo terminal autentica una dirección de red entre el dispositivo terminal y cualquiera del al menos un dispositivo servidor y comunica datos con él. Cuando el dispositivo servidor recibe una solicitud del dispositivo terminal, el dispositivo servidor proporciona un servicio de acuerdo con la dirección de red autenticada que posee el dispositivo terminal que ha emitido la solicitud.

Preferiblemente, el dispositivo servidor identifica el dispositivo terminal que ha emitido la solicitud, basándose únicamente en la dirección de red utilizada en la interacción con el dispositivo terminal a través de una capa de red, sin realizar procesamiento de autenticación en una capa de aplicación.

Preferentemente, el dispositivo terminal incluye un primer programa de comunicación dirigido a una capa de enlace de datos, un segundo programa de comunicación dirigido a una capa de transporte y una capa de red, y un programa de autenticación de direcciones conectado entre el primer programa de comunicación y el segundo programa de comunicación. El programa de autenticación de direcciones autentica, entre el programa de autenticación de direcciones y un dispositivo de destino, la dirección de red que se utilizará para la transmisión de datos solicitada por el segundo programa de comunicación.

Preferiblemente, el dispositivo terminal incluye un módulo de función de comunicación que proporciona una función de comunicación y un dispositivo semiconductor que tiene la dirección de red autenticada codificada en el mismo. El dispositivo semiconductor autentica la dirección de red entre el dispositivo semiconductor y un dispositivo de destino, utilizando el módulo de función de comunicación.

Efectos ventajosos de la invención

Según una forma de la presente invención, al prestar un servicio adaptado a un dispositivo o a un usuario que utiliza el dispositivo, no es necesario ni una aplicación especial ni un procedimiento de autenticación adicional. Por lo tanto, se puede reducir el tiempo de respuesta involucrado con la prestación de un servicio.

Breve descripción de los dibujos

La Fig. 1 es un diagrama esquemático que muestra una configuración general ejemplar de un sistema de red según la presente realización.

La Fig. 2 es un diagrama esquemático que muestra una configuración ejemplar de un dispositivo terminal según la presente realización.

La Fig. 3 es un diagrama esquemático que muestra una configuración ejemplar de un dispositivo terminal según la presente realización.

La Fig. 4 es un diagrama esquemático que muestra otra configuración ejemplar del dispositivo terminal según la presente realización.

La Fig. 5 es un diagrama esquemático para ilustrar la interacción entre dispositivos en el sistema de red según la presente realización.

La Fig. 6 es un diagrama de secuencia que muestra un procedimiento de procesamiento ejemplar involucrado con la prestación de un servicio en el sistema de red de acuerdo con la presente realización.

La Fig. 7 es un diagrama para ilustrar una aplicación ejemplar para proporcionar un servicio mediante la utilización del sistema de red de acuerdo con la presente realización.

La Fig. 8 es un diagrama para ilustrar otra aplicación ejemplar para proporcionar un servicio mediante la utilización del sistema de red de acuerdo con la presente realización.

La Fig. 9 es un diagrama que ilustra el filtrado ejemplar de una dirección de red utilizando el sistema de red según la presente realización.

Descripción de realizaciones

Una realización de la presente invención se describirá en detalle con referencia a los dibujos. Los elementos iguales o correspondientes en los dibujos tienen los mismos caracteres de referencia asignados y la descripción de los mismos no se repetirá.

A. Visión general

Según la presente realización, se proporciona un servicio basado en una dirección de red autenticada y una plataforma para proporcionar el servicio. En una red convencional, no ha habido ningún concepto técnico de autenticación de una dirección de red en sí y la dirección de red se ha utilizado principalmente sólo para establecer la conexión de comunicación. A continuación, se ha realizado normalmente un procedimiento de autenticación mediante el uso de una aplicación para la autenticación. Por el contrario, dado que en la presente realización se autentica una dirección de red en sí, el establecimiento de la conexión de comunicación per se también sirve como procedimiento de autenticación y no se requiere un procedimiento de autenticación adicional o similar mediante el uso de una aplicación.

Por lo tanto, al prestar un servicio adaptado a un dispositivo o a un usuario que utiliza el dispositivo, no se requiere ni una aplicación especial ni un procedimiento de autenticación adicional. Por lo tanto, se puede reducir el tiempo de respuesta involucrado con la prestación de un servicio.

Una "dirección de red" significa aquí información de identificación para identificar de forma única un dispositivo a través de alguna red y generalmente está constituida por una cadena de caracteres que incluye una combinación de caracteres, números y/o signos. Aunque se asume una dirección de protocolo de Internet (IP, por sus siglas en inglés) como ejemplo típico de dirección de red, puede aplicarse una dirección de orden inferior, como una dirección de control de acceso a medios (MAC, por sus siglas en inglés), o una dirección de orden superior, como un nombre de host o un localizador uniforme de recursos (URL, por sus siglas en inglés) gestionado por un sistema de nombres de dominio (DNS, por sus siglas en inglés). Independientemente de una diferencia de red, como una red global y una red privada, también se puede seleccionar arbitrariamente un protocolo a utilizar. Puede adoptarse como la dirección de red una dirección de red específica de un protocolo adoptado.

Cuando se adopta típicamente una dirección IP, el número de bits definido es diferente para cada versión. Bajo el protocolo de Internet versión 4 (IPv4), actualmente establecido, se define un espacio de direcciones de 32 bits, y en el protocolo de Internet versión 6 (IPv6), actualmente establecido, se define un espacio de direcciones de 128 bits. En la presente realización, una dirección IP conforme a IPv6 se describe principalmente como la dirección de red.

Por "dirección de red autenticada" se entiende un estado en el que la autenticidad de la dirección de red asignada a cada dispositivo está garantizada para un destino o un tercero, es decir, un estado que garantiza que una dirección de red utilizada por cada dispositivo para la comunicación de datos no es falsificada, mediante la adopción de un esquema como el que se describirá más adelante.

Un "dispositivo" aquí engloba cosas arbitrarias que pueden comunicar datos a través de una red. Típicamente, el dispositivo puede implementarse como un único aparato de comunicación o puede implementarse como parte de algo o como incorporado en algo.

B. Configuración general del sistema de red

Inicialmente se describirá una configuración general de un sistema de red 1 según la presente realización.

La Fig. 1 es un diagrama esquemático que muestra una configuración general ejemplar del sistema de red 1 según la presente realización. En referencia a la Fig. 1, los dispositivos terminales 100-1, 100-2, 100-3,... que representan dispositivos ejemplares (que también pueden denominarse colectivamente en lo sucesivo "dispositivo terminal 100") y los dispositivos servidores 200-1, 200-2, 200-3,... que representan otros dispositivos (que también pueden denominarse colectivamente en lo sucesivo "dispositivo servidor 200") están conectados a una red 2 como Internet.

Por ejemplo, un smartphone o un teléfono portátil se asume como dispositivo terminal 100-1 y el dispositivo terminal 100-1 está conectado a la red 2 con una estación base 6 proporcionada por una entidad de comunicación móvil interpuesta. Por ejemplo, una tableta se asume como dispositivo terminal 100-2, y, por ejemplo, un ordenador personal portátil se asume como dispositivo terminal 100-3. Los dispositivos terminales 100-2 y 100-3 están conectados a la red 2, por ejemplo, interponiendo un punto de acceso 4.

Cada uno de los dispositivos servidores 200-1, 200-2, 200-3,... es un dispositivo que proporciona un servicio arbitrario. Cada dispositivo servidor 200 proporciona un servicio solicitado al ser accedido desde cualquier dispositivo terminal 100.

Así, el sistema de red 1 incluye al menos un dispositivo servidor 200 (un segundo dispositivo) y al menos un dispositivo terminal 100 (un primer dispositivo) que puede acceder a cualquiera del al menos un dispositivo servidor 200.

En el sistema de red 1 según la presente realización, el dispositivo servidor 200 puede obtener una dirección de red autenticada del dispositivo terminal 100 que ha accedido al dispositivo servidor. Del mismo modo, el dispositivo terminal 100 puede obtener una dirección de red autenticada del dispositivo servidor 200 al que ha accedido el dispositivo terminal.

El procesamiento para autenticar mutuamente la dirección de red se realiza entre el dispositivo terminal 100 y el

dispositivo servidor 200, y la autenticación satisfactoria de la dirección de red permite el inicio de la comunicación de datos. En concreto, el dispositivo terminal 100 autentica la dirección de red entre el dispositivo terminal y cualquiera de al menos un dispositivo servidor y comunica datos con él. Al adoptar dicha configuración para la comunicación de datos, el dispositivo terminal 100 y el dispositivo servidor 200 pueden obtener mutuamente la dirección de red autenticada del destino.

Por ejemplo, cuando el dispositivo servidor 200 recibe una solicitud del dispositivo terminal 100, proporciona un servicio de acuerdo con la dirección de red autenticada del dispositivo terminal 100 que ha emitido la solicitud. A saber, el dispositivo servidor 200 puede proporcionar un servicio de acuerdo con la dirección de red autenticada obtenida al dispositivo terminal 100 que ha emitido la solicitud. Más adelante se describirá un servicio ejemplar de acuerdo con la dirección de red. Dado que el dispositivo terminal 100 también puede obtener la dirección de red autenticada del dispositivo servidor 200, también puede transmitir un comando específico de acuerdo con el dispositivo servidor 200 de destino.

Así, en el sistema de red 1 según la presente realización, la dirección de red autenticada de cada dispositivo terminal 100 puede obtenerse de modo que pueda proporcionarse un servicio específico a cada dispositivo terminal 100 sin requerir una aplicación para realizar el procesamiento de autenticación. Dado que la comunicación de datos entre dispositivos tales como el dispositivo terminal 100 y el dispositivo servidor 200 implica la obtención de la dirección de red autenticada, un período de tiempo requerido para proporcionar un servicio específico al dispositivo terminal 100 es también extremadamente corto y el tiempo de espera hasta la prestación de un servicio puede ser más corto que en una configuración en la que el procesamiento de autenticación se realiza con el uso de una aplicación.

C. Configuración del dispositivo para realizar la autenticación de dirección de red

Ahora se describirá una configuración ejemplar de un dispositivo para realizar la autenticación de una dirección de red utilizada en el sistema de red 1 según la presente realización. Para realizar la autenticación de una dirección de red, por ejemplo, se supone una implementación de hardware y una implementación de software. A continuación, se describe una implementación ejemplar.

c1: Implementación de hardware

La Fig. 2 es un diagrama esquemático que muestra una configuración ejemplar de un dispositivo terminal 100A según la presente realización. En referencia a la Fig. 2, el dispositivo terminal 100A incluye un procesador 102, una memoria principal 104, una pantalla 106, una unidad de entrada 108, un módulo de comunicación 110 y un almacenamiento secundario 130.

El procesador 102 es una entidad de procesamiento que realiza diversos tipos de procesamiento en el dispositivo terminal 100A. El procesador 102 desarrolla y ejecuta un programa o varias instrucciones almacenadas en el almacenamiento secundario 130 de la memoria principal 104.

La memoria principal 104 es un almacenamiento volátil tal como una memoria de acceso aleatorio dinámico (DRAM, por sus siglas en inglés) o una memoria de acceso aleatorio estático (SRAM, por sus siglas en inglés). El almacenamiento secundario 130 es un almacenamiento no volátil como una memoria flash o un disco duro. El almacenamiento secundario 130 almacena un sistema operativo (SO) 132 y una o más aplicaciones arbitrarias 134.

La pantalla 106 es un componente que presenta un resultado del procesamiento realizado por el procesador 102 al exterior, y se implementa, por ejemplo, mediante una pantalla de cristal líquido (LCD, por sus siglas en inglés) o una pantalla orgánica de electroluminiscencia (EL, por sus siglas en inglés).

La unidad de entrada 108 es un componente que acepta una operación mediante un usuario e implementada, por ejemplo, mediante un aparato de entrada arbitrario como un teclado, un panel táctil o un ratón.

El módulo de comunicación 110 es un componente principal que proporciona una dirección de red autenticada e incluye un chip de autenticación de direcciones 112, un módulo WiFi 114 y un módulo LTE 118.

El chip de autenticación de direcciones 112 es un dispositivo semiconductor que tiene una dirección de red autenticada y la información necesaria para la autenticación codificada en el mismo, y autentica una dirección de red en la comunicación de datos con otro dispositivo mediante el módulo WiFi 114 y/o el módulo LTE 118.

Más específicamente, en la comunicación de datos mediante el módulo WiFi 114 o el módulo LTE 118, el chip de autenticación de direcciones 112 realiza un procesamiento para autenticar mutuamente, entre el chip de autenticación de direcciones y otro dispositivo, una dirección de red autenticada proporcionada por adelantado. De este modo, el chip de autenticación de direcciones 112 autentica una dirección de red entre el chip de autenticación de direcciones y un dispositivo de destino, mediante un módulo de función de comunicación (módulo WiFi 114 y/o módulo LTE 118). Circuitos que son resistentes a la manipulación se adoptan preferentemente como chip de autenticación de direcciones 112.

El módulo WiFi 114 y/o el módulo LTE 118 proporcionan una función de la capa física y de la capa de enlace de datos del modelo de referencia de interconexión de sistemas abiertos (OSI, por sus siglas en inglés). El módulo WiFi 114 proporciona, al estar conectado a una antena 116, una función de comunicación inalámbrica conforme a un esquema de acceso inalámbrico como una red de área local inalámbrica (LAN, por sus siglas en inglés) o WiMAX. El módulo LTE 118 proporciona, al estar conectado a una antena 120, una función de comunicación inalámbrica conforme a un esquema de acceso inalámbrico como la evolución a largo plazo (LTE, por sus siglas en inglés), el acceso múltiple por división de código de banda ancha (W-CDMA, por sus siglas en inglés) o CDMA2000.

Aunque el módulo de comunicación 110, que incluye el módulo WiFi 114 y/o el módulo LTE 118, se ejemplifica para facilitar la descripción, no es necesario incluir ambos módulos. Puede incorporarse un módulo solo o uno o más módulos que proporcionen otras funciones de comunicación. En ese caso, se puede proporcionar como función de comunicación no sólo una función de comunicación inalámbrica, sino también una función de comunicación por cable.

Por lo tanto, el módulo de comunicación 110 incluye un módulo de función de comunicación (módulo WiFi 114 y/o módulo LTE 118) que proporciona la función de comunicación y un dispositivo semiconductor (chip de autenticación de direcciones 112) que tiene una dirección de red autenticada codificada en el mismo.

Adoptando la implementación de hardware según lo expuesto anteriormente, la dirección de red autenticada puede ser proporcionada y obtenida en el dispositivo terminal 100A.

c2: Implementación de software

La Fig. 3 es un diagrama esquemático que muestra una configuración ejemplar de un dispositivo terminal 100B según la presente realización. En referencia a (A) de la Fig. 3, el dispositivo terminal 100B incluye el procesador 102, la memoria principal 104, la pantalla 106, la unidad de entrada 108, el almacenamiento secundario 130, un módulo WiFi 144 y un módulo LTE 148.

El procesador 102 es una entidad de procesamiento que realiza diversos tipos de procesamiento en el dispositivo terminal 100B. El procesador 102 desarrolla y ejecuta un programa o varias instrucciones almacenadas en el almacenamiento secundario 130 de la memoria principal 104. El almacenamiento secundario 130 almacena un programa de autenticación de direcciones 136 e información de gestión de autenticación 138 además del SO 132 y una o más aplicaciones arbitrarias 134.

El módulo WiFi 144 y/o el módulo LTE 148 proporcionan la función de la capa física y la capa de enlace de datos del modelo de referencia OSI. El módulo WiFi 144 proporciona, al estar conectado a una antena 146, la función de comunicación inalámbrica conforme a un esquema de acceso inalámbrico tal como LAN inalámbrica o WiMAX. El módulo LTE 148 proporciona, al estar conectado a una antena 150, una función de comunicación inalámbrica conforme a un esquema de acceso inalámbrico como LTE, W-CDMA o CDMA2000.

Aunque la configuración que incluye el módulo WiFi 144 y/o el módulo LTE 148 se ejemplifica para facilitar la descripción, no es necesario incluir ambos módulos. Puede incorporarse un módulo solo o uno o más módulos que proporcionen otras funciones de comunicación. En ese caso, se puede proporcionar como función de comunicación no sólo una función de comunicación inalámbrica, sino también una función de comunicación por cable.

Como resultado de la ejecución del programa de autenticación de direcciones 136 en el dispositivo terminal 100B, se proporciona la dirección de red autenticada. A continuación, se ejemplifica una configuración de software para proporcionar una dirección de red autenticada.

La Fig. 3 muestra en (B) un diagrama esquemático para ilustrar el procesamiento involucrado con la comunicación de datos en el dispositivo terminal 100B. Como se muestra en (B) de la Fig. 3, el módulo WiFi 144 y/o el módulo LTE 148 que proporcionan la función de la capa física realizan la transmisión/recepción de una señal real (datos) por medio de un controlador de enlace de datos 1322 (una función de una parte de SO 132).

La aplicación 134, como un navegador web, utiliza un socket TCP/IP 1324 para la comunicación de datos. El socket TCP/IP 1324 puede proporcionarse como una función de una parte de SO 132. Aunque la Fig. 3 ilustra en (B) el socket TCP/IP 1324 a modo de ejemplo, puede adoptarse, por ejemplo, un socket UDP/IP.

El socket TCP/IP 1324 normalmente realiza la transmisión y recepción de datos hacia y desde otro dispositivo mediante la transmisión/recepción interna de datos hacia/desde el controlador de enlace de datos 1322.

En contraste, en el dispositivo terminal 100B según la presente realización, el programa de autenticación de direcciones 136 está dispuesto entre el socket TCP/IP 1324 y el controlador de enlace de datos 1322. El programa de autenticación de direcciones 136 autentica una dirección de red asignada a cada dispositivo mutuamente entre el programa de autenticación de direcciones y un dispositivo de destino en una sesión específica, y sólo cuando la autenticación tiene éxito, el programa de autenticación de direcciones transmite y recibe datos en la sesión específica.

Al adoptar dicho esquema, desde un punto de vista de la aplicación 134, se puede mantener la transparencia sin ser consciente de la presencia del programa de autenticación de direcciones 136. Es decir, la aplicación 134 sólo debe transmitir un paquete que incluya los datos necesarios, y puede confiar y utilizar una dirección de red incluida en el encabezado de un paquete recibido de cualquier dispositivo, tal cual.

El programa de autenticación de direcciones 136 autentica mutuamente una dirección de red entre el programa de autenticación de direcciones y otro dispositivo basándose en la información almacenada en la información de gestión de autenticación 138 preparada por adelantado de forma segura. La información de gestión de autenticación 138 incluye no sólo una dirección de red asignada a cada dispositivo, sino también un código para garantizar que la dirección de red es auténtica (es decir, autenticada). El programa de autenticación de direcciones 136 autentica mutuamente una dirección de red transmitiendo información adicional incluida en la información de gestión de autenticación 138 a un destino, junto con la dirección de red definida en la información de gestión de autenticación 138.

Sin limitarse a un dispositivo de destino con el que se comunican datos, el programa de autenticación de direcciones puede autenticar una dirección de red entre el programa de autenticación de direcciones y un dispositivo servidor de autenticación externo o similar.

Así, el dispositivo terminal 100B incluye un programa de comunicación (controlador de enlace de datos 1322) dirigido a la capa de enlace de datos, un programa de comunicación (socket TCP/IP 1324) dirigido a la capa de transporte y a la capa de red, y el programa de autenticación de direcciones 136 conectado entre el controlador de enlace de datos 1322 y el socket TCP/IP 1324.

Aunque la Fig. 3 muestra una configuración en la que el programa de autenticación de direcciones 136 está dispuesto lógicamente entre las capas del socket TCP/IP 1324 y el controlador de enlace de datos 1322, cualquier implementación puede ser aplicable sin estar limitada como tal, siempre que el programa de autenticación de direcciones 136 pueda autenticar mutuamente una dirección de red entre el programa de autenticación de direcciones y un destino.

Por ejemplo, el socket TCP/IP 1324 y el programa de autenticación de direcciones 136 pueden estar dispuestos lógicamente en paralelo, y el socket TCP/IP 1324 puede ser impedido de iniciar la transmisión y recepción de un paquete a menos que una dirección de red sea autenticada entre el programa de autenticación de direcciones 136 y un dispositivo de destino. En este caso, una vez que el programa de autenticación de direcciones 136 autentica una dirección de red, la transmisión/recepción de datos continúa a partir de entonces entre el socket TCP/IP 1324 y el controlador de enlace de datos 1322 y el programa de autenticación de direcciones 136 no tiene que estar involucrado en la transferencia interna de datos.

Dado que los componentes correspondientes entre los componentes del dispositivo terminal 100B son los mismos que los del dispositivo terminal 100A, no se repetirá la descripción detallada.

Adoptando la implementación de software según lo expuesto anteriormente, se puede proporcionar una dirección de red autenticada al dispositivo terminal 100B.

c3: Otra implementación de software

Sin limitarse a la configuración funcional implicada en la comunicación de datos mostrada en (B) de la Fig. 3, puede adoptarse otra implementación. La Fig. 4 es un diagrama esquemático que muestra otra configuración ejemplar del dispositivo terminal según la presente realización.

En una implementación ejemplar mostrada en (A) de la Fig. 4, por encima de una estructura general de capas, es decir, la capa física y la capa de enlace de datos (módulo WiFi 144 y/o módulo LTE 148), el controlador de enlace de datos 1322 y el socket TCP/IP 1324 están dispuestos secuencialmente. La aplicación arbitraria 134 utiliza el socket TCP/IP 1324 para la comunicación de datos.

En la implementación ejemplar mostrada en (A) de la Fig. 4, en el momento de inicio de o durante la transmisión/recepción de datos por el socket TCP/IP 1324 a/desde un nodo destino, el socket TCP/IP 1324 solicita al programa de autenticación de direcciones 136 que autentique el destino. El programa de autenticación de direcciones 136 determina, realizando el procesamiento de autenticación descrito anteriormente, si el destino es o no un nodo fiable o si los datos transmitidos/recibidos a/desde el destino han sido manipulados, y proporciona un resultado del mismo al socket TCP/IP 1324. El procesamiento básico realizado por el programa de autenticación de direcciones 136 es similar al realizado por el programa de autenticación de direcciones 136 mostrado en (B) de la Fig. 3 descrito anteriormente.

En la implementación mostrada en (A) de la Fig. 4, el socket TCP/IP 1324 solicita al programa de autenticación de direcciones 136 que realice el procesamiento de autenticación necesario. Por lo tanto, desde el punto de vista de la aplicación 134, la comunicación segura con el destino que tiene la dirección de red autenticada puede establecerse

utilizando la interfaz igual que en la comunicación normal.

En una implementación ejemplar mostrada en (B) de la Fig. 4, por encima de la estructura general de capas, es decir, la capa física y la capa de enlace de datos (módulo WiFi 144 y/o módulo LTE 148), el controlador de enlace de datos 1322 y el socket TCP/IP 1324 están dispuestos secuencialmente. La aplicación arbitraria 134 utiliza el socket TCP/IP 1324 para la comunicación de datos y también interactúa con el programa de autenticación de direcciones 136 para la autenticación necesaria.

En la implementación ejemplar mostrada en (B) de la Fig. 4, en el momento o durante la transmisión/recepción de datos por la aplicación 134 a/desde un nodo de destino, la aplicación 134 solicita al programa de autenticación de direcciones 136 que autentique el destino. El programa de autenticación de direcciones 136 transmite/recibe datos a/desde el socket TCP/IP 1324 y determina, realizando el procesamiento de autenticación descrito anteriormente, si el destino es o no un nodo fiable o si los datos transmitidos/recibidos a/desde el destino han sido manipulados. A continuación, el programa de autenticación de direcciones 136 proporciona un resultado de la autenticación a la aplicación 134. El procesamiento básico realizado por el programa de autenticación de direcciones 136 es el mismo que el realizado por el programa de autenticación de direcciones 136 mostrado en (B) de la Fig. 3 descrito anteriormente.

Adoptando la implementación como se muestra en (B) de la Fig. 4, la comunicación segura con el destino que tiene la dirección de red autenticada puede establecerse sin cambiar una estructura de una capa de comunicación tal como el controlador de enlace de datos 1322 y el socket TCP/IP 1324.

c4: Interacción entre dispositivos

A continuación se describirá una interacción ejemplar entre dispositivos como el dispositivo terminal 100 y el dispositivo servidor 200.

La Fig. 5 es un diagrama esquemático para ilustrar la interacción entre dispositivos en el sistema de red 1 según la presente realización. La Fig. 5 muestra un procesamiento ejemplar cuando se transmiten/reciben datos entre un dispositivo 1 y un dispositivo 2.

Refiriéndose a la Fig. 5, el dispositivo 1 y el dispositivo 2 incluyen cada uno una función de autenticación de red (correspondiente al chip de autenticación de direcciones 112 mostrado en la Fig. 2 o al programa de autenticación de direcciones 136 mostrado en la Fig. 3). La función de autenticación de red de cada dispositivo realiza el procesamiento para autenticar una dirección de red. Este procesamiento de autenticación se realiza básicamente en la capa de red. Una vez completado el procesamiento de autenticación, la función de autenticación de red de cada dispositivo se utiliza como dirección de red en la transmisión/recepción de datos por parte de una aplicación (capa de aplicación) ejecutada en cada dispositivo.

Una aplicación o un socket TCP/IP responsable de la generación y recepción de paquetes puede ser notificado de una dirección de red autenticada.

Adoptando la configuración como se muestra en la Fig. 5, una dirección de red autenticada mutuamente puede ser utilizada sin que se requiera un procesamiento especial de autenticación en el lado de una aplicación.

D. Procedimiento de procesamiento ejemplar

A continuación se describirá un procedimiento de procesamiento ejemplar en el sistema de red 1 según la presente realización.

La Fig. 6 es un diagrama de secuencia que muestra un procedimiento de procesamiento ejemplar implicado en la prestación de un servicio en el sistema de red 1 según la presente realización. La Fig. 6 muestra un procedimiento de procesamiento en un ejemplo típico donde el dispositivo servidor 200 proporciona un servicio solicitado en respuesta al acceso desde el dispositivo terminal 100 al dispositivo servidor 200.

Específicamente, refiriéndose a la Fig. 6, inicialmente, cuando un usuario realiza alguna operación en la aplicación 134 (paso S2), una solicitud de acceso de la aplicación 134 al dispositivo servidor 200 se transfiere a la función de autenticación de red (chip de autenticación de direcciones 112 mostrado en la Fig. 2 o programa de autenticación de direcciones 136 mostrado en la Fig. 3) (paso S4). La función de autenticación de red del dispositivo terminal 100 realiza el procesamiento para la autenticación mutua de una dirección de red entre la función de autenticación de red del dispositivo terminal 100 y la función de autenticación de red (la función correspondiente al chip de autenticación de direcciones 112 mostrado en la Fig. 2 o el programa de autenticación de direcciones 136 mostrado en la Fig. 3) del dispositivo servidor 200 (paso S6). Una vez completado el procesamiento de autenticación, el dispositivo terminal 100 utiliza la dirección de red autenticada para transferir la solicitud de acceso emitida al dispositivo servidor 200 (paso S8).

En el dispositivo servidor 200, la solicitud de acceso transmitida desde el dispositivo terminal 100 es recibida por la función de autenticación de red, sometida al procesamiento necesario y transferida a la aplicación (paso S10). La aplicación del dispositivo servidor 200 identifica la dirección de red utilizada para la comunicación de datos en la solicitud de acceso recibida del dispositivo terminal 100 (paso S12) y determina un servicio a prestar de acuerdo con la dirección de red identificada (paso S14).

A continuación, la aplicación del dispositivo servidor 200 transmite los datos de acuerdo con el servicio determinado al dispositivo terminal 100 (paso S16). Estos datos son recibidos por la función de autenticación de red del dispositivo servidor 200, sometidos al procesamiento necesario y transmitidos al dispositivo terminal 100 (paso S18).

En el dispositivo terminal 100, los datos transmitidos desde el dispositivo servidor 200 son recibidos por la función de autenticación de red, sometidos al procesamiento necesario y transferidos a la aplicación 134 (paso S20). A continuación, la aplicación 134 presenta al usuario contenidos de acuerdo con los datos recibidos (paso S22).

En el sistema de red 1 según la presente realización, cuando se accede al dispositivo servidor 200 desde el dispositivo terminal 100, éste puede proporcionar un servicio específico al dispositivo terminal 100 sin realizar un procesamiento de autenticación adicional, porque la dirección de red incluida en ese acceso ha sido autenticada. En concreto, el dispositivo servidor 200 identifica el dispositivo terminal 100 que ha emitido la solicitud basándose únicamente en la dirección de red utilizada en la interacción con el dispositivo terminal 100 en la capa de red, sin realizar el procesamiento de autenticación en la capa de aplicación.

E. Aplicación ejemplar

A continuación se describirá un servicio ejemplar proporcionado en el sistema de red 1 mostrado en la Fig. 6.

e1: Aplicación ejemplar número 1

Se asume un servidor web como dispositivo servidor 200 y tal configuración como proporcionar una página web específica de acuerdo con una dirección de red del dispositivo terminal 100 que realiza un acceso se describirá inicialmente a modo de ejemplo.

La Fig. 7 es un diagrama para ilustrar una aplicación ejemplar para proporcionar un servicio mediante el uso del sistema de red 1 según la presente realización. La Fig. 7 muestra en (A) una tabla de gestión de red ejemplar 210 mantenida por el dispositivo servidor 200. En la tabla de gestión de red 210, la información de pantalla inicial 214 que representa una pantalla inicial e información de preferencias 216 que representa una preferencia se definen en asociación con una dirección de red (dirección IP) 212 del dispositivo terminal 100 que realizó un acceso en el pasado o que realizará un acceso. Los contenidos de la tabla de gestión de red 210 pueden ser actualizados manualmente por un usuario o por el dispositivo servidor 200 en respuesta a una operación de un usuario.

Cuando se accede al dispositivo servidor 200 desde el dispositivo terminal 100, el dispositivo servidor hace referencia a la tabla de gestión de red 210 con una dirección de red proporcionada al dispositivo terminal 100 que sirve como clave, y determina la información de pantalla inicial 214 y la información de preferencias 216 correspondientes. A continuación, el dispositivo servidor 200 determina el contenido de una página web que se proporcionará al dispositivo terminal 100 que ha realizado un acceso, basándose en la información de pantalla inicial 214 y la información de preferencias 216 determinadas.

La Fig. 7 muestra en (B) una pantalla web ejemplar cuando el dispositivo servidor 200 proporciona un servicio de banca en línea a modo de ejemplo. Por ejemplo, en una pantalla web 220A ejemplar presentada en una pantalla del dispositivo terminal 100 provisto de una dirección IP 1, se disponen botones para la gestión básica de cuentas como "procedimiento de pago", "comprobar saldo" y "procedimiento de transferencia". En una pantalla web ejemplar 220B presentada en la pantalla del dispositivo terminal 100 provisto de una dirección IP 2, se disponen botones relativos a la moneda extranjera, como "comprar moneda extranjera" y "vender moneda extranjera", junto con un gráfico que muestra la variación en el tiempo del tipo de cambio.

Dicha pantalla inicial puede determinarse, por ejemplo, haciendo referencia a la información de pantalla inicial 214 en la tabla de gestión de red 210. Además, haciendo referencia a la información de preferencias 216 en la tabla de gestión de red 210, se puede proporcionar no sólo la pantalla inicial sino también un servicio de acuerdo con la preferencia para cada dispositivo terminal 100 (es decir, un usuario que opera el dispositivo terminal 100).

Como se ha expuesto anteriormente, la pantalla inicial y diversos contenidos de servicio proporcionados en el momento del acceso al dispositivo servidor 200 pueden personalizarse con base en la dirección de red proporcionada al dispositivo terminal 100.

e2: Aplicación ejemplar número 2

Un servidor de gestión de uso en un hotel o similar se asume como dispositivo servidor 200 y tal configuración como

el uso del dispositivo terminal 100 como una llave electrónica (un certificado de uso) se describirá ahora a modo de ejemplo.

La Fig. 8 es un diagrama para ilustrar otra aplicación ejemplar para proporcionar un servicio haciendo uso del sistema de red 1 según la presente realización. La Fig. 8 muestra en (A) una tabla de gestión de uso ejemplar 230 mantenida por el dispositivo servidor 200. La tabla de gestión de uso 230 almacena el contenido de la reserva realizada a través de un sitio de reservas (un número de habitación 234 y un período de estancia permitido 236) en asociación con una dirección de red 232 proporcionada al dispositivo terminal 100 utilizado para una operación de reserva.

Específicamente, cuando un usuario opera su propio dispositivo terminal 100 para hacer una reserva de un alojamiento a través de un sitio de reservas, el dispositivo servidor 200 añade contenido de la reserva a la tabla de gestión de uso 230 junto con la dirección de red proporcionada al dispositivo terminal 100 utilizado para la reserva del alojamiento.

Como se muestra en (B) de la Fig. 8, una unidad de comunicación inalámbrica 242 está dispuesta delante de cada habitación de un alojamiento 240. Cuando un usuario que se aloja en el alojamiento se acerca a una habitación reservada mientras porta el dispositivo terminal 100 utilizado para realizar la reserva del alojamiento, la unidad de comunicación inalámbrica 242 establece una comunicación inalámbrica con el dispositivo terminal 100. La comunicación inalámbrica entre el dispositivo terminal 100 y la unidad de comunicación inalámbrica 242 puede iniciarse automáticamente o en respuesta a una operación explícita del usuario.

A continuación, cuando la dirección de red proporcionada al dispositivo terminal 100 por el usuario coincide con cualquier entrada de la dirección de red 232 en la tabla de gestión de uso 230, el dispositivo servidor 200 desbloquea una habitación reservada basándose en el correspondiente número de habitación 234 y el periodo de estancia permitido 236.

Aunque la Fig. 8 ilustra una configuración en la que el dispositivo terminal 100 se utiliza como llave para cada habitación de un alojamiento como un hotel como ejemplo típico, el dispositivo terminal puede utilizarse como cualquier certificado de uso sin estar limitado como tal. Por ejemplo, el propio dispositivo terminal 100 puede utilizarse como entrada para diversas instalaciones, como un parque de atracciones, o diversos eventos, como conciertos. El propio dispositivo terminal 100 también puede utilizarse como billete de tren o avión.

Como se ha descrito anteriormente, en el sistema de red 1 según la presente realización, ya que la propia dirección de red proporcionada al dispositivo terminal 100 está autenticada, no se requiere una aplicación o similar para mostrar un ticket como en la tecnología existente, y se pueden reducir las barreras para la prevalencia de un sistema en el que el propio dispositivo terminal 100 se utiliza como certificado de uso.

Tal y como se ha expuesto anteriormente, el dispositivo terminal 100 puede utilizarse fácilmente como un certificado arbitrario para su uso basado en una dirección de red proporcionada al dispositivo terminal 100.

e3: Aplicación ejemplar número 3

Ahora se describirá una configuración que realiza el procesamiento para autenticar una dirección de red en sí de una manera más multifacética. La Fig. 9 es un diagrama que ilustra un filtrado ejemplar de una dirección de red utilizando el sistema de red 1 según la presente realización. La Fig. 9 muestra una configuración ejemplar en la que el programa de autenticación de direcciones 136 está dispuesto en una tercera capa (la capa de red) del modelo de referencia OSI y TCP (o UDP) está dispuesto en una cuarta capa (la capa de transporte) a modo de ejemplo.

En la Fig. 9, la información de gestión de autenticación 138 está dispuesta como una configuración para realizar el filtrado. La información de gestión de autenticación 138 puede incluir una lista negra 1382 y/o una lista blanca 1384. Tanto la lista negra 1382 como la lista blanca 1384 no tienen que estar preparadas y sólo se puede preparar una de ellas.

La lista negra 1382 define una dirección de red desde la cual el acceso debe ser bloqueado y la lista blanca 1384 define una dirección de red desde la cual el acceso debe ser permitido.

La Fig. 9 muestra en (A) un ejemplo en el que una función de filtrado es implementada por el programa de autenticación de direcciones 136. Más específicamente, cuando una dirección de red autenticada de un destino coincide con cualquier entrada definida en la lista negra 1382, el programa de autenticación de direcciones 136 corta o prohíbe la comunicación con un destino (un nodo de lista negra) que tenga la dirección de red autenticada. Es decir, un paquete procedente del nodo de lista negra es bloqueado por el programa de autenticación de direcciones 136 y no se entrega a la aplicación 134.

Alternativamente, sólo cuando la dirección de red autenticada coincide con cualquier entrada definida en la lista blanca 1384, el programa de autenticación de direcciones 136 permite la comunicación con un destino (un nodo de lista blanca) que tenga la dirección de red autenticada. A saber, un paquete del nodo de la lista blanca se entrega desde el programa de autenticación de direcciones 136 a la aplicación 134. La aplicación 134 proporciona un servicio basado

en la propia dirección de red autenticada por el programa de autenticación de direcciones 136 y el paquete recibido.

La Fig. 9 muestra en (B) un ejemplo en el que la función de filtrado es implementada por la aplicación 134. Más concretamente, cuando la aplicación 134 recibe un paquete del programa de autenticación de direcciones 136, determina si una dirección de red (autenticada por el programa de autenticación de direcciones 136) de un remitente del paquete coincide o no con alguna entrada de la lista negra 1382 o de la lista blanca 1384.

Cuando la dirección de red del remitente del paquete recibido coincide con alguna entrada definida en la lista negra 1382, la aplicación 134 bloquea el paquete. Cuando la dirección de red del remitente del paquete recibido coincide con cualquier entrada definida en la lista blanca 1384, la aplicación 134 procesa ese paquete y proporciona un servicio solicitado.

Como se ha expuesto anteriormente, además de la función para autenticar la propia dirección de red, combinando la función de filtrado utilizando la lista negra/lista blanca, se puede realizar un sistema de red más práctico.

F. Otra realización

Aunque un sistema de red que incluye uno o más dispositivos terminales 100 y uno o más dispositivos servidores 200 se ilustra como una configuración ejemplar que utiliza una dirección de red autenticada entre dispositivos en la realización descrita anteriormente, la configuración también es aplicable a la comunicación de datos entre dispositivos terminales 100 o entre dispositivos servidores 200 sin estar limitada como tal. Sin limitarse a un marco de trabajo como el dispositivo terminal 100 o el dispositivo servidor 200, la configuración está disponible para la comunicación de datos entre dispositivos arbitrarios.

G. Ventajas

Según la presente realización, se proporciona un servicio que utiliza una dirección de red autenticada y una plataforma para proporcionar ese servicio. Dado que la propia dirección de red está autenticada, el establecimiento de la conexión de comunicación per se también puede servir como procedimiento de autenticación, y no es necesario un procedimiento de autenticación adicional utilizando la aplicación. De este modo, pueden prestarse diversos servicios adecuados para IoT.

Debe entenderse que la realización aquí descrita es ilustrativa y no restrictiva en todos los aspectos. El alcance de la presente invención se define por los términos de las reivindicaciones más que por la descripción anterior y se pretende que incluya cualquier modificación dentro del alcance y significado equivalente a los términos de las reivindicaciones.

Lista de signos de referencia

1 sistema de red; 4 punto de acceso; 6 estación base; 100, 100A, 100B dispositivo terminal; 102 procesador; 104 memoria principal; 106 pantalla; 108 unidad de entrada; 110 módulo de comunicación; 112 chip de autenticación de direcciones; 114, 144 módulo WiFi; 116, 120, 146, 150 antena; 118, 148 módulo LTE; 130 almacenamiento secundario; 132 SO; 134 aplicación; 136 programa de autenticación de direcciones; 138 información de gestión de autenticación; 200 dispositivo servidor; 210 tabla de gestión de red; 212 dirección de red (dirección IP); 214 información de pantalla inicial; 216 información de preferencias; 220A, 220B pantalla ejemplar; 230 tabla de gestión de uso; 232 dirección de red; 234 número de habitación; 236 período de tiempo disponible; 240 alojamiento; 242 unidad de comunicación inalámbrica; 1322 controlador de enlace de datos; 1324 socket TCP/IP.

REIVINDICACIONES

1. Un sistema de red (1) que comprende:

al menos un dispositivo servidor (200, 200-1, 200-2, 200-3); y
un dispositivo terminal (100, 100-1, 100-2, 100-3, 100A, 100B) configurado para acceder a cualquiera del al menos un dispositivo servidor, donde
el dispositivo terminal está configurado para autenticar una dirección de red de cualquiera del al menos un dispositivo servidor y comunicar datos con cualquiera del al menos un dispositivo servidor, y
cuando el dispositivo servidor recibe una solicitud del dispositivo terminal, el dispositivo servidor presta un servicio de acuerdo con una dirección de red autenticada del dispositivo terminal que ha emitido la solicitud, **caracterizado** porque
el dispositivo terminal comprende un primer programa de comunicación (1322; 132) dirigido a una capa de enlace de datos, un segundo programa de comunicación (1324; 132) dirigido a una capa de transporte y una capa de red, y un programa de autenticación de direcciones (136) conectado entre el primer programa de comunicación y el segundo programa de comunicación, y
el programa de autenticación de direcciones está adaptado para autenticar, entre el programa de autenticación de direcciones y el dispositivo servidor, una dirección de red del dispositivo servidor que se utilizará para la transmisión de datos solicitada por el segundo programa de comunicación.

2. El sistema de red según la reivindicación 1, donde
el dispositivo servidor identifica el dispositivo terminal que ha emitido la solicitud, basándose únicamente en la dirección de red utilizada en la interacción con el dispositivo terminal a través de una capa de red, sin realizar el procesamiento de autenticación en una capa de aplicación.

3. Un método para la comunicación en red en un sistema de red (1) con al menos un dispositivo servidor (200, 200-1, 200-2, 200-3) y un dispositivo terminal (100, 100-1, 100-2, 100-3, 100A, 100B) configurado para acceder a cualquiera del al menos un dispositivo servidor, que comprende:
autenticar (S6), en el dispositivo terminal, una dirección de red de cualquiera del al menos un dispositivo servidor;
comunicar (S8, S10), en el dispositivo terminal, datos con el cualquiera del al menos un dispositivo servidor; y
proporcionar (S16, S18, S20, S22), en el dispositivo servidor, un servicio de acuerdo con una dirección de red autenticada del dispositivo terminal que ha emitido una solicitud, cuando el dispositivo servidor recibe la solicitud del dispositivo terminal, **caracterizado** porque
el dispositivo terminal comprende un primer programa de comunicación (1322; 132) dirigido a una capa de enlace de datos, un segundo programa de comunicación (1324; 132) dirigido a una capa de transporte y una capa de red, y un programa de autenticación de direcciones (136) conectado entre el primer programa de comunicación y el segundo programa de comunicación, y
el programa de autenticación de direcciones está adaptado para autenticar, entre el programa de autenticación de direcciones y el dispositivo servidor, una dirección de red del dispositivo servidor que se utilizará para la transmisión de datos solicitada por el segundo programa de comunicación.

4. El método según la reivindicación 3, que comprende, además
identificar (S12), en el dispositivo servidor, el dispositivo terminal que ha emitido la solicitud, basándose únicamente en la dirección de red utilizada en la interacción con el dispositivo terminal a través de una capa de red, sin realizar el procesamiento de autenticación en una capa de aplicación.

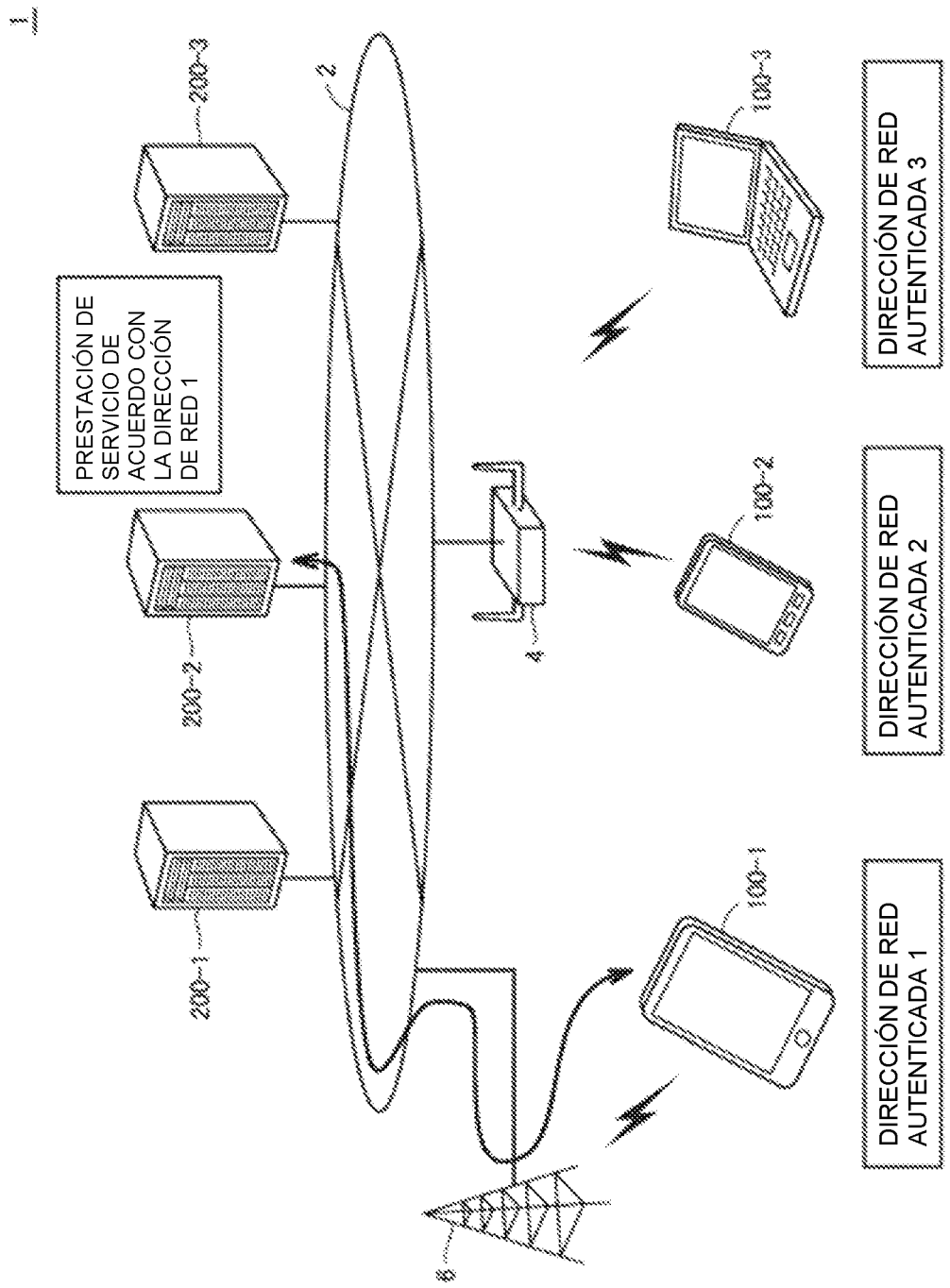

1
200-3
2
PRESTACIÓN DE SERVICIO DE ACUERDO CON LA DIRECCIÓN DE RED 1
200-2
200-1
4
100-3
100-2
100-1
6
DIRECCIÓN DE RED AUTENTICADA 3
DIRECCIÓN DE RED AUTENTICADA 2
DIRECCIÓN DE RED AUTENTICADA 1

Fig. 1

Fig. 2

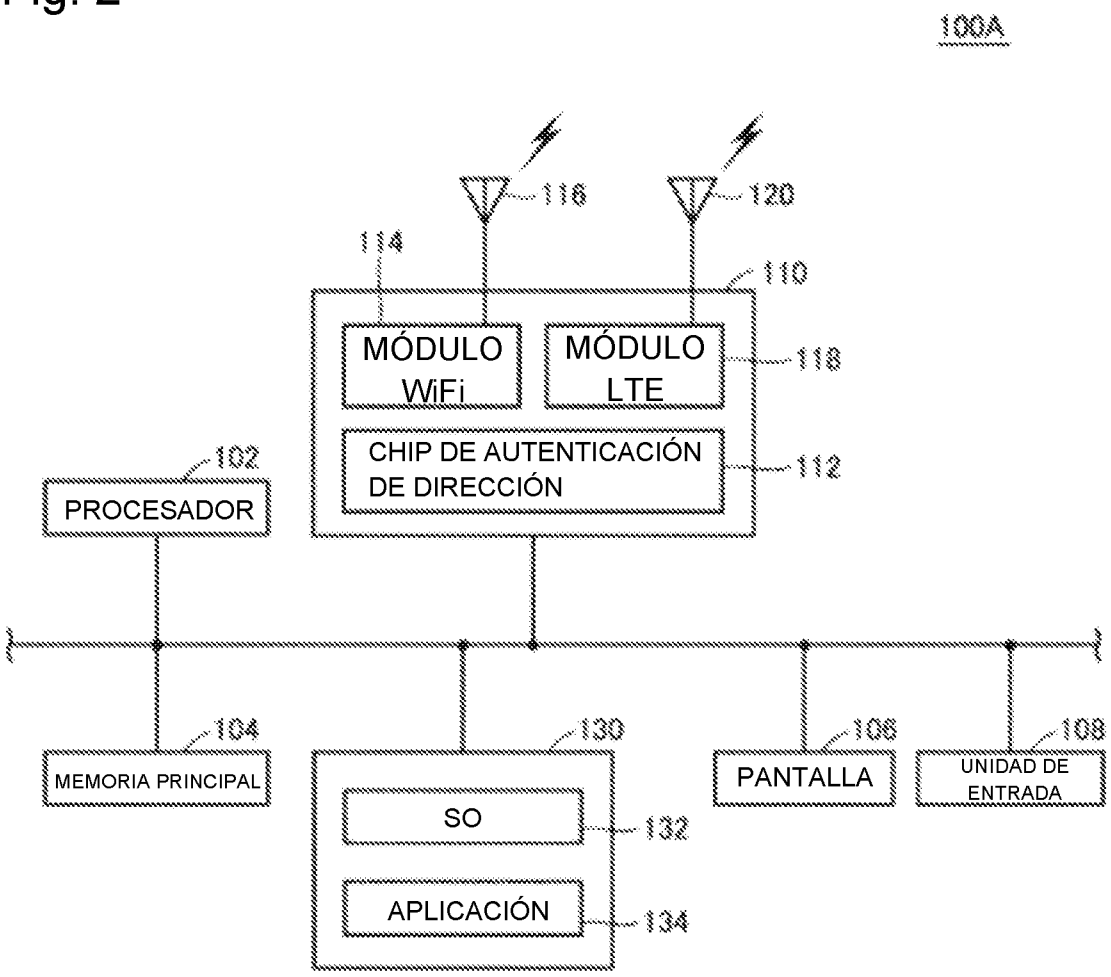

100A
116
120
114
110
MÓDULO WiFi
MÓDULO LTE
118
CHIP DE AUTENTICACIÓN DE DIRECCIÓN
112
102
PROCESADOR
104
MEMORIA PRINCIPAL
130
SO
132
APLICACIÓN
134
106
PANTALLA
108
UNIDAD DE ENTRADA

Fig. 3

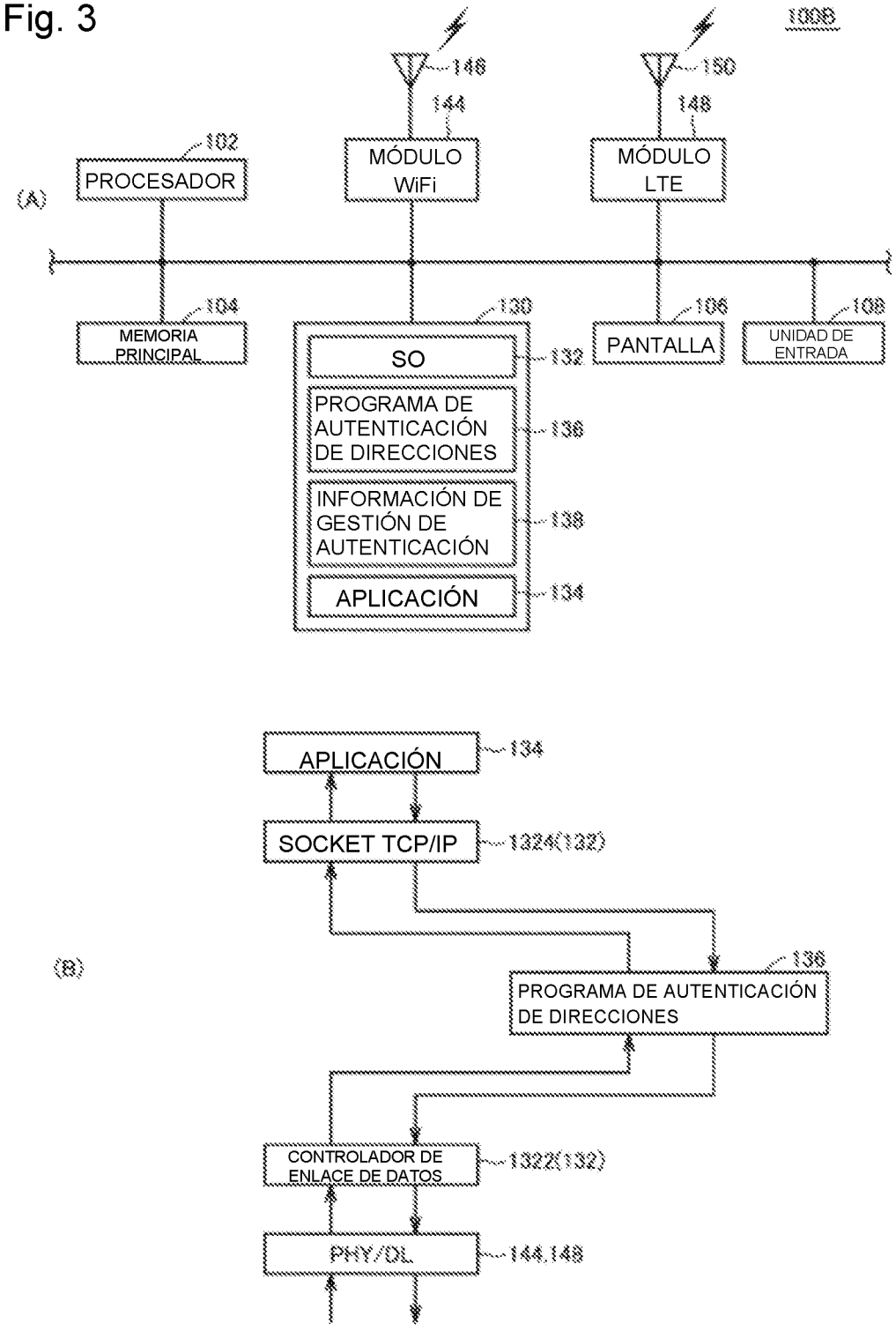

1000
146
150
144
148
102
PROCESADOR
MÓDULO WiFi
MÓDULO LTE
(A)
104
MEMORIA PRINCIPAL
130
SO
132
PROGRAMA DE AUTENTICACIÓN DE DIRECCIONES
136
INFORMACIÓN DE GESTIÓN DE AUTENTICACIÓN
138
APLICACIÓN
134
106
PANTALLA
108
UNIDAD DE ENTRADA
APLICACIÓN
134
SOCKET TCP/IP
1324(132)
(B)
136
PROGRAMA DE AUTENTICACIÓN DE DIRECCIONES
CONTROLADOR DE ENLACE DE DATOS
1322(132)
PHY/DL
144,148

Fig. 4

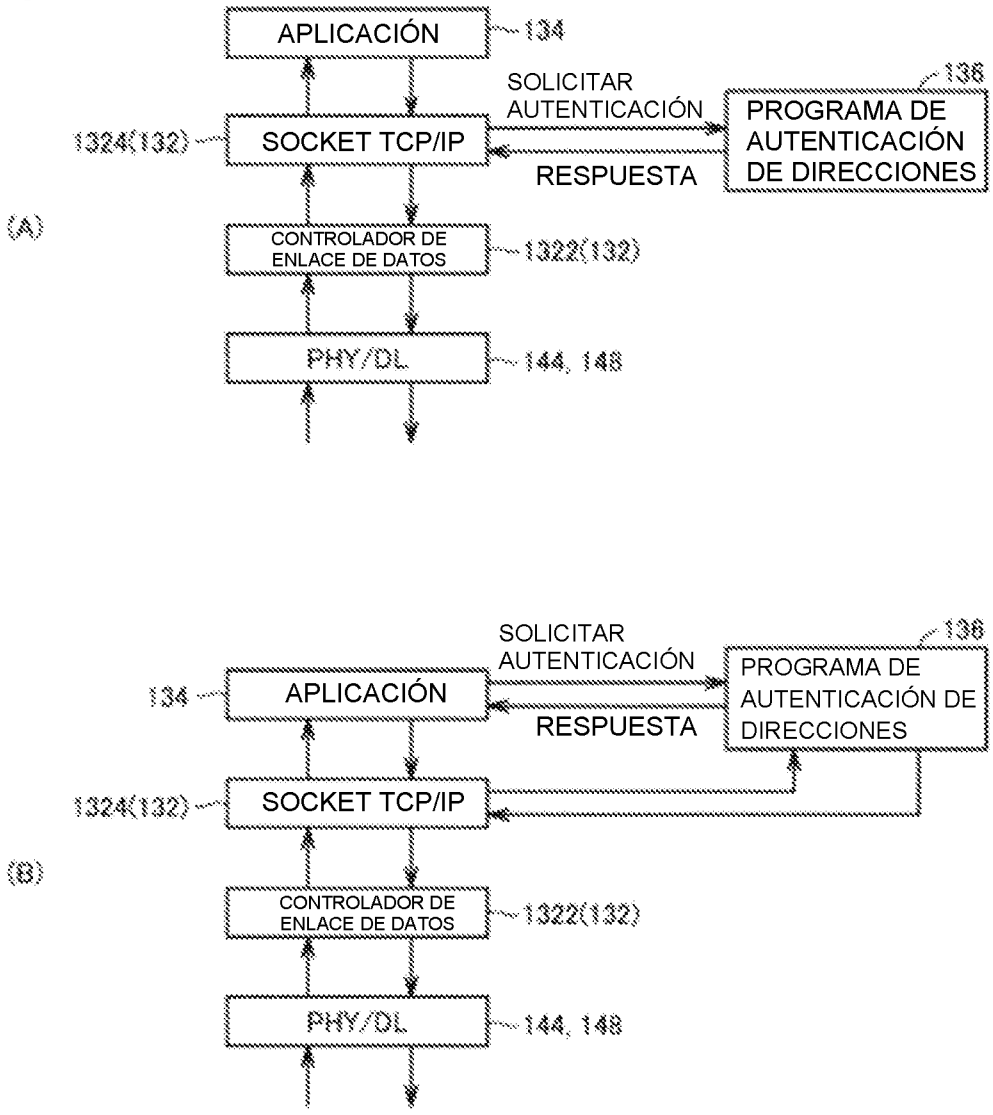

(A)
APLICACIÓN
134
SOLICITAR AUTENTICACIÓN
RESPUESTA
136
PROGRAMA DE AUTENTICACIÓN DE DIRECCIONES
1324(132)
SOCKET TCP/IP
CONTROLADOR DE ENLACE DE DATOS
1322(132)
PHY/DL
144, 148
(B)
SOLICITAR AUTENTICACIÓN
RESPUESTA
136
PROGRAMA DE AUTENTICACIÓN DE DIRECCIONES
134
APLICACIÓN
1324(132)
SOCKET TCP/IP
CONTROLADOR DE ENLACE DE DATOS
1322(132)
PHY/DL
144, 148

Fig. 5

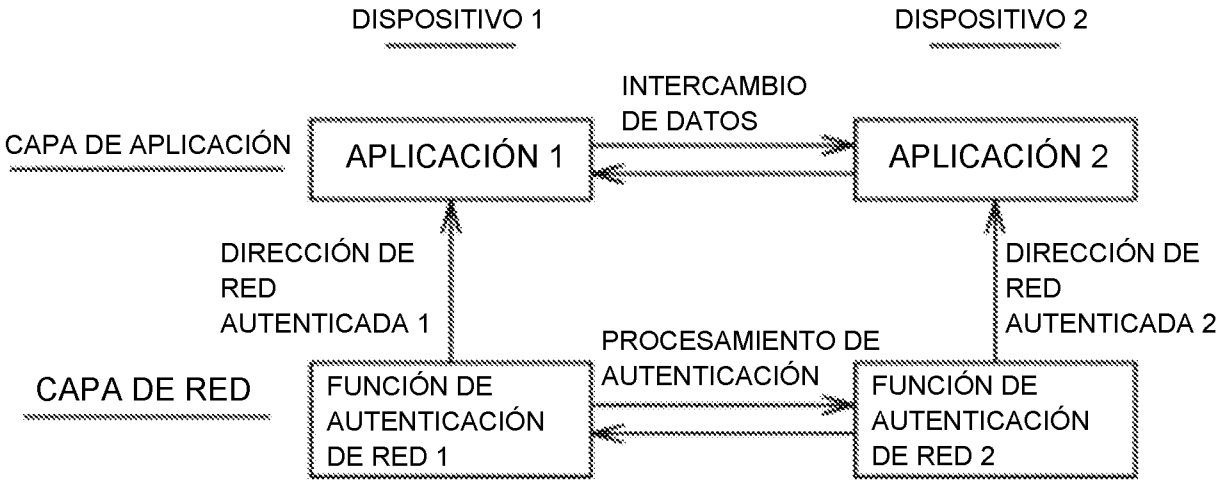

DISPOSITIVO 1
DISPOSITIVO 2
INTERCAMBIO DE DATOS
CAPA DE APLICACIÓN
APLICACIÓN 1
APLICACIÓN 2
DIRECCIÓN DE RED AUTENTICADA 1
DIRECCIÓN DE RED AUTENTICADA 2
PROCESAMIENTO DE AUTENTICACIÓN
CAPA DE RED
FUNCIÓN DE AUTENTICACIÓN DE RED 1
FUNCIÓN DE AUTENTICACIÓN DE RED 2

Fig. 6

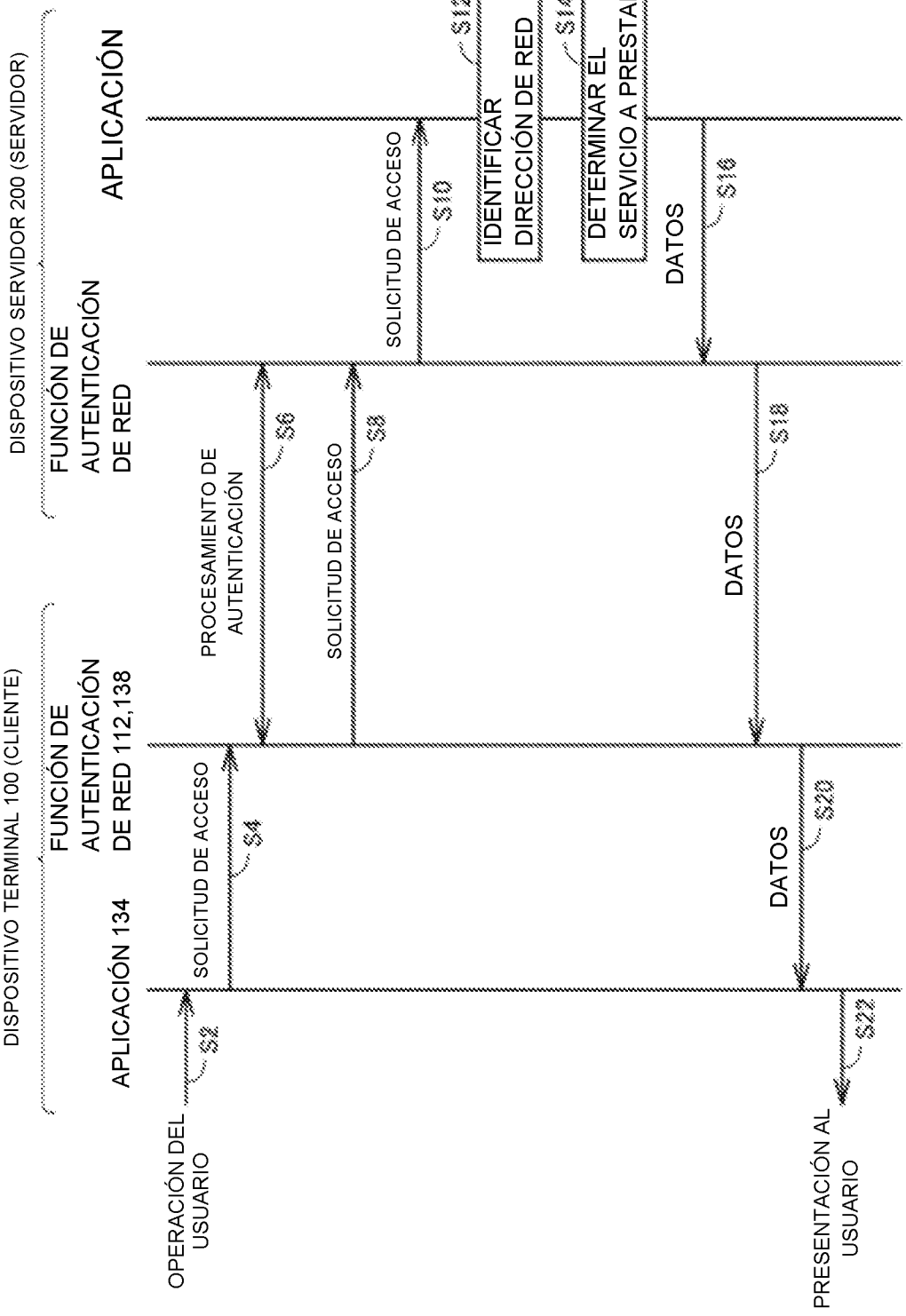

DISPOSITIVO TERMINAL 100 (CLIENTE)
APLICACIÓN 134
FUNCIÓN DE AUTENTICACIÓN DE RED 112,138
DISPOSITIVO SERVIDOR 200 (SERVIDOR)
FUNCIÓN DE AUTENTICACIÓN DE RED
APLICACIÓN
OPERACIÓN DEL USUARIO
S2
SOLICITUD DE ACCESO
S4
PROCESAMIENTO DE AUTENTICACIÓN
S6
SOLICITUD DE ACCESO
S8
SOLICITUD DE ACCESO
S10
S12
IDENTIFICAR DIRECCIÓN DE RED
S14
DETERMINAR EL SERVICIO A PRESTAR
DATOS
S16
DATOS
S18
DATOS
S20
PRESENTACIÓN AL USUARIO
S22

Fig. 7

(A)

210

DIRECCIÓN IP	PANTALLA INICIAL	Número de preferencia
2AB:200FF:FE00:5042	0005	82849416
2AB:282CA:8A00:8627	0004	18384678
8AD:38ED:ACA82:4052	0015	98587518
⋮	⋮	⋮

212 214 216

(B)

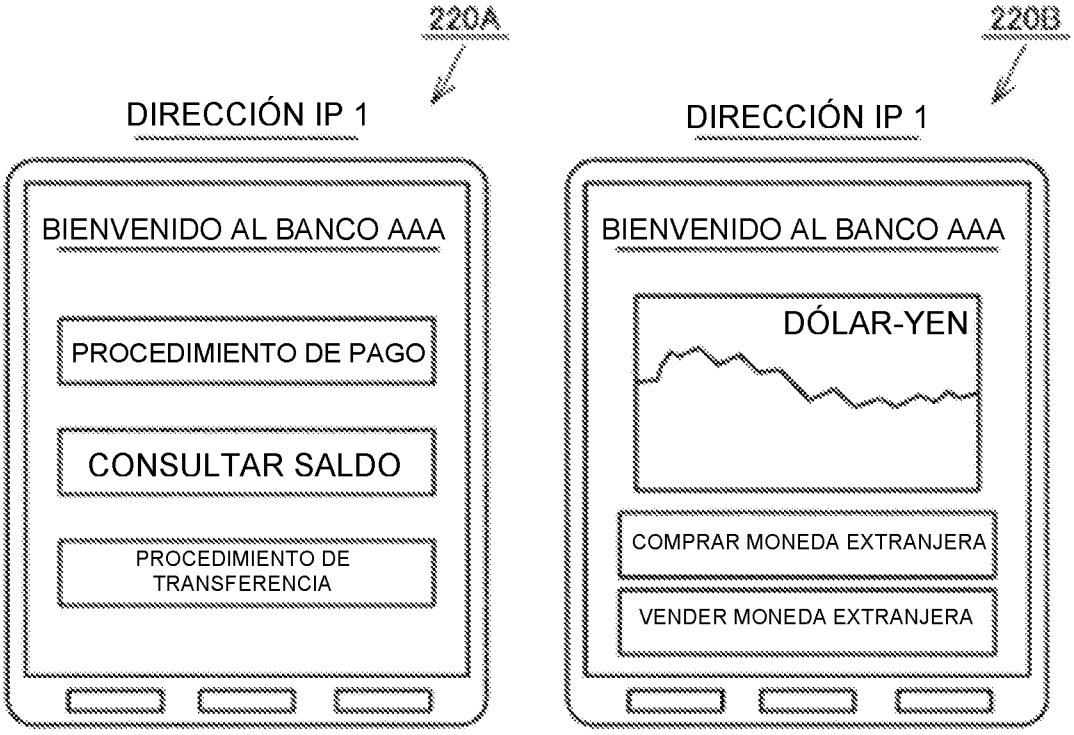


Fig. 8

230

(A)

DIRECCIÓN IP	Número de habitación	VÁLIDO DURANTE
2AB:200FF:FE00:5042	2001	180801:15:00-180802:10:00
2AB:282CA:8A00:8627	2002	180801:15:00-180804:10:00
8AD:38ED:ACA82:4052	2003	180802:15:00-180804:10:00
⋮	⋮	⋮

232 234 236

(B)

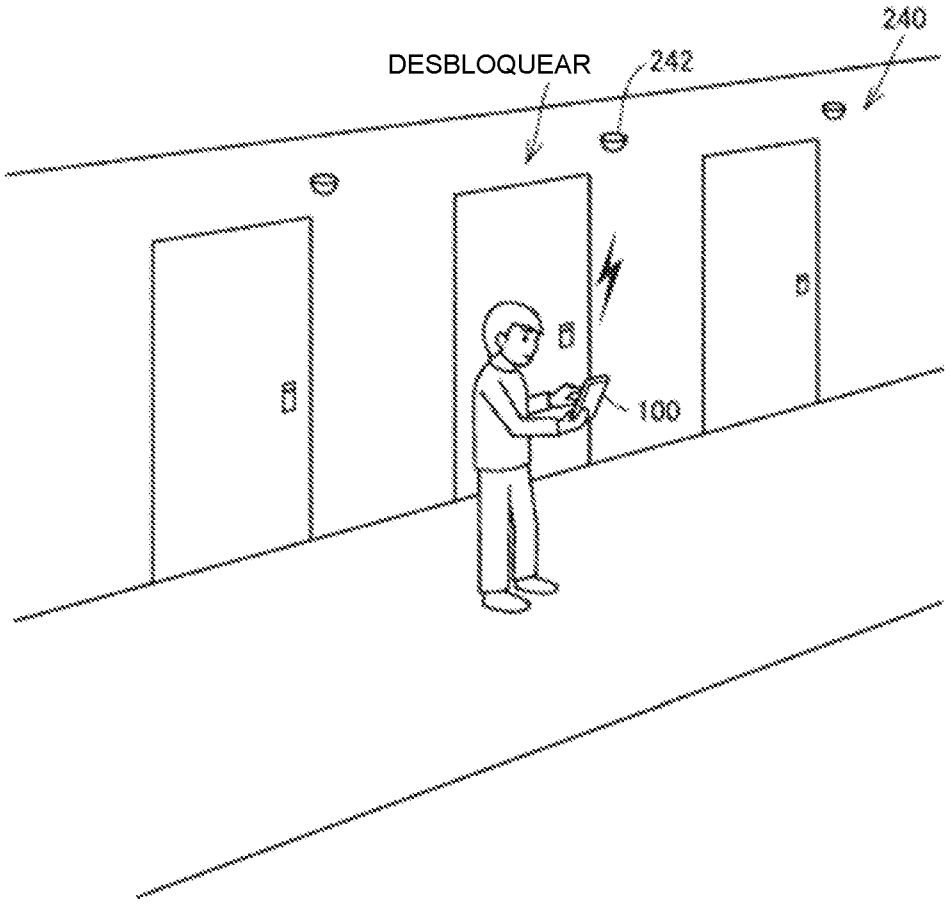
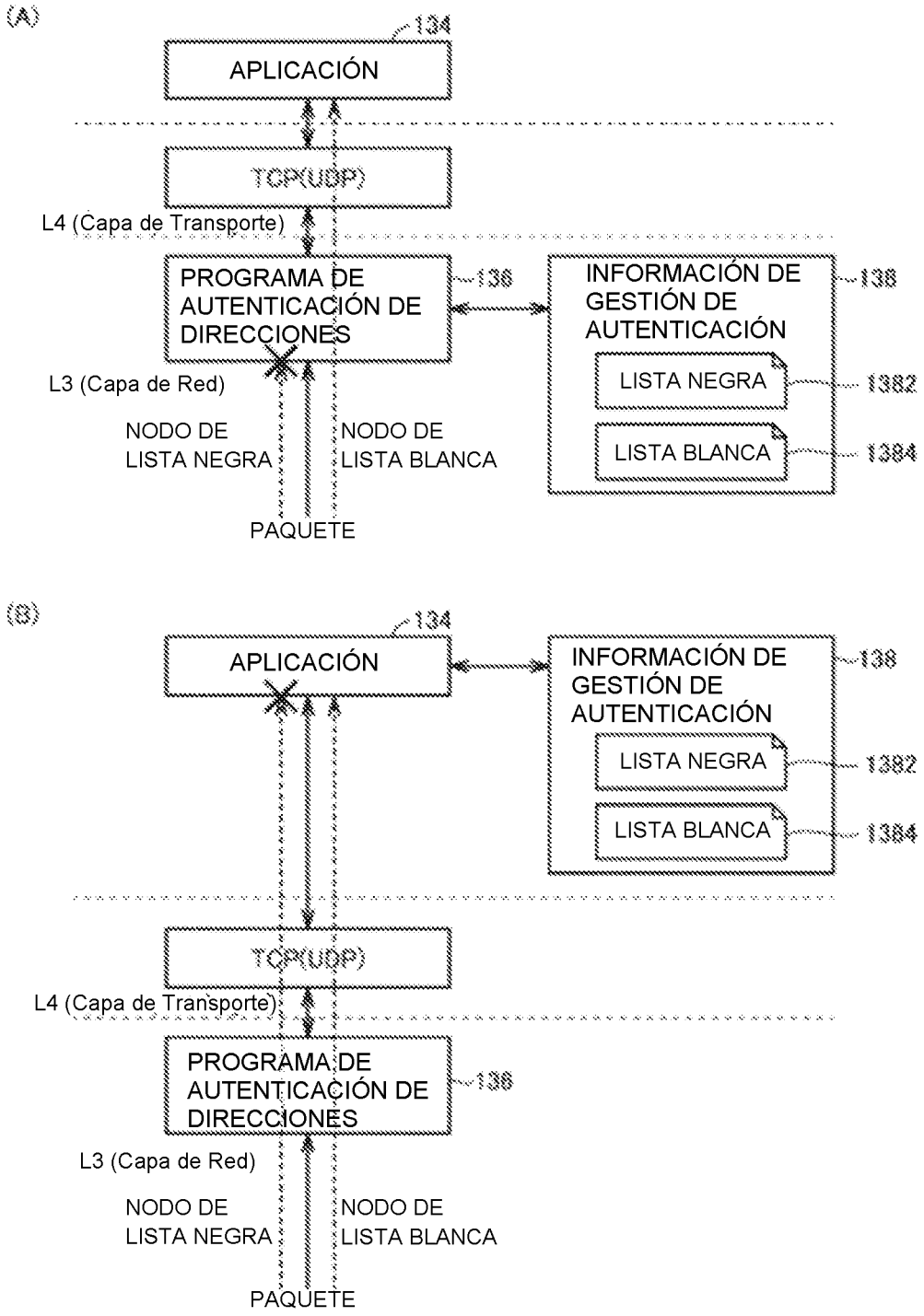


Fig. 9


(A)
134
APLICACIÓN
TCP(UDP)
L4 (Capa de Transporte)
PROGRAMA DE AUTENTICACIÓN DE DIRECCIONES
138
INFORMACIÓN DE GESTIÓN DE AUTENTICACIÓN
138
LISTA NEGRA
1382
LISTA BLANCA
1384
L3 (Capa de Red)
NODO DE LISTA NEGRA
NODO DE LISTA BLANCA
PAQUETE
(B)
134
APLICACIÓN
INFORMACIÓN DE GESTIÓN DE AUTENTICACIÓN
138
LISTA NEGRA
1382
LISTA BLANCA
1384
TCP(UDP)
L4 (Capa de Transporte)
PROGRAMA DE AUTENTICACIÓN DE DIRECCIONES
138
L3 (Capa de Red)
NODO DE LISTA NEGRA
NODO DE LISTA BLANCA
PAQUETE