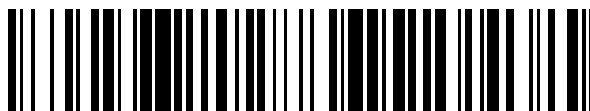


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 609 660**

51 Int. Cl.:

**H04L 12/28** (2006.01)

**H04L 12/46** (2006.01)

**H04L 29/06** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **22.05.2012 PCT/FI2012/050484**

87 Fecha y número de publicación internacional: **29.11.2012 WO2012160257**

96 Fecha de presentación y número de la solicitud europea: **22.05.2012 E 12788813 (9)**

97 Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2715983**

54 Título: **Disposición de dispositivo para implementar un control remoto de propiedades**

30 Prioridad:

**24.05.2011 FI 20115512**

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

**21.04.2017**

73 Titular/es:

**TOSIBOX OY (100.0%)  
Teknologiantie 12 A  
90590 Oulu, FI**

72 Inventor/es:

**YLIMARTIMO, VEIKKO**

74 Agente/Representante:

**CURELL AGUILÁ, Mireia**

ES 2 609 660 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Disposición de dispositivo para implementar un control remoto de propiedades.

5 La presente invención se refiere a un método de control remoto de accionadores en una propiedad y un sistema de control remoto con sus componentes.

10 Los dispositivos y sistemas que se pueden controlar en forma remota cada vez más se instalan dentro de propiedades y casas. El propósito de estos sistemas es asegurar y/o mantener las condiciones dentro de las propiedades, para que el vivir en ellas sea tanto seguro como placentero. El espectro de dispositivos controlados y monitoreados en forma remota es muy amplio. La misma propiedad puede tener dispositivos de diferentes proveedores. Estos dispositivos con frecuencia, no se comunican directamente entre ellos. También es común que cada sistema tenga su propio lógico de operación, cuyo control remoto requiere del uso de una solución de comunicaciones de datos particular.

15 Los proveedores de servicio para edificios han empezado a resolver el problema en forma general, al ordenar a un operador que el objetivo cliente sea su propiedad, lo que representa costos de conexión adicionales, el cual contiene ciertas características acordadas específicas sobre el objetivo y deben mantenerse por separado, ya sea por una red telefónica o por una red de banda ancha, la red de banda ancha puede ser una conexión de banda ancha de red 20 2G/3G permanente. La mayoría de los proveedores han encontrado que este es el modo más fácil de operación para ellos en este momento, incluso cuando cuenta con varias desventajas.

25 Cuando se proporciona una conexión nueva adicional para el objetivo, los asuntos de comunicaciones de datos deben ser acordados por separado con el administrador de la Intranet local. El administrador de la Intranet probablemente tiene que realizar configuraciones de red adicionales para la conexión, de modo que se pueda establecer una conexión remota exitosa.

30 Con frecuencia, se debe esperar una conexión adicional, especialmente una conexión permanente con la red por un tiempo prolongado, incluso de semanas. Cuando finalmente se recibe la conexión, con frecuencia no funciona en la forma acordada cuando se adquirió con el operador, y se debe negociar sobre los procedimientos de reparación y esperar a que el operador actúe sobre el problema.

35 Los operadores siguen prometiendo mucho, con respecto a la operación de las conexiones de banda ancha inalámbricas. Cuando se conecta el objetivo remoto con la nueva conexión inalámbrica y no funciona correctamente, se deben tomar medidas que son tediosas, consumidoras de tiempo, altamente costosas.

40 Los operadores también intentan que los clientes sean usuarios de la conexión al agrupar juntos la conexión, un módem y por ejemplo, un tiempo obligatorio de uso de 24 meses. Sin embargo, no todos los usuarios desean participar en estos acuerdos, más bien, desean "tener su propio régimen".

45 Se puede intentar resolver el uso remoto del objetivo con una solución de aplicación específica. De este modo, el proveedor del dispositivo debe comprar del operador su propia red de radio y formar en ella su nombre privado de punto de acceso (APN); lo cual determina los ajustes de comunicaciones de datos en las redes GPRS( General Packet Radio Service) y HSDPA (High Speed Downlink Packet Access)/HSUPA (High Speed Uplink Packet Access).  
50 Con el uso de la configuración APN, se proporciona una conexión Internet a través de una red 2G/3G/4G inalámbrica en los dispositivos en el objetivo. En tales casos, el usuario debe pagar por separado la conexión y por los módems de interfaz y los programas que habilitan el uso remoto. Con frecuencia, tal conexión adicional no puede o no debe usarse para más de un propósito, por ejemplo, para el uso remoto de dispositivos suministrado por el proveedor de servicios del edificio. En la actualidad, los operadores también limitan la cantidad máxima de transferencia de datos en tales conexiones, que cuando se excede, puede provocar gastos más altos en la facturación para el propietario de la conexión.

55 En los objetivos tipo cooperación de domicilios, que tienen varias propiedades, las propiedades pueden conectarse con el "uso remoto" que ocurre solamente dentro de la Intranet formada entre las propiedades. No se obtiene un contacto remoto real para tales objetivos, cuando el usuario del contacto remoto está físicamente en cualquier otro lugar diferente a una de las propiedades dentro de la Intranet.

60 El documento US2010/0014529 representa cómo es posible en un sistema de comunicación conectar dos aparatos de comunicación de red arbitraria mediante la selección de una ruta apropiada o la identificación de una dirección IP en un entorno que incluye una red que utiliza varios encaminadores NAT.

65 Un aparato de comunicación de red del documento US2010/0014529 incluye una unidad de búsqueda directa que transmite en primer lugar una primera petición de búsqueda directa a otro aparato de comunicación de red arbitrario. Cuando la información referente al otro aparato de comunicación de red se obtiene tras la petición de búsqueda directa, una unidad de control de comunicación de dicho aparato de comunicación de red lleva a cabo la comunicación con otro aparato de comunicación de red basado en la información de búsqueda directa.

5 El aparato de comunicación de red incluye también una unidad de obtención de información de ruta que obtiene información de ruta del aparato de comunicación de red de un servidor que tiene información de ruta de los aparatos de comunicación de red. La unidad de obtención de información de ruta debería solicitar la información de ruta únicamente en un caso, en el que la información referente al aparato de comunicación de red no se obtiene como respuesta a la transmisión de la solicitud de búsqueda directa del aparato de comunicación de red.

10 El documento JP2010086175 muestra cómo es posible proporcionar un acceso remoto a una red LAN sin un sistema de gestión para garantizar la validez de una clave de encriptado para ser utilizada para la autenticación de un usuario y sin utilizar ningún certificado emitido por una autoridad de certificación.

15 En el sistema representado, un usuario introduce su contraseña y datos de identificación de usuario en un ordenador cliente que está conectado con la LAN. Después de que el ordenador cliente genera una clave de encriptado para ser utilizada para la autenticación del usuario y un número de identificación de usuario. La clave de encriptado y el número de identificación de usuario están almacenados en una memoria USB que está conectado con el ordenador cliente. La contraseña y el número de identificación de usuario se transmiten encriptados a un servidor de autenticación de dicha LAN.

20 Cuando el usuario desea acceder a dicho ordenador cliente desde otro ordenador remoto que está situado fuera de dicha LAN, se genera un código de autenticación que utiliza la clave de encriptado mediante la utilización de dicha memoria USB que está conectada con otro ordenador remoto. El código de autenticación generado se transmite al servidor de autenticación de dicha LAN. El servidor de autenticación de dicha LAN lleva a cabo la autenticación del usuario verificando el código de autenticación recibido.

25 Un objetivo de la presente invención es proporcionar una disposición de control remoto para dispositivos técnicos en una propiedad y un método de control remoto que usa esta disposición de control remoto, cuando la conexión de Internet ya existe en las propiedades y hogares se utiliza como tal en el uso remoto de vigilancia y vigilancia del edificio. Con un par de dispositivos de uso remoto según la invención, la conexión del objetivo de la propiedad se altera para ser apropiada para el uso remoto.

30 Las funciones ya existentes de la conexión de red de datos en el objetivo y en la Intranet en el objetivo no se alteran.

35 Los objetivos de la invención se alcanzan con una configuración de dispositivo, en donde un dispositivo de red de control local instalado en forma fija en la propiedad y una clave de la red de control de la casa de la persona que realiza en monitoreo de la propiedad, establecen una conexión de dos vías segura sobre Internet, con base en la información de contacto que recibieron desde el servidor de red de control local según la invención. El dispositivo de red de control local en la propiedad, con el cual están conectados los dispositivos para ser controlados o monitoreados en forma remota en la propiedad, se conecta con un dispositivo de conexión de red/terminal de red en la propiedad, por ejemplo, un módem.

40 Las direcciones IP actuales del dispositivo de red de control local y la clave de red de control local se mantienen en el servidor de red de control local relacionado con la invención, las direcciones IP se usan para establecer una conexión entre tales dispositivos. Debido a los procedimientos adicionales y a los métodos para establecer una conexión según la invención, ambos dispositivos se pueden conectar con una red privada, no pública, y aun así, pueden establecer una conexión de transferencia de datos entre ellos sobre Internet. Ventajosamente, es suficiente establecer una conexión de transferencia de datos sobre Internet entre la clave de red de control local móvil y el dispositivo de red de control local instalado, de modo que los dispositivos en algún punto dentro de la conexión establecida también pueden obtener una dirección IP pública, incluso en forma simultánea, el dispositivo de red de control local y la clave de red de control local tienen direcciones IP no públicas. El servidor de red de control local no participa en establecer la conexión de transferencia de datos real después de que ha enviado las direcciones IP para que queden disponibles para los dispositivos.

50 Una ventaja con el sistema de control remoto de propiedad según la invención es que ambos dispositivos en el par de dispositivos de red de control local pueden buscar su ruta desde su ubicación hasta la dirección IP del dispositivo de la propiedad que se conecta con Internet y para almacenar la ruta buscada en un servidor de red de control local separado en Internet para la identificación y la dirección IP de los pares de dispositivos.

55 Otra ventaja de la invención es que cada par de dispositivos de red de control local según la invención forma, entre ellos, en forma independiente un par de dispositivo único predeterminado o un grupo de dispositivos, que se identifican entre ellos en la red. Debido al método de identificación, la clave de red de control local llevada con el usuario o en un programa de ordenador instalado en algún dispositivo de procesamiento de datos, el programa de ordenador implementa las funciones de una clave de red de control local, establece una conexión de red solamente son su par único de dispositivos de la red de control local y la conexión no puede establecerse con cualquier otro dispositivo de red. De este modo, la clave de red de control local funciona como una clave altamente segura para las "puertas de red" de la propiedad.

Otra ventaja de la invención es que el par de dispositivos del sistema de control remoto según la invención, puede establecer en forma independiente entre ellos con la ayuda de la información de dirección del servidor de red de control local, un modelo OSI seguro de dos vías directo (Open Systems Interconnection Reference Model), un nivel de capa de enlace de datos (Capa 2) o también una conexión de transferencia de datos de nivel de capa de red (Capa 3) a través de los dispositivos de la red local de servicio e Internet (VPN, Virtual Private Network) sin tener una conexión establecida circulando a través de todo el servidor externo. La conexión de transferencia remota asegurada de nivel de capa de enlace de datos es un requerimientos básico para muchos usos flexibles y usos de los dispositivos de control de servicio del edificio.

Otra ventaja de la invención es que el par de dispositivos de red de control local se puede establecer en la conexión con el fabricante o en conexión con el arranque que ocurre después. En ambos casos, el par de dispositivos se forma, ventajosamente, al conectar el dispositivo de red de control local y la clave de red de control local juntos, por ejemplo, a través de un puerto USB, ya sea solo o ambos de ellos reciben el código de identificación de cada uno de ellos.

Otra ventaja de la invención es que en el sistema de control remoto según la invención, los programas de la clave de red de control local con sus identificadores de seguridad y las contraseñas se pueden almacenar en un servidor externo, desde donde se recuperan para una nueva clave de red de control local o un programa instalado dentro de una terminal, el programa simula una clave de red de control local, a cambio de los identificadores de seguridad o contraseñas.

La clave de red de control local según la invención se caracteriza en que puede comprender un procesador, una memoria y un código de programa de ordenador almacenado en la misma, que están configurados para:

- recibir un código de identificación de dispositivo enviado por su propio par de terminales de red, que es un dispositivo de red de control local, con el cual se permite que la clave de control de red local establezca una conexión de transferencia de datos, en el que dicha conexión de transferencia de datos solo se permite entre ellos, y enviar su propio código de identificación de dispositivo a su único par de terminales de red, cuando la clave de red de control local y el par de terminales de red se conectan juntos los puertos USB, y a continuación la clave de red de control está adaptada para:
  - solicitar desde el servidor de red de control local, la información de camino de red de su par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo-a-extremo con su único par de terminales de red;
  - recibir desde el servidor de red de control local, la información de camino de red de su par de dispositivos de terminal de red; y
  - establecer, con la ayuda de la información de camino de red recibida, con su par de terminales de red única, la red privada virtual para el control remoto de los accionadores de una propiedad, a cuya red privada virtual no pertenece el servidor de red de control local.

El dispositivo de red de control local en una propiedad según la invención se caracteriza en que su procesador, la memoria y el código de programa de ordenador almacenado en la misma, para establecer una red privada virtual, están configurados para:

- recibir un código de identificación de dispositivo enviado por su único par de terminales de red, que es una clave de red de control local, con la cual se permite que el dispositivo de control de red local establezca una conexión de transferencia de datos, en el que dicha conexión de transferencia de datos solo se permite entre ellos, y enviar su propio código de identificación de dispositivo a su par de terminales de red, cuando el dispositivo de red de control local y la clave de red de control local están conectados juntos los puertos USB, y a continuación la clave de red de control está adaptada:
  - solicitar desde el servidor de red de control local, la información de camino de red de su único par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo-a-extremo con su par de terminales de red;
  - recibir desde el servidor de red de control local, la información de camino de red de su único par de dispositivos de terminal de red; y
  - establecer, con la ayuda de la información de camino de red recibida, con su único par de terminales de red única, la red privada virtual para el control remoto de los accionadores de una propiedad, a cuya red privada virtual no pertenece servidor de red de control local.

El producto de programa de ordenador para proporcionar las funciones clave de la red de control local que comprende unos medios de código de programa de ordenador adaptados para realizar las siguientes etapas de

código de programa cuando dicho programa se ejecuta en un procesador está caracterizado por que, el programa de ordenador comprende, para ser adaptado para establecer una red privada virtual:

- 5 - unos medios de código para recibir un código de identificación de dispositivo enviado por un único par de terminales de red que es un dispositivo de red de control local, con el cual se permite que la clave de control de red local establezca una conexión de transferencia de datos, en el que se permite dicha conexión de transferencia de datos solo entre ellos, y para enviar su propio código de identificación de dispositivo al único par de terminales de red cuando una clave de red de control local y un dispositivo de red de control local están conectados juntos con sus puertos USB;
- 10 - unos medios de código para solicitar desde el servidor de red de control local la información de camino de red del par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo-a-extremo con el único par de terminales de red;
- 15 - unos medios de código para recibir la información de camino de red del par de terminales de red desde el servidor de red de control local, y
- 20 - unos medios de código para establecer la red privada virtual por medio de la información de camino de red recibida con el par de terminales de red del control remoto de los accionadores en la propiedad, a cuya red privada virtual no pertenece el servidor de red de control local.

El producto de programa de ordenador para proporcionar las funciones del dispositivo de red de control local que comprende unos medios de código de programa de ordenador adaptados para realizar las siguientes etapas de código de programa cuando dicho programa se ejecuta en un procesador está caracterizado por que, el programa de ordenador comprende, para ser adaptado para establecer una red privada virtual:

- 25 - unos medios de código para recibir un código de identificación de dispositivo enviado por su único par de terminales de red, que es una clave de red de control local, con la cual se permite que la clave de control de red local establezca una conexión de transferencia de datos, en la que dicha conexión de transferencia de datos solo se permite entre ellos, y para enviar su propio código de identificación de dispositivo a su único par de terminales de red, cuando la clave de red de control local y un dispositivo de red de control local están conectados juntos con sus puertos USB;
- 30 - unos medios de código para solicitar desde el servidor de red de control local la información de camino de red del par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo-a-extremo con el par de terminales de red;
- 35 - unos medios de código para recibir la información de camino de red de su par de terminales de red desde el servidor de red de control local; y
- 40 - unos medios de código para establecer la red privada virtual por medio de la información de camino de red recibida con su par de terminales de red para el control remoto de los accionadores en la propiedad, a cuya red privada virtual no pertenece el servidor de red de control local;
- 45 - unos medios de código para establecer una red privada virtual por medio de la información de camino de red recibida con el par de terminales de red del control remoto de los accionadores en la propiedad, a cuya red privada virtual no pertenece el servidor de red de control local.

50 Algunas formas de realización ventajosas de la invención son provistas en las reivindicaciones dependientes.

La idea básica de la invención es la siguiente: con el fin de implementar el control remoto en cierta propiedad, se fabrican un par de dispositivos, un dispositivo de red de control local y una clave de red de control local (dispositivo), en donde por lo menos un dispositivo de red de control local y la por lo menos una clave de red de control local (dispositivo) pueden establecer una conexión de transferencia de datos solamente entre ellos. La clave de red de control local (dispositivo) puede ser un dispositivo electrónico separado fabricado para este propósito o puede ser algún dispositivo de procesamiento, en donde se ha instalado un programa de ordenador según la invención, el programa implementa las funciones de la clave de red de control local.

60 El dispositivo de red de control local en la propiedad a ser controlado en forma remota se instala en una red de Intranet existente o en una red de Internet en la propiedad a ser controlada. Establece una subred, una red de Intranet de control, en la red de Intranet o de Internet, con la cual se conectan los diferentes accionadores de la red de Intranet de control a ser controlados en la propiedad, ya sea con una conexión cableada o inalámbrica de transferencia de datos.

65 En una forma de realización ventajosa de la invención, una clave de red de control local individual o varias claves de red de control locales pueden funcionar como el par de dispositivos de dos o más dispositivo de red de control

locales en diferentes propiedades. Los códigos de diferente del dispositivo de red de control local y de la clave de red de control local se almacenan en los dispositivos en conexión con su fabricante o los dispositivos cambian sus códigos de identificación cuando se conectan, por ejemplo, con uno de sus puertos USB. Con el uso de los códigos de identificación, el dispositivo de red de control local y la clave de red de control local pueden establecer una conexión segura de transferencia de datos, de dos vías entre ellos. La conexión de transferencia de datos puede ventajosamente, estar con base en una capa de enlace de datos modelo OSI (Capa 2) o en una capa de red (Capa 3).

En conexión con el arranque, ambos dispositivos determinan la información de ruta de los dispositivos desde su red de ubicación hasta el terminal de red conectada con Internet, la información de ruta es necesaria para establecer la conexión. Esta información de ruta se almacena en el servidor de red de control local según la invención, conectado con Internet. Cuando la clave de red de control local desea establecer una conexión de transferencia de datos a través de Internet a su par de dispositivos en alguna propiedad, recupera su información de ruta del dispositivo de red de control local que funciona como su par desde el servidor de red de control local. Con el uso de la información de ruta obtenida, la clave de red de control local empieza a establecer una conexión de transferencia de datos extremo-a-extremo directa. Cuando se ha establecido la conexión de transferencia de datos directa, la conexión de transferencia de datos VPN directa ventajosamente, usa la capa de red que se ha establecido entre la clave de red de control local y el dispositivo de red de control local en la propiedad.

Un dispositivo de red de control local según la invención se instala en la red de transferencia de datos interna de una propiedad para ser controlada en forma remota entre una red de transferencia de datos interna existente relacionada con el control y gestión de la propiedad y una terminal de la red que se basa en el tráfico desde la propiedad hasta Internet. Todos los dispositivos relacionados con el control de la propiedad se conectan con las entradas del dispositivo de red de control local y la salida del dispositivo de red de control local se conecta con la entrada propuesta para el dispositivo de Intranet del terminal de red que se basa en el tráfico de Internet.

La clave de red de control local según la invención se puede conectar con algún otro dispositivo de transferencia de datos, que tiene la capacidad para establecer la conexión de transferencia de datos con Internet. Los posibles dispositivos de transferencia de datos por ejemplo, son una PC, un ordenador de tableta o un teléfono inteligente. Le conexión de la clave de red de control local con el dispositivo de transferencia de datos puede llevarse a cabo, por ejemplo, con la ayuda de una interfaz LAN (Red de Área Local); o una interfaz WLAN (LAN inalámbrica), una interfaz WAN (Red de Área Amplia), una interfaz USB (Bus Serie Universal) o una interfaz de antena.

En una forma de realización ventajosa de la invención, el programa de ordenador que implementa las funciones de la clave de red de control local se almacena en un medio de almacenamiento de datos portátil, por ejemplo, un bus USB, desde el cual el programa de ordenador se puede instalar en un dispositivo de procesamiento de datos apropiado. El programa instalado en el dispositivo de procesamiento de datos simula todas las funciones de la clave de red de control local.

Cuando la clave de red de control local está conectada con el dispositivo de transferencia de datos conectado con la red local o con el programa de ordenador que implementa las funciones de la clave de red de control local, se instala en el dispositivo de transferencia de datos, la clave de red de control local primero determina su propia ruta a través de las diferentes subredes hasta el servidor de red de control local. Cuando la ruta se confirma, la información de ruta de la clave de red de control local se almacena en el servidor de red de control local según la invención.

Cuando se forma un canal de transferencia de datos extremo-a-extremo de dos vías entre la clave de red de control local y el dispositivo de red de control local, la información de ruta del par de dispositivos a través de las diferentes subredes se almacena en el servidor de red de control local, se utiliza para formar el canal de transferencia de datos. Cuando se ha establecido la conexión de transferencia de datos, la transferencia de datos se lleva a cabo para que el servidor de red de control local ya no participe en la transferencia de datos.

A continuación, la invención será descrita con detalle en la descripción, se hace referencia a los dibujos adjuntos, en los que:

La figura 1 muestra como un ejemplo, una conexión de transferencia de datos de dos vías, según la invención, que se puede establecer entre un control remoto de gestión de dispositivo del control remoto y un control individual o un dispositivo de gestión de una propiedad.

La figura 2 muestra un segundo ejemplo según la invención, en la que se establece la conexión de transferencia de datos de dos vías entre el control remoto de gestión del dispositivo cliente y un control individual o el dispositivo de gestión de la propiedad.

La figura 3 muestra un diagrama de flujo ejemplificativo sobre la forma en que se establece la conexión de transferencia de datos entre el dispositivo cliente y el dispositivo en la propiedad.

La figura 4 muestra un ejemplo de un dispositivo de red de control local según la invención.

La figura 5a muestra un ejemplo de una clave de red de control local según la invención.

La figura 5b muestra otro ejemplo de otra clave de red de control local según la invención; y

La figura 6 muestra un ejemplo de un servidor de red de control local según la invención.

Las formas de realización en la siguiente descripción se proporcionan como ejemplos solamente, y los expertos en la materia podrán comprender la idea básica de la invención también en otra forma diferente a la descrita en la presente memoria. Aunque la descripción se puede referir a cierta forma de realización o formas de realización en varios lugares, no significa que la referencia está dirigida solamente a una forma de realización o que la característica descrita se puede usar solamente con una forma de realización descrita. Las características individuales de dos o más formas de realización se pueden combinar y se pueden proporcionar nuevas formas de realización para la invención.

Las figuras 1 y 2 muestran dos formas de realización 1A y 1B ventajosas del sistema de control remoto según la invención. En los ejemplos de las figuras 1 y 2, una clave de red de control local 42 o un dispositivo 41c de procesamiento de datos, que tiene un software se ha convertido en una clave de red de control local, que se usa para establecer una conexión de transferencia de datos en un dispositivo de red de control local 61 en cierta propiedad. La clave de red de control local o el dispositivo de red de control local 41 convertido en la clave de red de control local según la invención, sin embargo, puede funcionar con dispositivo de red de control locales separados en dos o más propiedades.

En ambas formas de realización de las figuras 1 y 2, la red de transferencia de datos principalmente tiene la misma estructura básica. En ambas figuras, la 1 y la 2, Internet se muestra con la referencia 2. Cierta red pública o la Intranet, referencia 3, también está conectada con Internet 2. La red 3 puede ser una red de transferencia de datos inalámbrica o permanente. En la figura 1, una primera red 4 de transferencia de datos, la red de control remoto local de la propiedad, está conectada con la red 3, con la cual el dispositivo cliente de la red de control remoto local implementa el control remoto, referencia 41a, será conectada. En la figura 2, el dispositivo 41c de procesamiento de datos que simula la clave de red de control local está conectado con la red pública/la red 3 de Intranet.

La Intranet local en la propiedad a ser controlada en forma remota está en las figuras 1 y 2 señalada con el número 5 de referencia. Una segunda red 6 de transferencia de datos, una Intranet de control local según la invención, está conectada con la red 5 Intranet local. Los accionadores 62-65 a ser controlados en forma remota en la propiedad están conectados con la Intranet de control local.

Resultará evidente para los expertos en la materia que también puede haber subredes entre el dispositivo de red de control local 61 y/o la clave de red de control local 42 o 41c, según la invención e Internet 2 como se muestra en las figuras 1 y 2.

En los Ejemplos de las figuras 1 y 2, la segunda terminal de red según la invención, el dispositivo de red de control local 61 (HCND), están conectados con la red de Intranet local 10.0.0.0/24, referencia 5. La red 5 de Intranet local está conectada con Internet 2 con el terminal 51 de red. El terminal 51 de red puede ser un enrutador, un módem o una firewall, que también puede incluir un traductor de dirección de red NAT. En los ejemplos de las figuras 1 y 2, la Intranet 5 local está detrás del firewall FW1 que contiene la función NAT, referencia 51. La dirección IP pública de el firewall FW1 que está en los ejemplos de la figura 1 es 2.240.1.1.2. en la Intranet 5 local la dirección IP interna de el firewall FW1 es 10.0.0.1. Otros dos dispositivos de procesamiento de datos ejemplificativos también están conectados con la red 5 Intranet local, cuyas direcciones IP en la red de Intranet local son 10.0.0.3 y 10.0.0.4.

La red de Intranet de control local 172.17.0.0./24 (HCI), referencia 6, está conectada con la red 5 Intranet local a través del dispositivo de red de control local 61. La dirección IP del dispositivo de red de control local 61 en la red de Intranet de control local es 172.17.0.1 y la red de Intranet local 10.0.0.2. En los ejemplos de las figuras 1 y 2, cuatro dispositivos/servidores 62, 63, 64, 65 están conectados con la Intranet 6 de control local. Los dispositivos/servidores pueden estar conectados con la Intranet 6 de control local con una conexión de transferencia de datos permanente o con una conexión inalámbrica.

La referencia 62 muestra un servidor de red de control de iluminación, cuya dirección IP en la red de Intranet de control local es 172.17.0.5. Para un usuario remoto, el servidor 62 de red de control de iluminación se observa como el dispositivo HCND4.

La referencia 63 muestra el servidor de red de control de calor, cuya dirección IP en la red de Intranet de control local es 172.17.0.3. Para un usuario remoto, el servidor 63 de control de calor, se observa como el dispositivo HCDN1.

La referencia 64 muestra el servidor de cámara de vigilancia, cuya dirección IP en la red de Intranet de control local es 172.17.0.3. Para el usuario remoto, el servidor de red 62 de cámara de vigilancia se observa como el dispositivo

HCDN2.

5 La referencia 65 muestra un servidor de red de acondicionamiento de aire, cuya dirección IP en la red de Intranet de control local es 172.17.0.2. Para un usuario remoto el servidor 65 de red de acondicionamiento de aire se observa como el dispositivo HCDN3.

10 En el ejemplo de la figura 1, la primera terminal de red según la invención, la clave de red de control local 41 (HCNK) está conectada con la red de control remoto local 172.17.0.0/24, referencia 4. La red 4 de control remoto local está detrás del firewall FW2 de la Intranet 3, referencia 31. La dirección IP pública de el firewall NAT 31 en este ejemplo es 240.2.1.2 y la dirección IP interna del firewall NAT es 10.0.1.1.

15 La red de control remoto local 172.17.0.0/24 (HCRN), referencia 4, está conectada con la red 3 de transferencia de datos a través de la clave de red de control local 42 según la invención. La dirección IP de la clave de red de control local 42 en la red de Intranet es 10.0.1.2 y la red de control remoto local 172.17.0.6. En los ejemplos de las figuras 1 y 2, el dispositivo 41a de procesamiento de datos ejemplificativo ha sido conectado con la red 4 de control remoto local, cuya dirección IOP del dispositivo de procesamiento de datos en la red 4 de control remoto local es 172.17.0.7. Este dispositivo 41a de procesamiento de datos se usa, cuando sea deseado para controlar en forma remota los dispositivos/servidores 62, 63, 64 o 65 conectados con la red 6 de Intranet de control local.

20 La clave de red de control local 42 y el dispositivo de red de control local 61 según la invención necesitan la información de ruta de cada uno, con el fin de tener la capacidad de establecer entre ellos una conexión de transferencia de datos extremo-a-extremo, con base en la capa de enlace de datos o la capa de red, en los ejemplos de las figuras 1 y 2, una conexión 55 de transferencia de datos VPN. La información de ruta se almacena por la clave de red de control local 42 y por el dispositivo de red de control local 61 según la invención, en un servidor de red de control local 21 (HCNS) en Internet.

30 En el ejemplo de la figura 1, los firewalls NAT no restringen por completo la comunicación UDP saliente. Son referidos como los firewalls NAT en un estado y "con memoria" que tampoco cambian los números de puerto de la fuente de las conexiones UDP (Protocolo de Datagrama del Usuario), cuando no los tienen. En el ejemplo de la figura 1, el objetivo es establecer en la capa de enlace de datos una conexión de nivel Ethernet entre la clave de red de control local 42 y el dispositivo de red de control local 61.

35 Cuando en el sistema 1A de control remoto según la figura 1, se desea establecer una conexión 55 de transferencia de datos que pertenece a una red privada virtual (VPN) entre los dispositivos, entonces ambos dispositivos, el 42 y el 61, recuperan desde el servidor de red de control local 21 la información de ruta almacenada en el mismo por el dispositivo de contraparte. Antes de presentar la información de ruta, el servidor de red de control local 21 verifica que pertenezca realmente a una clave de red de control local/par de dispositivos de red de control local permitidos. Con la ayuda de la información de ruta recuperada, la clave de red de control local 42 y el dispositivo de red de control local 61 establecen una conexión VPN directa entre ellos. Cuando la conexión 55 VPN está completa, el dispositivo 41a de procesamiento de datos en la red 4 de control remoto local puede hacer contacto con un dispositivo 62, 63, 64 o 65 en la red 6 de control local.

45 Para que sea posible establecer la conexión de transferencia de datos, la clave de red de control local 42 y el dispositivo de red de control local 62 deben determinar su camino de red desde su propia red por lo menos hasta Internet 2. Esta determinación del camino de red puede hacerse por ejemplo, en las siguientes formas, en donde la clave de red de control local 42 y el dispositivo de red de control local 61 se utilizan ventajosamente.

50 Con un protocolo DHCP (Dynamic Host Configuration Protocol) se pueden recuperar los ajustes IP para la interfaz de red del dispositivo de procesamiento de datos. Los ajustes que se pueden obtener con el procedimiento DHCP son por lo menos la dirección IP del dispositivo de procesamiento de datos, la máscara de red, la pasarela por especificación y el servidor DNS (Sistema de Nombre de Dominio), el cual transforma los nombres del dominio en direcciones IP.

55 Un procedimiento de trazar ruta, es una herramienta que usa un protocolo TCP/IP, la cual determina la ruta o transferencia de paquetes del camino de red para la máquina determinada. En el procedimiento de trazar ruta, el dispositivo de transferencia de datos conectado con la red confirma el camino de red al añadir el valor Tiempo a Vida (TTL) de los paquetes que envía, uno por vez, empezando desde cero.

60 La confirmación del camino de red típicamente ocurre en la siguiente forma. El dispositivo de procesamiento de datos envía a la pasarela por especificación un paquete IP con alguna dirección objetivo en la red externa con el uso del valor "0" TTL. La pasarela por especificación responde a esto con un mensaje de TTL expirado. Por ejemplo, la dirección IP, el retraso, etc., de la pasarela por especificación que libera este mensaje.

65 Después, el dispositivo de procesamiento de datos envía a la pasarela por especificación un paquete IPO con alguna dirección objetivo en la red externa con el uso de un valor 1 TTL. Otra vez, el enrutador sigue la pasarela por especificación y responde con un mensaje "TTL expirado", desde el cual, la dirección IP del siguiente enrutador



(segundo) queda libre. Este proceso de transmisión/respuesta se continúa al incrementar el valor TTL hasta que se alcance el objetivo deseado. En este caso de Internet, el objetivo final típicamente se alcanza con un valor TTL de 6-15. El resultado final es que el dispositivo de procesamiento de datos conoce el camino de red para el mundo exterior, por ejemplo, Internet.

5 Un protocolo ICMP (Protocolo de Mensaje de Control Internet) se puede utilizar para confirmar las direcciones externas. Una etiqueta de ruta de registro de un paquete ICMP se usa en el procedimiento ICMP; la etiqueta solicita a las capas operativas de los dispositivos en el camino de la red a registrar el título del paquete ICMP, la dirección IP del enrutador de transmisión.

10 En el ejemplo de la figura 1, las determinaciones de ruta de red se llevan a cabo por la clave de red de control local 41 y por el dispositivo de red de control local 61 con al menos uno de los procesos antes descritos. Estos dispositivos almacenan los caminos de red descubiertos en el servidor de red de control local 21, el cual los almacena en su memoria.

15 La clave de red de control local 42 y el dispositivo de red de control local 61 según la invención, ventajosamente, también tienen la capacidad de determinar un ciberespacio libre. Los dispositivos están configurados para determinar para sí mismos un ciberespacio disponible automáticamente, con el uso de la información de camino de red en el servidor de red de control local 21. Los dispositivos solicitan al servidor de red de control local 21 a dar cierta parte libre de ciberespacio. El servidor de red de control local 21 examina los caminos de red que ha recibido y regresa algún bloque de red, en donde no se menciona ninguna dirección en el camino de red de cualquier dispositivo conocido.

20 El dispositivo de red de control local 61 también ventajosamente, ofrece los servicios DHCP y DNS en sus propias subredes 4 y 6 para los dispositivos conectados con las mismas. Además, la clave de red de control local 42 y el dispositivo de red de control local 61 funcionan como una pasarela por especificación para los dispositivos conectados con la subred.

25 La figura 2 muestra otro sistema 1B de control remoto según la invención. En la figura 2, el dispositivo 41c de procesamiento de datos utilizado por el usuario está conectado con una red de transferencia de datos ilustrada con el número 3 de referencia. La forma de realización de la figura 2 difiere de la forma de realización de la figura 1 en que las funciones de la clave de red de control local 42 de la figura 1 se sustituyen con una memoria 42b USB, que se puede conectar con un dispositivo 41c de procesamiento de datos utilizado por el cliente. En esta forma de realización, el dispositivo 41c de procesamiento de datos y la memoria 42b USB juntos forman la clave de red de control local.

30 En otra forma de realización conveniente de la invención, el programa de ordenador que implementa las funciones de la clave de red de control local según la invención, es instalado desde la memoria 42b USB hasta en el dispositivo 41c de procesamiento de datos.

35 Ventajosamente, el programa de ordenador se puede almacenar en el dispositivo 41c de procesamiento de datos por ejemplo, desde el bus 42b USB al acoplar el bus USB con el puerto USB en el dispositivo 41c de procesamiento de datos. Para los expertos en la materia será evidente que se pueden usar otros medios de almacenamiento de datos como el medio de almacenamiento para el programa de ordenador. En esta forma de realización, el dispositivo 41c de procesamiento de datos simula la clave de red de control local según la invención, con el programa de ordenador instalado en el mismo.

40 En la figura 2, la clave de red de control local 42 de la figura 2 se simula en su totalidad o en parte en el dispositivo 41c de procesamiento de datos del usuario. El usuario hace contacto con este software de simulación con un navegador de su dispositivo 41c de procesamiento de datos, o en forma alternativa, el software de simulación abre una ventana de navegador en el dispositivo 41c de procesamiento de datos. La simulación se inicia al arrancar el programa de simulación según la invención, en el dispositivo 41c de procesamiento de datos, el programa de simulación implementa todas las funciones de una clave de red de control local 42 por el software.

45 En esta forma de realización, todas las funciones de la clave de red de control local 42 de la figura 1, es decir, la comunicación, el establecimiento de arranque y conexión se implementan con el dispositivo 41c de procesamiento de datos del usuario, por lo cual la clave de red de control local 42 de la figura 1 no se necesita para establecer una conexión con un par 61 de dispositivos en la propiedad.

50 Cuando por alguna razón el establecimiento de tal túnel VPN directo no se exitoso entre la clave de red de control local 42, 42b o 41c y el dispositivo de red de control local 61 presentados en las figuras 1 y 2 o es exitosa solamente en ocasiones, las disposiciones de control remoto descritas pueden utilizar una doble clave de red de control local conectada con Internet 2, la cual ayuda en el establecimiento y mantenimiento de la conexión. En dicho sistema de control remoto, la clave de red de control local doble ayuda a crear el túnel VPN al formar dos túneles VPN que están dispuestos desde diferentes ubicaciones dentro de un solo túnel VPN. Para el usuario del dispositivo cliente, el sistema de control remoto funciona en la misma forma que en los sistemas de control remoto presentados en la

figura 1 o en la figura 2.

A continuación se presenta un ejemplo de la operación del sistema 1A de control remoto según la invención, en el Ejemplo de la figura 1.

5 El dispositivo de red de control local 61:

10 El dispositivo de red de control local 61 está conectado con la red 10.0.0.0/24 (la Intranet 5 local) por ejemplo, al acoplar un cable con el puerto WAN del dispositivo de red de control local 61. El dispositivo de red de control local 61 automáticamente recupera sus ajustes IP con el procedimiento DHCP. Un firewall FW1 en la red 5 Intranet de inicia, ventajosamente funciona como el servidor DHCP, el firewall proporciona al dispositivo de red de control local 61 la dirección IP 10.0.0.2 en una máscara de red de 24 bits (255.255.255.0). el servidor DHCP también proporciona la dirección del enrutador por especificación 10.0.0.1 y la dirección del servidor DNS 10.0.0.1.

15 El dispositivo de red de control local 61 empieza la comunicación al confirmar, con la ayuda del servidor DENS, la dirección IP del servidor de red de control local 21 (HCNS; direcciones DNS etahallinta.fi). El servidor DNS 10.0.0.1 proporciona la dirección IP del servidor de red de control local 21 como 240.1.1.1.

20 El dispositivo de red de control local 61 hace contacto 240.1.1.1 con el servidor de red de control local 21 sobre Internet con un protocolo TCP o UDP. El dispositivo de red de control local 61 autentica los derechos operativos mutuos con el servidor de red de control local 21 con certificados y/o contraseñas determinadas en conexión con la fabricación. Esta conexión de transferencia de datos ventajosamente, está encriptada por ejemplo, con un encriptado SSL/TLS. El servidor de red de control local 21 busca la conexión entrante de la dirección IP pública del dispositivo de red de control local 61, que en el ejemplo de la figura 1 es 240.1.1.2. El dispositivo de red de control local 61 notifica al servidor de red de control local 21 de su propia dirección y la máscara de red (10.0.0.2/24). El servidor de red de control local 21 almacena esta información en su base de datos.

25 El dispositivo de red de control local 61 ventajosamente también lleva a cabo una operación de trazar la ruta hacia el servidor de red de control local 21 y reporta el camino de red al servidor de red de control local 21. El servidor de red de control local 21 almacena el camino de red recibido del dispositivo de red de control local 61 en su base de datos.

30 Después, el dispositivo de red de control local 61 ventajosamente, también lleva a cabo una operación de Ruta de Registro ICMP y reporta la ruta descubierta al servidor de red de control local 21. El servidor de red de control local 21 almacena la ruta recibida desde el dispositivo de red de control local 61 en su base de datos.

35 Después, el dispositivo de red de control local 61 lleva a cabo una determinación automática del ciberespacio libre al enviar un interrogatorio al servidor de red de control local 21. El servidor de red de control local 21 regresa al dispositivo de red de control local 61 en los ejemplos de las figuras 1 y 2, el ciberespacio 172.17.0.0/24.

40 El dispositivo de red de control local 61 toma el ciberespacio dentro del uso para su Intranet 6 y como su propia dirección IP, el dispositivo de red de control local 61 toma 172.17.0.1. El dispositivo de red de control local 61 notifica al servidor de red de control local 21 acerca de la toma de uso, el servidor almacena esta información en su base de datos.

45 En las figuras 1 y 2, el dispositivo de red de control local 61 se muestra con su propio dispositivo separado, el cual establece su propia subred para controlar los dispositivos en una propiedad. Será evidente para los expertos en la materia que las funciones del dispositivo de red de control local 61 se pueden integrar como parte de un dispositivo de ingeniería casera o de cómputo, que tiene una capacidad suficiente de procesador y de memoria, y medios de conexión para conectar los diferentes medios técnicos con una conexión de transferencia de datos cableada o con una conexión de transferencia de datos inalámbrica.

50 La clave de red de control local 42:

55 El puerto WAN de la clave de red de control local 42 está conectado con la red 10.0.1.0/24 (red 3 de transferencia de datos). La clave de red de control local 21 recupera la información de la dirección IP desde el servidor DHCP, con el cual funciona el firewall FW2, referencia 31. La clave de red de control local obtiene la dirección IP 10.0.1.2. la dirección del enrutador 31 por especificación de la clave de red de control local 42 es 10.0.1.1 y la dirección del servidor 31 DNS es 10.0.1.1, que se obtienen del servidor DHCP.

60 La clave de red de control local 42 empieza la comunicación al confirmar, con la ayuda del servidor DNS, la dirección IP del servidor de red de control local 21 (HCNS, dirección DNS hcns.fi). En los ejemplos de las figuras 1 y 2, el servidor DNS 10.0.1.1 proporciona 240.1.1.1 como la dirección IP del servidor de red de control local 21.

65 Después, la clave de red de control local 42 hace contacto con el servidor de red de control local 21 en la dirección 240.1.1.1 sobre Internet principalmente con el protocolo UDP, y después con el protocolo TCP. La clave de red de control local 42 autentica los derechos operativos mutuos con el servidor de red de control local 21 con los

5 certificados y/o contraseñas pre-distribuidas. La conexión de transferencia de datos ventajosamente, está encriptada, por ejemplo, con un encriptado SSL/TLS. El servidor de red de control local 21 busca la conexión entrante de la dirección IP pública 240.2.1.2 de la clave de red de control local 42. La clave de red de control local 42 también notifica al servidor de red de control local 21 de su propia dirección y la máscara 10.0.1.2724 de red. El servidor de red de control local 21 almacena esta información en su base de datos.

Después, la clave de red de control local 42 lleva a cabo una operación de traza de ruta y reporta el camino de red descubierto al servidor de red de control local 21, que almacena la información en su base de datos.

10 La clave de red de control local 42 ventajosamente también lleva a cabo una operación de ruta de registro ICMP y reporta el camino de red descubierto al servidor de red de control local 21, que almacena la información en su base de datos.

15 El servidor de red de control local 21 verifica la información de ruta recibida y cuando se traslapa, el servidor de red de control local 21 lo reporta a la clave de red de control local 42, y cuando es necesario, lleva a cabo la determinación automática del ciberespacio libre otra vez.

El dispositivo 41c de procesamiento de datos como la clave de red de control local:

20 En la forma de realización IB según la figura 2, la clave de red de control local 42 ha sido reemplazada con el dispositivo 41c de procesamiento de datos del usuario, en donde el programa de ordenador comprende las funciones de la clave de red de control local que ha sido almacenada (referencia 42e) desde la clave de red de control local 42b, según la segunda forma de realización de la clave de red de control local 1. La clave de red de control local 42b puede también ser denominado bus USB. En la forma de realización de la figura 2, las  
25 funciones antes descritas de la clave de red de control local 42 se llevan a cabo por el programa de ordenador instalado en el dispositivo 41c de procesamiento de datos del usuario desde el bus 42b USB.

Un ejemplo para controlar un accionador con el uso del sistema 1A de control remoto.

30 Algún dispositivo está conectado con el sistema 1A de control remoto al conectar el dispositivo a ser conectado con una interfaz Intranet del dispositivo de red de control local 61 ya sea con una conexión permanente o inalámbrica.

35 Por ejemplo, un servidor 63 de red de control de calor (HCWS) está conectado con la red 6 Intranet de control local. En este ejemplo, después de que se conecta el servidor 63 de red de control de calor, el servidor 63 de red de control de calor recupera sus ajustes IP con el servicio DHCP. EL servidor de red de control de calor obtiene desde el dispositivo 61 172.17.0.4 de red de control local su propia dirección 172.17.0.1, como la dirección del enrutador por especificación, 172.17.0.1, como la dirección del servidor DNS. Además, obtiene desde el servidor DNS hcws.hcnd.local, como su nombre en el ejemplo de la figura 1.

40 El dispositivo de red de control local 61 almacena la información DHCP y la proporciona al servidor 63 de red de control de calor en su base de datos local.

45 La clave de red de control local 42 está predeterminada para formar un par con el dispositivo de red de control local 61. De esta forma es posible establecer una conexión de transferencia de datos directa entre la Intranet 6 de control local y la red 3 Ethernet, con la cual está conectada la clave de red de control local 42.

50 La clave de red de control local 42 empieza el proceso de emparejado. Notifica al servidor de red de control local 21 que desea establece una conexión de transferencia de datos con el dispositivo de red de control local 61, ventajosamente, al usar el protocolo UDP. El servidor de red de control local 61 decide que la conexión de transferencia de datos debe establecerse con los siguientes números de puerto:

- la clave de red de control local: puerto fuente UDP 10500, puerto objetivo UDP 10501, dirección IP objetivo 240.1.1.2
- 55 - el dispositivo de red de control local: puerto fuente UDP 10501, puerto objetivo UDP 10500, dirección IP objetivo 240.2.1.2.

60 El servidor de red de control local 21 reporta esta información a la clave de red de control local 42 y al dispositivo de red de control local 61.

Después, la clave de red de control local 42 envía el paquete UDP a la dirección 240.1.1.2 con el puerto 10500 fuente para el puerto 10501 objetivo. Este paquete enviado obtiene el paso a través del firewall FW2, la cual contiene una función NAT; ya que el tráfico saliente está muy restringido. El firewall 31 FW2 recuerda el paquete UDP como una conexión para los siguientes X segundos con la información de contacto 10.0.0.2; 240.1.1.2, 10500 y  
65 10501.

## ES 2 609 660 T3

El paquete UDP alcanza el firewall 51 FW1, que no permite en tráfico entrante y deja caer el paquete. El paquete no llega a la dirección 10.0.02.

5 El dispositivo de red de control local 61 envía el paquete UDP a la dirección 240.2.1.2 con el puerto 10501 fuente hasta el puerto 10500 objetivo. El paquete UDP enviado obtiene el paso a través del firewall 51 NAT FW1, debido a que el tráfico saliente no está restringido. El firewall 51 FW1 recuerda el paquete UDP como una conexión para los siguientes X segundos con la información de contacto 10.0.0.2; 240.2.1.2, 10501 y 10500.

10 El paquete UDP alcanza el firewall 31 FW2. El firewall 31 FW2 recuerda que la dirección IP 10.0.1.2 ha establecido la dirección UDP para la dirección 240.1.1.2 con el puerto 10500 fuente y el puerto 10501 objetivo. Debido a que el paquete UDP llega desde la dirección 240.2.1.2 fuente con el puerto 10501 fuente y con el puerto 10500 objetivo, el firewall 31 FW2 interpreta el paquete como una comunicación de retorno relacionada con la conexión establecida por el dispositivo 10.0.1.2. El firewall FW2 después lleva a cabo una operación de cambio de dirección. Cambia la dirección objetivo del paquete UDP a 10.0.1.2. Después, el firewall 31 FW2 enruta el paquete UDP a la dirección 15 10.0.1.2. Ahora la clave de red de control local 42 recibe un mensaje desde el dispositivo de red de control local 61. Una conexión de transferencia de datos de una vía desde el dispositivo 61 de la red de control local a la clave de red de control local 42 ahora existe.

20 Después, la clave de red de control local 42 envía un paquete UDP a la dirección 240.1.1.2 con el puerto 10500 fuente hasta el puerto 10501 objetivo. El paquete UDP alcanza el firewall 51 FW1. El firewall 51 FW1 recuerda que la dirección 10.0.0.2 ha establecido la conexión UDP con la dirección 240.2.1.2 con el puerto 10501 fuente y el puerto 10500 objetivo. Debido a que el paquete llega desde la dirección 240.2.1.2 fuente con el puerto 10500 fuente y con el puerto 10501 objetivo, el firewall 51 FW2 interpreta el paquete UDP recibido como una comunicación de retorno para la conexión establecida por el dispositivo 10.0.0.2. El firewall 51 FW1 lleva a cabo un cambio de 25 dirección, es decir, cambia la dirección objetivo del paquete a 10.0.0.2. Después, el firewall 51 FW1 enruta el paquete a la dirección 10.0.0.2.

30 Ahora existe la conexión UDP de dos vías entre la clave de red de control local 42 y el dispositivo de red de control local 61. Estos dispositivos pueden comunicarse entre sí en forma bidireccional. El dispositivo de red de control local 61 y la clave de red de control local 42 ventajosamente forman un túnel VPN de nivel de capa de enlace de datos entre ellos, con el uso de por lo menos un software OpenVPN.

35 El dispositivo de red de control local 61 forma un puente en el túnel 55 VPN creado con la red 172.17.0.2/24 de control remoto local, referencia 6, que administra. En la misma forma, la clave de red de control local 42 empieza a formar un puente en el túnel 55 VPN creado con su puerto LAN, de modo que tiene la capacidad de proporcionar las interfaces de Intranet en la red 172.17.0.0/24 en el nivel de capa de enlace de datos. Después de estas operaciones, la red 4 de control remoto local y la Intranet 6 de control local forman una red VPN Privada sobre Internet 2.

40 Ahora, un dispositivo 41a cliente se puede conectar a través de la Ethernet con la interfaz de Internet de la clave de red de control local 42, la interfaz por ejemplo, puede ser una interfaz LAN. Después la conexión hecha con el dispositivo 41a cliente recupera sus ajustes IP desde el dispositivo de red de control local 61 con el uso del protocolo DHCP. El interrogatorio DHCP enviado por el dispositivo 41a o 41c cliente llega al puerto LAN de la clave de red de control local 42, cuyo puerto está en puente con el túnel 55 VPN. La clave de red de control local 42 envía el paquete Ethernet formado por el dispositivo 41a o 41c cliente, como tal al túnel 55 VPN. El paquete DHCP enviado 45 por el dispositivo 41a o 41c cliente alcanza el dispositivo de red de control local 61 a lo largo del túnel 55 VPN.

50 El dispositivo de red de control local 61 tiene un servidor DHCP, el cual responde en un mensaje de retorno con una dirección IP 172.17.0.7/24, el enrutador por especificación 172.17.0.1 y el servidor DNS 172.17.0.1. El mensaje de retorno del dispositivo de red de control local 61 en forma correspondiente se conduce a lo largo del túnel 55 VPN hasta la clave de red de control local 42, la cual envía el paquete hacia abajo a su interfaz de red LAN. A través de la interfaz de red LAN, el dispositivo 41a o 41c cliente recibe el paquete de retorno DHCP y toma los ajustes incluidos en el paquete de retorno IP. La dirección IP del dispositivo cliente es ahora 172.17.0.7/24, el enrutador por especificación es 172.17.0.1 y el servidor DNS es 172.17.0.1.

55 El dispositivo 41a cliente ahora es lógicamente una parte de la red 172.17.0.0/24 VPN y tiene la capacidad de comunicarse directamente a nivel Ethernet con el dispositivo 172.17.0.4 justo como si estuviera físicamente acoplado con la red 172.17.0.0/24 (Intranet 6 de control local). Las limitaciones técnicas del túnel 55 VPN y de las conexiones Internet, tal como la velocidad y retrasos de la conexión, se deben tomar en cuenta cuando se comunican.

60 Los dispositivos que van a ser controlados en forma remota están conectados con la interfaz LAN del dispositivo de red de control local 61, ya sea en forma permanente o inalámbrica. En los ejemplos de las figuras 1 y 2, los dispositivos a ser conectados son un control 65 de acondicionamiento de aire, un control 63 de control remoto, una cámara 64 de vigilancia, y un control 62 de iluminación. Los servidores de red de los dispositivos a ser controlados 65 en forma remota reciben su dirección IP desde el servidor DHCP compuesto, ventajosamente en el dispositivo de red de control local.

El dispositivo 61 de red de control local nombra las direcciones IP que ofrece en una manera predeterminada. En los ejemplos de las figuras 1 y 2, la dirección IP 172.17.0.4 es "HCND1", que es control de calor. En forma correspondiente, la dirección 172.17.0.3 es "HCND2" que es la cámara de vigilancia.

El usuario del dispositivo 41 cliente ahora puede comunicarse directamente en el nivel Ethernet con los dispositivos 62, 63, 64 y 65 a ser controlados en forma remota, presentados en la figura 1. La comunicación no difiere de la manera en que sería usada, cuando el dispositivo 41a cliente se acopla físicamente en forma directa con la red 172.17.0.0/24 de la Intranet de control local que da servicio a los dispositivos a ser controlados en forma remota.

Cuando se utiliza el sistema 1A de control remoto según la invención, el usuario del dispositivo 41a cliente introduce por ejemplo, `http://hcnd1q` como una dirección en el navegador. El navegador del dispositivo cliente hace un interrogatorio DNS al dispositivo de red de control local 61 (desde la dirección 172.17.0.1) para el nombre "HCND1". El dispositivo de red de control local 61 regresa al dispositivo 41a cliente el nombre con la dirección 172.17.0.4 IP de HCND1. El navegador del dispositivo 41a cliente del usuario ventajosamente abre la página HTTP `http://HCND1` desde el servidor de red de control de calor 172.17.0.4. El usuario tiene ahora la conexión de gestión directo con el servidor 63 de red de control de calor que controla los controles de calor.

El usuario del dispositivo 41a cliente también puede realizar una búsqueda de dirección para el nombre "HCND". El dispositivo de red de control local 61 responde al interrogatorio con su propia dirección IP 172.17.0.1 y proporciona una página de índices a ser vista por el navegador del dispositivo 41a cliente del usuario. En la página de índices, el usuario busca una lista de todos los recursos acoplados con la interfaz LAN del dispositivo de red de control local 61. En el ejemplo de las figuras 1y 2, la siguiente lista se observa en el navegador:

hcnd1	172.17.0.4
hcnd2	172.17.0.3
hcnd3	172.17.0.2
hcnd4	172.17.0.5

En la página de índices es posible que el usuario del dispositivo cliente renombre los objetos presentados por ejemplo, HCND1 con el nombre de "control de calor" y HCND2 con el nombre "cámara de vigilancia". El dispositivo de red de control local automáticamente almacena los cambios de nombre para las direcciones IP en cuestión. Ahora el usuario del dispositivo 41a cliente puede hacer contacto, por ejemplo, con el control de calor al introducir solamente "control de calor" en la línea del navegador.

En conexión con las figuras 1 y 2, se ha usado un ejemplo para mostrar la forma en que el dispositivo 41a, 41b, 41c cliente y el dispositivo 62-65 a ser controlados en forma remota en la propiedad se pueden hacer para intercambiar información y comandos de control en el sistema de control remoto, según la invención.

En la forma de realización según la figura 1, los pares de la clave de red de control local 42 y el dispositivo de red de control local 61 se determinan, ventajosamente, en conexión con la fabricación.

En la forma de realización según la figura 2, el emparejado de la clave de red de control local 42b y el dispositivo de red de control local 61 se puede determinar en conexión con la fabricación o con el objetivo de uso final. Cuando la determinación de los pares se lleva a cabo en el objetivo de uso final, entonces la clave de red de control local 42b en la forma de realización según la figura 2, está conectada temporalmente con el dispositivo de red de control local 61. La conexión, convenientemente, se implementa por medio de los puertos USB de los dispositivos o a través de una red de radio inalámbrica.

A través del acoplamiento de la clave de red de control local 42b y del dispositivo de red de control local 61 se puede recibir el código de identificación de su par de dispositivo y enviar su propio código de identificación a su par de dispositivo. Después, estos dos dispositivos pueden establecer una conexión de transferencia de datos solamente entre sí.

La transferencia del programa de ordenador de la clave de red de control local al terminal 41c del usuario se implementa como sigue.

Cuando la clave de red de control local 42b se acopla momentáneamente por su conexión con el dispositivo 41c de procesamiento de datos, entonces el programa de ordenador contenido en la clave de red de control local 42b con sus códigos de identificación individuales se instala en el dispositivo 41c de procesamiento de datos del usuario, referencia 42e. En conexión con la instalación del dispositivo 41c de procesamiento de datos, se le pide al usuario si desea tomar en uso una función de protección del dispositivo y/o programa. Cuando se desea activar la función de protección, entonces el programa de instalación de la clave de red de control local solicita al usuario que ofrezca su contraseña solamente al dispositivo 41c de procesamiento de datos del usuario o al programa instalado o ambos de ser deseado.

La clave de red de control local con sus programas, códigos de identificación individuales y contraseñas cuando sea deseado, también se almacenan por ejemplo, en un servidor de red interna protegido, desde donde se pueden mover de regreso a una nueva clave de red de control local (por ejemplo, cuando el dispositivo de clave original se pierde o se fractura).

5 En una forma de realización ventajosa de la invención, el programa de ordenador contenido en la clave de red de control local 42b por ejemplo, puede estar almacenado en varios dispositivos de procesamiento de datos 41c, que, por lo tanto, pueden funcionar en paralelo con el primer dispositivo de procesamiento de datos.

10 En una forma de realización ventajosa de la invención, el programa de ordenador contenido en la clave de red de control local 4b, por ejemplo, puede estar situada en un servidor en Internet, desde el cual puede ser recuperado. En esta forma de realización ventajosa, la clave de red de control local física 42b un servidor en Internet, desde donde puede ser recuperada. En esta forma de realización ventajosa, la propia clave de red de control local 42b física puede comprender únicamente el código de identificación necesario para identificar el par de dispositivo.

15 La figura 3 muestra como un diagrama de flujo las operaciones antes descritas después de que la clave de red de control local 42 o 42b y el dispositivo de red de control local 61 se han formado en pares.

20 En el paso 300, el dispositivo de red de control local 61 está conectado con la red 5 de Intranet local y con la clave de red de control local 42 o el dispositivo 41c de procesamiento de datos, que simula la clave de red de control local con la red 3 Intranet. Todos los dispositivos a ser controlados en forma remota en la propiedad están conectados con el dispositivo de red de control local 61 ya sea con una conexión permanente o con una conexión inalámbrica.

25 En el paso 301, tanto el dispositivo de red de control local 61 como la clave de red de control local 42 o 41c determinan su camino de red. En el paso 302, el dispositivo de red de control local 61 y la clave de red de control local 42 almacenan sus caminos de red determinados en el servidor de red de control local 21.

30 En el paso 303, los dispositivos 42, o 41c y 61 según la invención a ser utilizados en el control remoto reciben información de que su par de dispositivo se ha registrado con el servidor de red de control local 21 o que el registro está faltante. Cuando uno de los dispositivos 42/41c o 61 según la invención, que pertenece al par del dispositivo no se ha registrado, entonces el sistema 1A o 1B de control remoto se mueve después de un retraso 312 específico después del paso 313 de escucha de la conexión del servidor de red de control local.

35 Al inicio del establecimiento de la conexión, tanto la clave de red de control local 42/41c y el dispositivo de red de control local 61 solicitan, en el paso 304, el camino de red de la contraparte desde el servidor de red de control local 21. El servidor de red de control local 21 verifica que es una pregunta de un par de dispositivo permitido, y después de verificar, envía los caminos de red a ambos dispositivos en el paso 305. Después, el servidor de red de control local 21 libera la conexión para ambos dispositivos 42/41c y 61, y por tanto, ya no es parte del túnel 55 VPN a ser formado.

40 En el paso 306, la clave de red de control local 42/41c y el dispositivo de red de control local 61 forman un túnel 55 VPN entre ellos.

45 En el paso 307, tanto el dispositivo 41a o 41c cliente del usuario y el dispositivo 62-65 objetivo en la propiedad están conectados con la red VPN establecida. En la forma de realización de la figura 1, el dispositivo 41a cliente del usuario está conectado con la red VPN por la clave de red de control local 42. En la forma de realización de la figura 2, el dispositivo 41c de procesamiento de datos del usuario en sí es uno de los puntos finales de la red VPN. El dispositivo 62-65 a ser controlado en forma remota en el objetivo se conecta con la red VPN por el dispositivo de red de control local 61.

50 En el paso 308, el dispositivo 41a o 41c cliente del usuario y los dispositivos 62-65 ser controlado en la propiedad son parte de la misma red VPN, por lo cual pueden intercambiar información entre sí. Después del retraso especificado en el sistema de control remoto, el paso 309 consiste de verificar si la conexión de transferencia de datos entre el dispositivo 41a y 41c cliente y los dispositivos 62-65 objetivo sigue activa. Cuando la conexión de transferencia de datos sigue activa, el proceso regresa al paso 308 y se permite que la transferencia de datos continúe.

55 Cuando en el paso 309 se encuentra que la conexión VPN ya no está activa, entonces se toma la decisión en el paso 310 con respecto a un posible nuevo intento para establecer una conexión. Cuando se decide hacer un nuevo intento para establecer una conexión, entonces el proceso regresa al paso 301. En esta alternativa, el proceso ventajosamente, también incluye los procesos necesarios para liberar la conexión VPN, para que el proceso para establecer la conexión, según la invención se puede retomar con éxito. El establecimiento de la conexión se intenta según un número predeterminado.

65 Cuando en el paso 310 se decide que no se realizará un nuevo intento para establecer la conexión VPN, debido a que se ha definido el número predeterminado de intentos para establecer la conexión o por alguna otra razón,

entonces el proceso avanza al paso 311. En el paso 311, la red VPN de transferencia de datos se libera.

Después de que la red VPN de transferencia de datos se libera, un retraso 312 predeterminado avanza en el proceso utilizado en el sistema 1A o 1B de control remoto. Después del retraso 312, el proceso lanza a la función 313 de escucha del servidor de red de control local. Ahí, el dispositivo de red de control local 61 que lleva corriente envía las solicitudes de contacto a través de la red al servidor de red de control local 21.

El dispositivo de red de control local 61 repite el proceso, el paso 314, hasta que se establece una conexión de red con el servidor de red de control local 21.

Cuando se establece la conexión de transferencia de datos para el servidor de red de control local 21, entonces, en el paso 314, se toma una decisión para moverse a un proceso para establecer una conexión VPN, por lo cual el proceso regresa al paso 301.

Todos los pasos del proceso antes descrito se implementan con comandos de programa, que se llevan a cabo en un procesador de propósitos especiales o de propósitos generales apropiado. Los comandos del programa se almacenan en un medio de almacenamiento utilizado por el dispositivo de red de control local 61 y la clave de red de control local 42, tales como memorias, desde las cuales el procesador puede recuperarlos e implementarlos. Las referencias a un medio legible por ordenador por ejemplo, también pueden contener componentes especiales, tales como memorias Flash USB programables, arreglos lógicos (FPLA), circuitos integrados de aplicación específica (ASIC) y procesadores de señal (DSP).

La figura 4 muestra las partes principales funcionales del dispositivo de red de control local 61 según la invención. El dispositivo de red de control local 61 tiene una fuente 621 de energía, la cual puede ser un acumulador o una fuente de alimentación con base en la corriente. Todos los componentes eléctricos del dispositivo de red de control local obtienen su voltaje operativo desde la fuente 621 de energía.

El dispositivo de red de control local 61 tiene uno o más procesadores 622. Los medios de procesador o el procesador pueden comprender una unidad de lógica aritmética, un grupo de diferentes registro y circuitos de control. Un arreglo 623 de almacenamiento de datos, tal como una unidad de memoria o un medio de memoria, sobre el cual se puede almacenar información legible por ordenador o programas o información del usuario, ha sido conectado con el medio procesador. El medio 623 de memoria típicamente contiene unidades de memoria, que permiten las funciones de lectura y escritura (Memoria de Acceso Aleatorio-RAM) y unidades de memoria que contienen una memoria no volátil, desde la cual solamente se pueden leer datos (Memoria de Solamente Lectura, ROM). La información de identificación de dispositivo, su camino de red actual, la información de identificación de la clave de red de control local 42 que funciona como su par y todos los programas necesarios para la operación del dispositivo de red de control local 61 están almacenados, convenientemente en los medios de memoria.

Algunos ejemplos de los programas almacenados en la memoria del dispositivo de red de control local 61 son un sistema operativo (por ejemplo, Linux), programas TCP/IP, programas VPN (por ejemplo, OpenVPN), programa de dispositivo/servidor del control remoto DHCP (es decir, ISC DHCP), un programa de servidor DNS (por ejemplo, drismasq), un programa de base de datos (es decir, SQLite), un programa de control remoto (por ejemplo, OpenSSH), un programa de confirmación/gestión de certificado (por ejemplo, GPG), y una biblioteca de interfaz del usuario (por ejemplo, LuCI).

El dispositivo de red de control local 61 también comprende unos elementos de interfaz, que comprenden medios 624, 625, 626, y 627 de entrada/salida para recibir o enviar información. La información recibida con los medios de entrada se transfiere para ser procesada por el medio 622 procesador del dispositivo de red de control local 61. Los elementos de interfaz de la información de transferencia del dispositivo de red de control local ya sea a la red de transferencia de datos o a los dispositivos de procesamiento de datos externos. Los elementos de interfaz del dispositivo de red de control local 61 ventajosamente son un puerto 624 WAN, uno o más puertos 625 LAN, un puerto 626 de antena y un puerto 627 USB. Los pares del dispositivo de red de control local 61 y de la clave de red de control local 42 o 41c ventajosamente se pueden formar por ejemplo, a través del puerto 627 USB.

Resultará evidente para los expertos en la materia que las funciones del dispositivo de red de control local 61 se pueden integrar como parte de un dispositivo de ingeniería o de cómputo, que tiene suficiente capacidad de procesador y de memoria y medios de conexión para conectar los medios técnicos con el mismo ya sea con una conexión de transferencia de datos cableada o con una conexión de transferencia de datos inalámbrica. Este dispositivo computarizado, en donde las funciones del dispositivo de red de control local 61 están integradas, está conectado con cierta red 5 de transferencia de datos, desde donde se tiene acceso a Internet pública.

La figura 5a muestra las partes principales funcionales de la clave de red de control local 42 según la invención. El dispositivo de red de control local 42 tiene una fuente 421 de energía. Puede ser un acumulador, o una fuente de alimentación con base en la corriente. Todos los componentes eléctricos del dispositivo de red de control local obtienen su voltaje operativo de la fuente 421 de energía.

La clave de red de control local 421 puede comprender uno o más procesadores 422. El procesador o medio procesador puede comprender una unidad de lógica aritmética, un grupo de diferentes registros y circuitos de control. Un arreglo 423 de almacenamiento de datos, tal como una unidad de memoria o un medio de memoria, sobre el cual se puede almacenar información legible por ordenador o programas o información del usuario, ha sido conectado con el medio procesador. El medio 423 de memoria típicamente contiene unidades de memoria, que permiten las funciones de lectura y escritura (Memoria de Acceso Aleatorio-RAM) y unidades de memoria que contienen una memoria no volátil, desde la cual solamente se pueden leer datos (Memoria de Solamente Lectura, ROM). La información de identificación de dispositivo, su camino de red actual, la información de identificación de los dispositivos de red de control local así como sus dispositivos pares y todos los programas necesarios para la operación de la clave de red de control local 42 están almacenados, convenientemente en los medios de memoria.

Algunos ejemplos de los programas almacenados en la memoria de la clave de red de control local 42 son un sistema operativo (por ejemplo, Linux), programas TCP/IP, programas VPN (por ejemplo, OpenVPN), programa de dispositivo/servidor del control remoto DHCP (es decir, ISC DHCP), un programa de servidor DNS (por ejemplo, drimasq), un programa de base de datos (es decir, SQLite), un programa de control remoto (por ejemplo, OpenSSH), un programa de confirmación/gestión de certificado (por ejemplo, GPG), y una biblioteca de interfaz del usuario (por ejemplo, LuCI).

La clave de red de control local 42 también comprende elementos de interfaz, que comprenden medios 424, 425 y 426 de entrada/salida para recibir o enviar información. La información recibida con los medios de entrada se transfiere para ser procesada por el medio 422 procesador de la clave de red de control local 42. Los elementos de interfaz de la información de transferencia del dispositivo de red de control local ya sea a la red de transferencia de datos o a los dispositivos de procesamiento de datos externos. Los elementos de interfaz del dispositivo de red de control local 42 ventajosamente son un puerto 424 WAN, un puerto 425 LAN, un puerto 426 USB y puerto 427 de antena.

La figura 5b muestra las partes principales funcionales de una clave de red de control local 42b según una segunda forma de realización de la invención. La clave de red de control local 41c puede comprender uno o más procesadores 422. El procesador o medio procesador puede comprender una unidad de lógica aritmética, un grupo de diferentes registros y circuitos de control. Un arreglo 423 de almacenamiento de datos, tal como una unidad de memoria o un medio de memoria, sobre el cual se puede almacenar información legible por ordenador o programas o información del usuario, ha sido conectado con el medio procesador. El medio 423 de memoria típicamente contiene unidades de memoria, que permiten las funciones de lectura y escritura (Memoria de Acceso Aleatorio-RAM) y unidades de memoria que contienen una memoria no volátil, desde la cual solamente se pueden leer datos (Memoria de Solamente Lectura, ROM). La información de identificación de la clave de red de control local 42b, su camino de red actual, la información de identificación de dispositivo de red de control local 61 funcionan como sus dispositivos pares y todos los programas necesarios para la operación de la clave de red de control local 41c están almacenados, convenientemente en los medios de memoria.

Algunos ejemplos de programas almacenados en la memoria de la clave de red de control local 42b son un sistema operativo (por ejemplo, Linux), programas TCP/IP, programas VPN (por ejemplo, OpenVPN), programa de dispositivo/servidor del control remoto DHCP (es decir, ISC DHCP), un programa de servidor DNS (por ejemplo, drimasq), un programa de base de datos (es decir, SQLite), un programa de control remoto (por ejemplo, OpenSSH), un programa de confirmación/gestión de certificado (por ejemplo, GPG), y una biblioteca de interfaz del usuario (por ejemplo, LuCI).

La clave de red de control local 42b también comprende elementos de interfaz, que comprenden medios 426 de entrada/salida para recibir o enviar información. La información recibida con los medios de entrada se transfiere para ser procesada por el medio 422 procesador de la clave de red de control local 42b. Los elementos de interfaz de la información de transferencia del dispositivo de red de control local se usan ventajosamente para transferir información desde la memoria 423 a la clave de red de control local ya sea a un dispositivo 41c de procesamiento de datos externo o al dispositivo de red de control local 61. La información o comandos correspondientes se pueden recibir a través de los elementos de interfaz, por ejemplo, desde el dispositivo de procesamiento de datos, con el cual está conectada la clave de red de control local 42b.

Con respecto a los niveles de derecho de acceso, existen por lo menos dos niveles de las clave de red de control local 42 o 42b antes descritas, por ejemplo, los dispositivos clave de nivel de usuario básico y administrador. Un usuario/propietario de un dispositivo clave de nivel de derecho de acceso más alto (por ejemplo, un administrador) tiene el derecho de control para todos los objetivos de control de los usuarios de la clave de red de control local en un nivel más bajo (tal como usuarios básicos). El propietario de un nivel de derecho de acceso al dispositivo clave de un nivel más bajo por otra parte, no tiene acceso a ningún otro objetivo de control de nivel de derecho de acceso más alto que sus propios objetivos.

La figura 6 muestra las partes principales funcionales del servidor de red de control local 21. El servidor de red de control local 21 comprende una fuente 211 de energía. Puede ser un acumulador o una fuente de alimentación con base en la corriente. Todos los componentes eléctricos del servidor de red de control local 21 obtienen su voltaje



operativo desde la fuente 211 de energía.

5 El servidor de red de control local 21 puede comprender uno o más procesadores 212. El procesador o medio procesador puede comprender una unidad de lógica aritmética, un grupo de diferentes registro y circuitos de control. Un arreglo 213 de almacenamiento de datos, tal como una unidad de memoria o un medio de memoria, sobre el cual se puede almacenar información legible por ordenador o programas o información del usuario, ha sido conectado con el medio procesador. El medio 213 de memoria típicamente contiene unidades de memoria, que permiten las funciones de lectura y escritura (Memoria de Acceso Aleatorio-RAM) y unidades de memoria que contienen una memoria no volátil, desde la cual solamente se pueden leer datos (Memoria de Solamente Lectura, ROM).

10 La información de identificación de los pares de dispositivos en el sistema de control remoto, los caminos de red actuales de cada par de dispositivos y todos los programas necesarios para establecer la conexión de transferencia de datos VPN a ser establecida entre los pares de dispositivos están almacenados, convenientemente en los medios de memoria.

15 Algunos ejemplos de los programas almacenados en la memoria del servidor de red de control local 21 son un sistema operativo (por ejemplo, Linux), programas TCP/IP, programas VPN (por ejemplo, OpenVPN), programa de dispositivo/servidor del control remoto DHCP (es decir, ISC DHCP), un programa de servidor DNS (por ejemplo, drismasq), un programa de base de datos (es decir, SQLife), un programa de control remoto (por ejemplo, OpenSSH), un programa de confirmación/gestión de certificado (por ejemplo, GPG), y una biblioteca de interfaz del usuario (por ejemplo, LuCI).

20

25 El servidor de red de control local 21 también comprende elementos de interfaz, que comprenden medios 214 y 215 de entrada/salida para recibir o enviar información. La información recibida con los medios de entrada se transfiere para ser procesada por el medio procesador 212 del servidor de red de control local 21. Los elementos de interfaz del servidor de red de control local 21 transfieren información a la red de transferencia de datos o a los dispositivos de procesamiento de datos externo. Los elementos de interfaz del servidor de red de control local 21 ventajosamente son un puerto 214 WAN y uno o más puertos 215 LAN.

30 El servidor de red de control local 21 ventajosamente también comprende una interfaz del usuario (no mostrada en la figura 6), que comprende medios para recibir la información desde el usuario del servidor 21. La interfaz del usuario puede comprender un teclado, una pantalla de tacto, un micrófono y una bocina.

35 Algunas formas de realización ventajosas del método de control remoto y del sistema de control remoto según la invención han sido descritas. La invención no está limitada a las soluciones antes descritas, más bien, la idea novedosa puede aplicarse en muchas formas dentro del alcance de las reivindicaciones.

**REIVINDICACIONES**

1. Clave de red de control local (42, 42b) para accionadores en una propiedad, que comprende:

- 5       - unos elementos de interfaz de red, que comprenden unos medios de entrada/salida (424, 425, 426, 427) para unas interfaces de red (3, 4);
- un procesador (422); y
- 10       - una memoria (423), que contiene un código de programa de ordenador;
- el procesador, la memoria y un código de programa de ordenador almacenado en la misma están configurados para:
  - 15           - determinar un camino de red desde la clave de red de control local (42, 42b) hasta Internet (2);
  - almacenar el camino de red determinado tanto en la memoria (423) de la clave de red de control local como en una memoria (213) de un servidor de red de control local (21);
- 20       caracterizado por que, para establecer una red privada virtual (55), el procesador, la memoria y el código de programa de ordenador almacenado en la misma están configurados además para:
  - 25           - recibir un código de identificación de dispositivo enviado por su propio par de terminales de red, que es un dispositivo de red de control local (61), con el cual se permite que la clave de control de red local establezca una conexión de transferencia de datos, en la que se permite dicha conexión de transferencia de datos solo entre ellos, y enviar su propio código de identificación de dispositivo a su único par de terminales de red, cuando la clave de red de control local (42, 42b) y el dispositivo de red de control local (61) están conectados juntos con sus puertos USB (426, 627) y a continuación, la clave de red de control (42, 42b) está adaptada para:
    - 30               - solicitar desde el servidor de red de control local (21) la información de camino de red de su único par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo a extremo con su único par de terminales de red;
    - 35               - recibir desde el servidor de red de control local (21), la información de camino de red de su único par de terminales de red; y
    - 40               - establecer con la ayuda de la información de camino de red recibida con su único par de terminales de red, la red (55) privada virtual para el control remoto de accionadores de una propiedad, a cuya red privada virtual no pertenece el servidor de red de control local (21).

2. Clave de red de control local según la reivindicación 1, caracterizada por que está configurada para instalar un programa de ordenador que implementa las funciones de clave de red de control local desde su memoria (423) hasta un dispositivo (41c) de procesamiento de datos conectado con Internet, estando el dispositivo (41c) de procesamiento de datos configurado para simular las funciones de clave de red de control local (42b) con el programa de ordenador instalado.

3. Clave de red de control local según la reivindicación 2, caracterizada por que está configurada para instalar también una contraseña utilizada para arrancar la simulación de clave de red de control local dentro de dicho dispositivo (41c) de procesamiento de datos.

4. Dispositivo de red de control local (61) para accionadores en una propiedad, que comprende:

- 55       - unos elementos de interfaz de red, que comprenden unos medios de entrada/salida (624, 625, 626, 627) tanto para una interfaz (5) de red como para unos dispositivos (62-65) que deben ser controlados de forma remota;
- por lo menos un procesador (622), y
- 60       - una memoria (623), que contiene un código de programa de ordenador;
- el procesador, la memoria y un código de programa de ordenador almacenado en la misma están configurados para:

65

- determinar un camino de red desde el dispositivo de red de control local (61) hasta Internet (2),
- almacenar el camino de red determinado tanto en la memoria (623) del dispositivo de red de control local como en una memoria (213) de un servidor de red de control local (21),

5 caracterizado por que, para establecer una red privada virtual (55), el procesador, la memoria y el código de programa de ordenador almacenado en la misma están configurados además para:

- 10 - recibir un código de identificación de dispositivo enviado por su único par de terminales de red, que es una clave de red de control local (42, 42b), con la cual se permite que el dispositivo de control de red local establezca una conexión de transferencia de datos, en la que se permite dicha conexión de transferencia de datos únicamente entre ellos, y enviar su propio código de identificación de dispositivo a su único par de terminales de red, cuando el dispositivo de red de control local (61) y la clave de red de control local (42, 42b) están conectados juntos con sus puertos USB (426, 627), y a continuación, el dispositivo de red de control local (61) está adaptado para:
  - 15 - solicitar desde el servidor de red de control local (21) la información de camino de red de su único par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo-a-extremo con su único par de terminales;
  - 20 - recibir desde el servidor de red de control local (21), la información de camino de red de su único par de terminales de red; y
  - 25 - establecer con la ayuda de la información de camino de red recibida con su único par de terminales de red, la red privada virtual (55) para el control remoto de los accionadores de una propiedad, a cuya red privada virtual no pertenece el servidor de red de control local (21).

30 5. Dispositivo de red de control local según la reivindicación 4, caracterizado por que está configurado para formar dicha red privada virtual (55) en la capa de enlace de datos de modelo OSI (Capa 2) o en la capa de red (Capa 3).

35 6. Producto de programa de ordenador que comprende unos medios de código de programa de ordenador adaptados para realizar las siguientes etapas de código de programa cuando dicho programa se ejecuta en un ordenador para proporcionar las funciones de clave de red de control local, caracterizado por que el programa de ordenador comprende:

- unos medios de código para determinar un camino de red desde la clave de red de control local (42, 42b) hasta Internet (2);
- 40 - unos medios de código para almacenar el camino de red determinado tanto en una memoria (423) de la clave de red de control local como en en una memoria (213) de un servidor de red de control local (21),

45 caracterizado por que, para ser adaptado para establecer una red privada virtual (55), el programa de ordenador además comprende:

- 50 - unos medios de código para recibir un código de identificación de dispositivo enviado por un único par de terminales de red, que es un dispositivo de red de control local (61), con el cual se permite que la clave de red de control local (42, 42b) establezca una conexión de transferencia de datos, en la que se permite dicha conexión de transferencia de datos únicamente entre ellos, y para enviar su propio código de identificación de dispositivo al único par de terminales de red, cuando una clave de red de control local (42, 42b) y un dispositivo de red de control local (61) están conectadas juntos con sus puertos USB (426, 627);
- 55 - unos medios de código para solicitar desde el servidor de red de control local (21) la información de camino de red del único par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo-a-extremo con el único par de terminales de red;
- unos medios de código para recibir la información de camino de red del único par de terminales de red desde el servidor de red de control local (21); y
- 60 - unos medios de código para establecer la red (55) privada virtual por medio de la información de camino de red recibida con el único par de terminales de red para el control remoto de los accionadores en la propiedad, a cuya red (55) privada virtual no pertenece el servidor de red de control local (21).

65 7. Producto de programa de ordenador según la reivindicación 6, caracterizado por que además comprende unos medios de código, que están configurados para instalar un programa de ordenador que implementa las funciones de clave de red de control local de la memoria (423) de la clave de red de control local (42b) a un dispositivo (41c) de

procesamiento de datos conectado con Internet, para que las funciones de la clave de red de control local (42b) puedan ser simuladas con el dispositivo (41c) de procesamiento de datos.

5 8. Producto de programa de ordenador según la reivindicación 7, caracterizado por que además comprende unos medios de código, que están configurados para instalar una contraseña utilizada para arrancar la simulación de la clave de red de control local (42b) dentro del dispositivo (41c) de procesamiento de datos.

10 9. Producto de programa de ordenador que comprende unos medios de código de programa de ordenador adaptados para realizar las siguientes etapas de código de programa cuando dicho programa se ejecuta en un ordenador para proporcionar las funciones del dispositivo de red de control local que comprende:

- unos medios de código para determinar un camino de red desde el dispositivo de red de control local (61) hasta Internet (2);

15 - unos medios de código para almacenar el camino de red determinado tanto en una memoria (623) del dispositivo de red de control local como en una memoria (213) de un servidor de red de control local (21),

caracterizado por que, para ser adaptado para establecer una red (55) privada virtual, el programa de ordenador además comprende:

20 - unos medios de código para recibir un código de identificación de dispositivo enviado por su único par de terminales de red, que es un dispositivo de red de control local (42, 42b), con el cual se permite que el dispositivo de red de control local (61) establezca una conexión de transferencia de datos, en la que se permite dicha conexión de transferencia de datos únicamente entre ellos, y para enviar su propio código de  
25 identificación de dispositivo a su único par de terminales de red, cuando el dispositivo de red de control local (61) y la clave de red de control local (42, 42b) están conectados juntos con sus puertos USB (426, 627);

30 - unos medios de código para solicitar desde el servidor de red de control local (21) la información de camino de red de su único par de terminales de red con el fin de establecer una conexión de transferencia de datos extremo-a-extremo con su único par de terminales de red;

- unos medios de código para recibir la información de camino de red de su único par de terminales de red desde el servidor de red de control local (21); y

35 - unos medios de código para establecer la red (55) privada virtual por medio de la información de camino de red recibida con su único par de terminales de red para el control remoto de los accionadores en la propiedad, a cuya red (55) privada virtual no pertenece el servidor de red de control local (21).

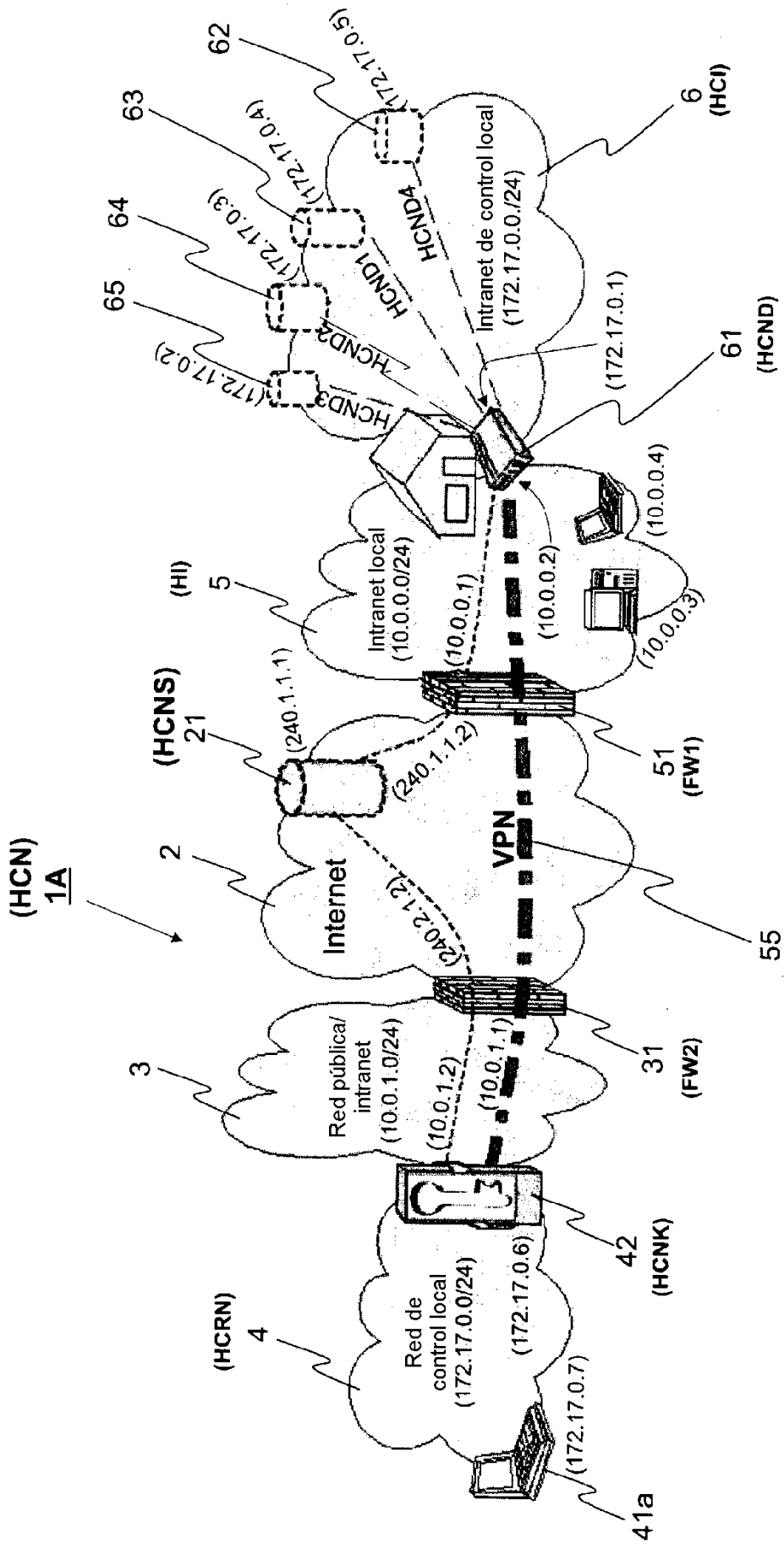


Fig. 1

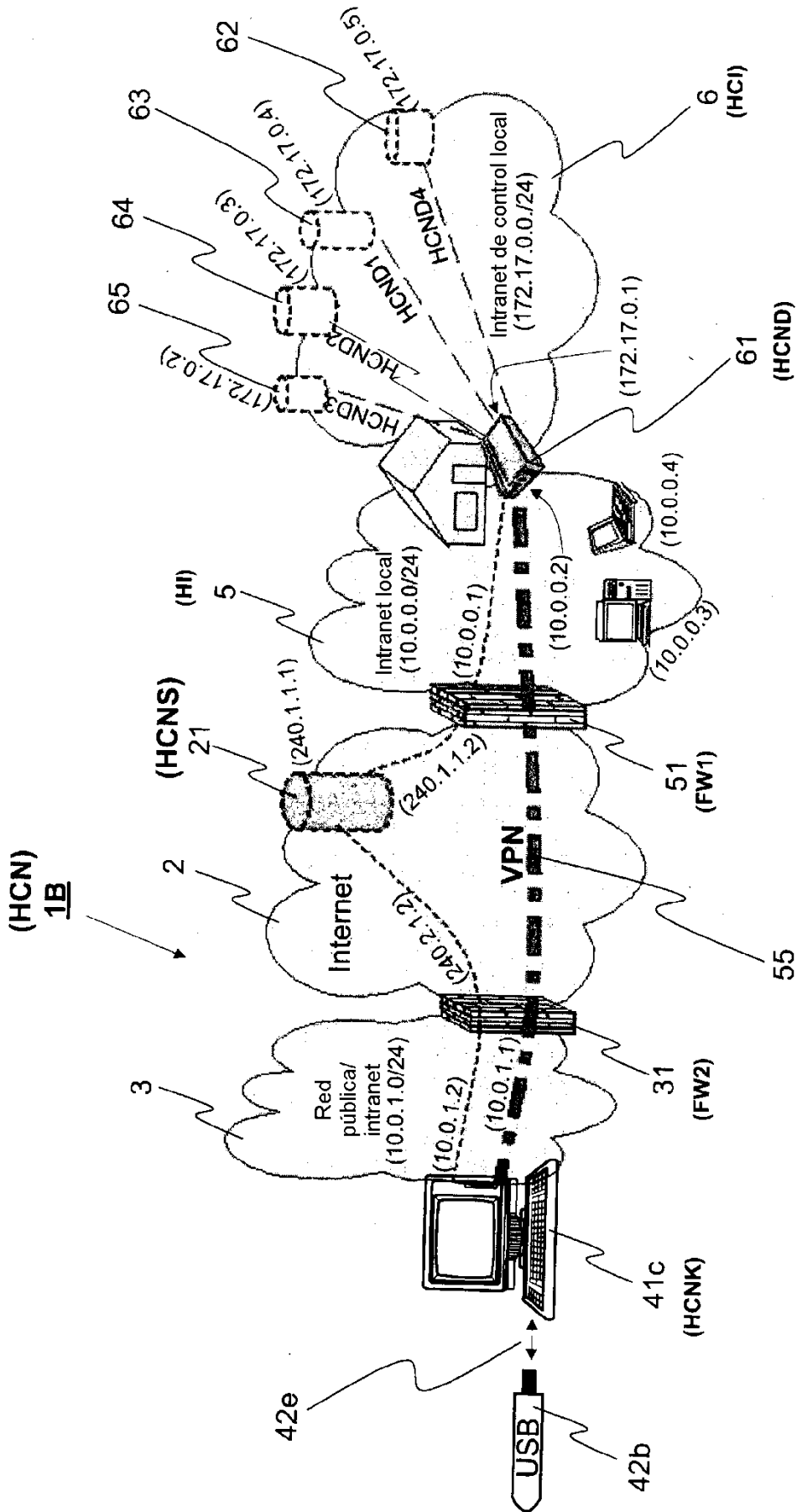


Fig. 2

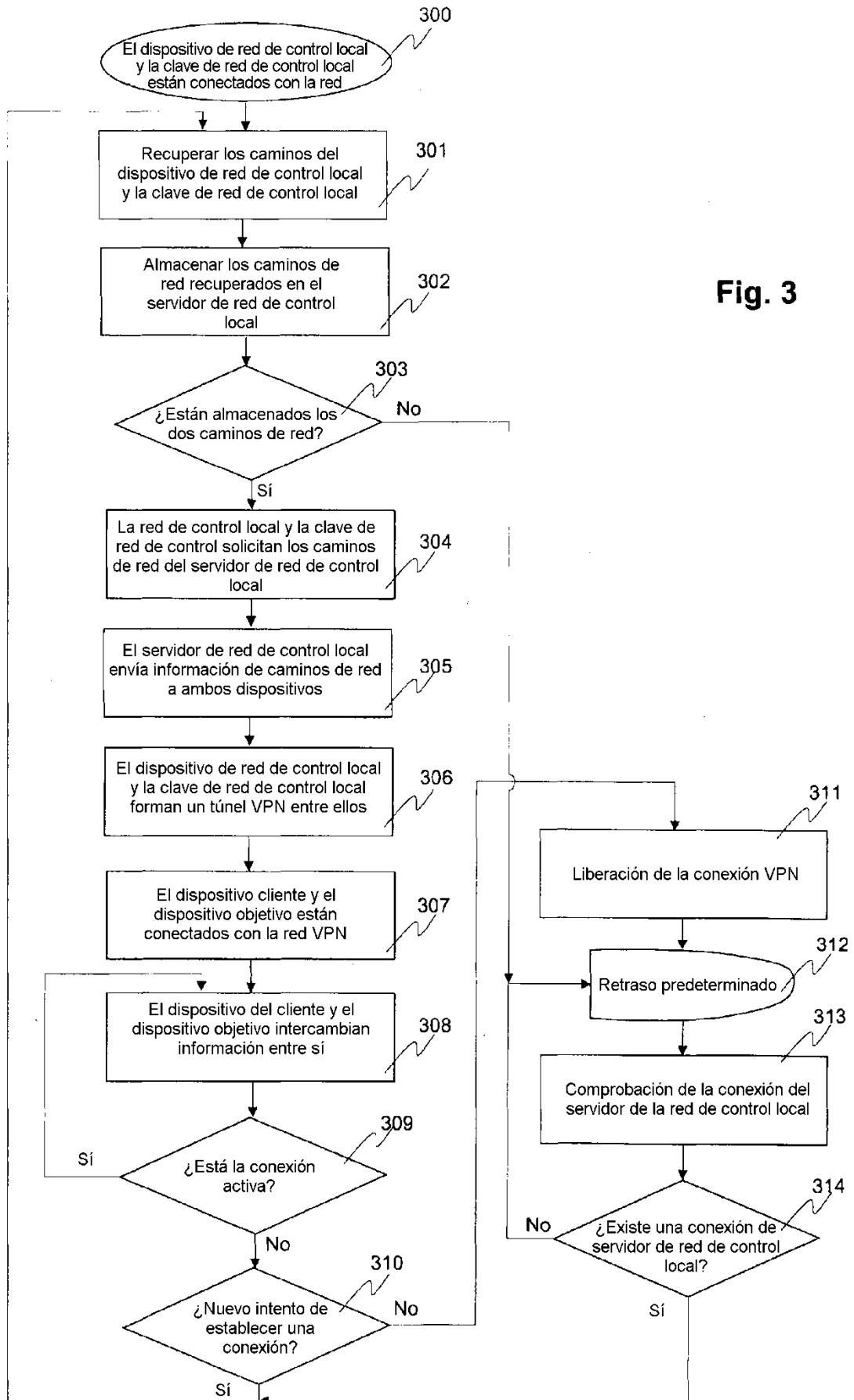


Fig. 3

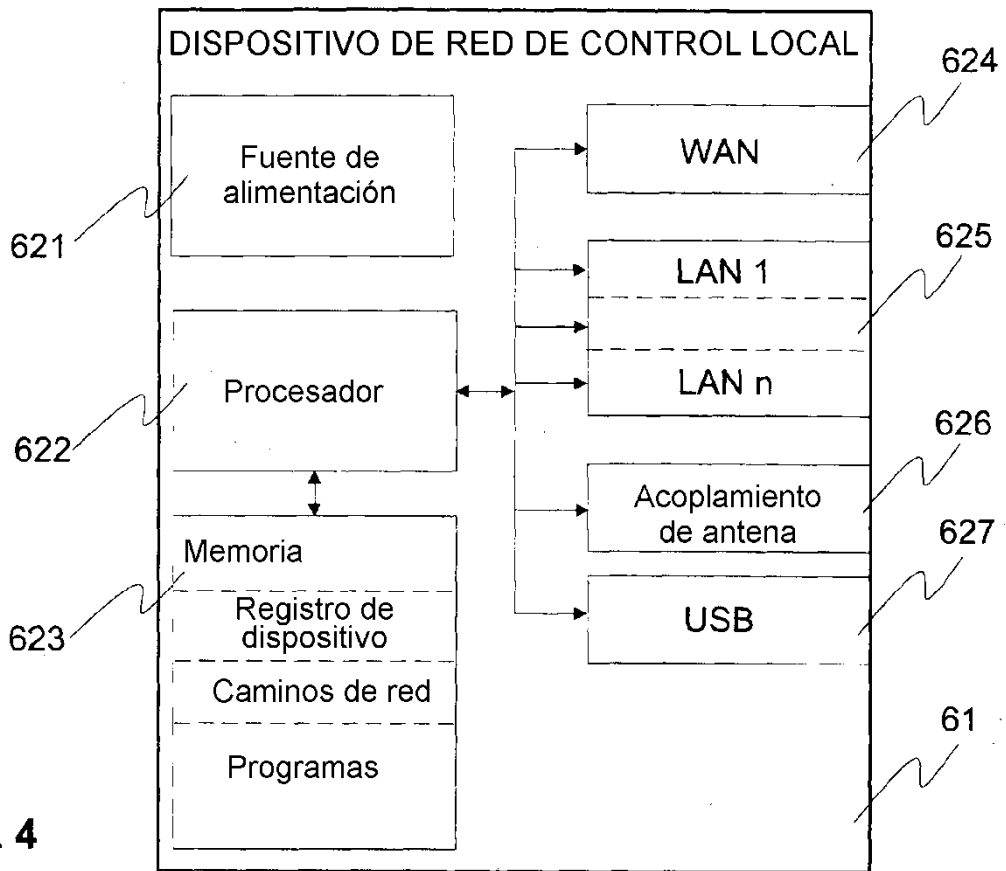


Fig. 4

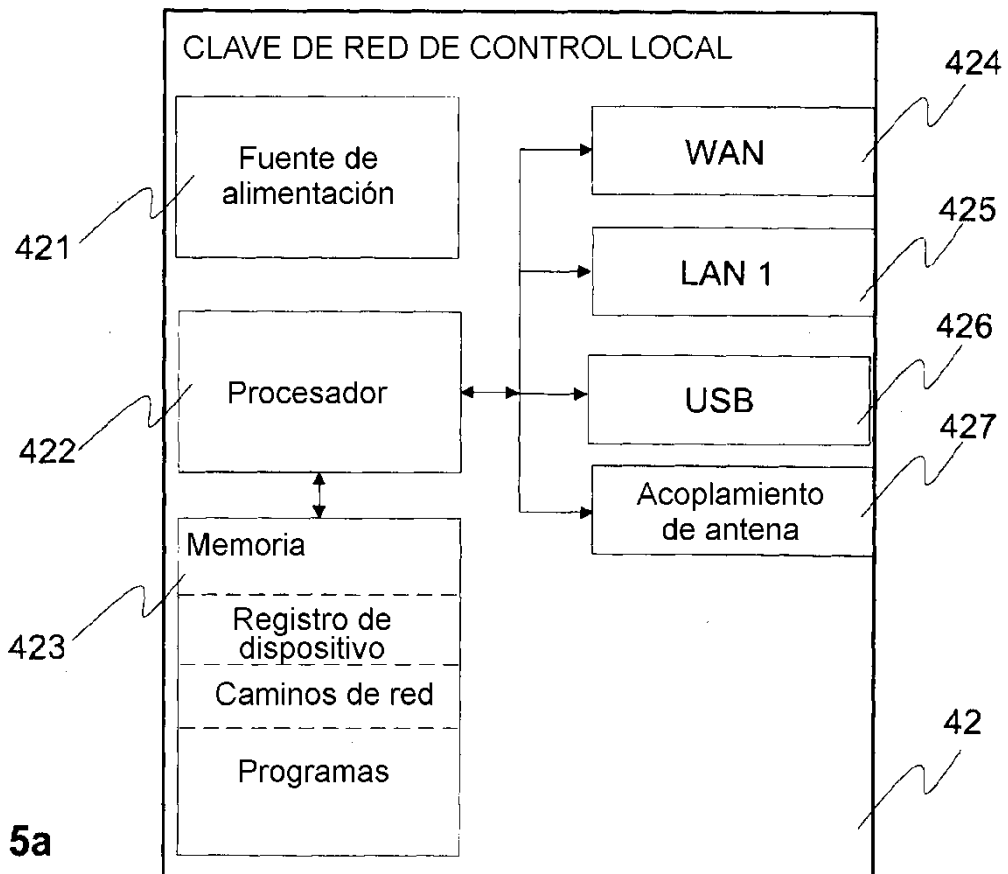


Fig. 5a



