(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 618 953**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.01.2013 PCT/FI2013/050011**

(87) Fecha y número de publicación internacional: **18.07.2013 WO2013104823**

(96) Fecha de presentación y número de la solicitud europea: **07.01.2013 E 13735938 (6)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2016 EP 2803177**

(54) Título: **Disposición de dispositivo y método para implementar una red de transferencia de datos utilizada en el control remoto de propiedades**

(30) Prioridad:

09.01.2012 FI 20125022

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.06.2017

(73) Titular/es:

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

(72) Inventor/es:

YLIMARTIMO, VEIKKO

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Disposición de dispositivo y método para implementar una red de transferencia de datos utilizada en el control remoto de propiedades.

La presente invención se refiere a un método para proporcionar una red de transferencia de datos requerida por los accionadores controlables remotamente en una propiedad.

Se están instalando cada vez más dispositivos y sistemas controlables remotamente en propiedades y viviendas. El propósito de los sistemas es garantizar y/o mantener unas condiciones en las propiedades, tales que vivir en ellas resulte seguro y agradable. El espectro de dispositivos controlados o monitorizados remotamente es amplio. La misma propiedad puede tener dispositivos de varios proveedores. Normalmente, estos dispositivos no se pueden comunicar de forma directa entre sí. Es también común que cada sistema tenga su módulo lógico de funcionamiento, cuyo control remoto requiere el uso de una solución particular de comunicaciones de datos.

Los proveedores de servicios del sector de la construcción han comenzado últimamente a poner solución al problema de forma muy general, pidiendo a un operador del cliente destinatario su propia conexión adicional, con un coste aparte, la cual contiene ciertas características acordadas específicas del destino, y cuyo mantenimiento debe llevarse a cabo por separado, por medio o bien de una red telefónica o bien de una red de banda ancha, pudiendo ser dicha red de banda ancha una conexión permanente de banda ancha de red 2G/3G inalámbrica. La mayoría de proveedores ha observado que, por el momento, este es el modo de funcionamiento más sencillo para ellos, aun cuando el mismo presenta varios aspectos problemáticos.

Si se proporciona una nueva conexión adicional para el destino, normalmente se debe llegar a un acuerdo sobre cuestiones de la comunicación de datos, con un administrador de la intranet local por separado. Probablemente, el administrador de la intranet debe llevar a cabo configuraciones de red adicionales para la conexión, de manera que el establecimiento de una conexión remota pueda resultar satisfactorio.

También se puede intentar solucionar el uso remoto del destino con una solución específica de cada aplicación. Así, el proveedor del dispositivo puede adquirir del operador su propia red de radiocomunicaciones, y constituir en ella un nombre de punto de acceso (APN) privado, que determina valores de configuración de las comunicaciones de datos en redes GPRS (Servicio General de Radiocomunicaciones por Paquetes) y HSDPA (Acceso por Paquetes de Enlace Descendente y Alta Velocidad) /HSUPA (Acceso por Paquetes de Enlace Ascendente y Alta Velocidad). Usando valores de configuración del APN, se proporciona una conexión de Internet por medio de una red 2G/3G/4G inalámbrica con los dispositivos en el destino. En tales casos, el usuario debe pagar por separado la conexión y los módems y programas de interfaz que habilitan su uso remoto. Normalmente, una conexión adicional de este tipo no puede usarse o puede que no se use para más de una finalidad práctica, por ejemplo, para el uso remoto de dispositivos suministrados por el proveedor de servicios del sector de la construcción. Adicionalmente, en la actualidad los operadores limitan generalmente la cantidad máxima de transferencia de datos en dichas conexiones, la cual, cuando se supera, puede generar facturas adicionales elevadas para el propietario de la conexión.

En destinos de tipo cooperativas de viviendas, que disponen de varias propiedades, las propiedades se pueden conectar al "uso remoto" que se produce solamente dentro de la intranet formada entre las propiedades. Para destinos de este tipo no se obtiene un contacto remoto "real" si el usuario del contacto remoto se encuentra físicamente en un lugar que no sea una de las propiedades en cuestión de la intranet.

Una publicación de Bryan Ford y Pyda Srisuresh “Peer-to-Peer communication Across Network Address translators”, USENIX, (14-3-2015), páginas 1 a 14, XP061012919, incluye ejemplos sobre cómo un dispositivo terminal arbitrario puede establecer una conexión de datos a través de traductores de direcciones de red (NAT) utilizando el *hole punching*.

Una propuesta de especificación de B. Ford, P. Srisuresh y D. Kegel “Peer-to-Peer (P2P) communication Across Network Address translators (NATs), rfc5128.txt”, 20080301 (1-3-2008), XP015055197, incluye en la práctica el mismo tipo de ejemplos que la publicación de Bryan Ford y Pyda Srisuresh “Peer-to-Peer communication Across Network Address translators”.

El documento WO 2012/160257 da a conocer un método de control remoto y un sistema de control remoto. De acuerdo con la invención, se crea una red privada virtual entre un primer terminal de red y un segundo terminal de red. Para crear la red privada virtual, tanto el primer terminal de red como el segundo terminal de red determinan sus rutas de red hacia Internet desde la red de transferencia de datos a la cual se conectan. Las rutas de red determinadas se almacenan en un servidor de control en Internet. Cuando se desea formar una red privada virtual, el servidor de control suministra las rutas de red almacenadas al primer terminal de red y al segundo terminal de red.

El documento WO 2012/113975 da a conocer un método de control remoto y un sistema de control remoto, donde se establece una red privada virtual entre un primer terminal de red y un segundo terminal de red. Para crear la red privada virtual, tanto el primer terminal de red como el segundo terminal de red determinan sus rutas de red hacia

Internet desde la red de transferencia de datos a la cual se conectan. Las rutas de red determinadas se almacenan en un servidor de control en Internet. Cuando se desea formar una red privada virtual, el servidor de control suministra las rutas de red almacenadas al primer terminal de red y al segundo terminal de red. Utilizando las rutas de red recibidas, el primer terminal de red y el segundo terminal de red establecen entre ellos una red privada virtual, a la cual también se conectan un dispositivo de cliente usado por la persona que lleva a cabo el control remoto y los accionadores que se van a controlar de forma remota, con el fin de implementar el control remoto.

Es un objetivo de la invención proporcionar una disposición nueva de transferencia de datos cifrados requerida por la disposición de control remoto de los dispositivos técnicos en una propiedad, donde la conexión de Internet ya existente en las propiedades y viviendas se utiliza como tal en el uso remoto del servicio del sector de la construcción y de la vigilancia. Con el método de establecimiento de la conexión de comunicaciones de datos según la invención, la conexión de destino de la propiedad se modifica para que resulte, como tal, adecuada para un uso remoto. No se modifican funciones ya existentes de la conexión de la red de datos en el destino y de la intranet en el destino.

Los objetivos de la invención se logran con un método de establecimiento de una conexión de transferencia de datos, en la cual un dispositivo de red de control doméstico instalado de una manera fija en una propiedad y una llave de red de control doméstico de una persona que lleva a cabo la monitorización de la propiedad, establecen una conexión bidireccional segura a través de Internet sobre la base de información de contacto que han recibido desde un servidor de red de control doméstico de acuerdo con la invención. El dispositivo de red de control doméstico en la propiedad, al cual están conectados los dispositivos a controlar o monitorizar remotamente en la propiedad, está conectado a un dispositivo de interfaz de red de datos/terminal de red en la propiedad, por ejemplo, un módem.

Las direcciones IP actuales del dispositivo de red de control doméstico y la llave de red de control doméstico se mantienen en el servidor de red de control doméstico relativo a la invención, usándose dichas direcciones IP para establecer una conexión entre dichos dispositivos. Debido a los métodos de establecimiento de conexión de acuerdo con la invención, los dos dispositivos mencionados se pueden conectar a alguna red privada, no pública, y pueden seguir estableciendo entre ellos mismos una conexión segura de transferencia de datos a través de Internet. Ventajosamente, para el establecimiento de la conexión de transferencia de datos a través de Internet entre la llave de red doméstica de control, móvil, y el dispositivo instalado, fijo, de red doméstica de control, basta con que dichos dispositivos, en algún punto de la conexión establecida, obtengan también una dirección IP pública, aun cuando simultáneamente el dispositivo de red de control doméstico y la llave de red de control doméstico tengan solamente direcciones IP no públicas. En una forma de realización preferida de la invención, el servidor de red de control doméstico no participa en el establecimiento de la conexión de transferencia de datos real, después de haber enviado las direcciones IP de los dispositivos con vistas a su disponibilidad para estos últimos.

Una ventaja asociada al método de establecimiento de la conexión de transferencia de datos utilizado en un sistema de control remoto de acuerdo con la invención en una propiedad, es que ambos dispositivos del par de dispositivos de red doméstica de control pueden buscar su encaminamiento desde la ubicación de su posición a la dirección IP del dispositivo de la propiedad que conecta con Internet y almacenar el encaminamiento buscado en un servidor aparte de red doméstica de control en Internet con vistas a su identificación y la dirección IP de los pares de dispositivos.

Es además una ventaja de la invención, que cada par de dispositivos de red doméstica de control de acuerdo con la invención constituye, independientemente, entre ellos mismos, un par de dispositivos o grupo de dispositivos único predeterminado, que se identifican entre sí en la red de transferencia de datos a establecer. Debido al método de identificación, la llave de red de control doméstico que lleva consigo el usuario o un programa de ordenador instalado en algún dispositivo de procesado de datos - implementando dicho programa de ordenador las funciones de una llave de red de control doméstico -, establece una conexión de red solamente con su propio par único de dispositivo de red de control doméstica, y la conexión no se puede establecer con ningún otro dispositivo de red.

Es además una ventaja de la invención, que el par de dispositivos del sistema de control remoto según la invención puede establecer, entre ellos mismos, independientemente, con la ayuda de la información de direcciones del servidor de red doméstica de control, una conexión de transferencia de datos de nivel de capa de enlace de datos (Capa 2) o también de nivel de capa de red (Capa 3) de acuerdo con un modelo OSI (Modelo de Referencia de Interconexión de Sistemas Abiertos) seguro bidireccional directo, a través de los dispositivos de red local de servicio e Internet (VPN; Red Privada Virtual).

Es además una ventaja de la invención que el par de dispositivos de red doméstica de control pueden establecer entre ellos una conexión segura de transferencia de datos también a través de cortafuegos tales que cambien ocasionalmente sus puertos o bien de origen o bien de destino.

El método de establecimiento de una red privada virtual entre un par de terminales de red predeterminados de una red doméstica de control de acuerdo con la invención se caracteriza por que una llave de red de control doméstico y un dispositivo de red de control doméstico dan inicio, con varios métodos de establecimiento conocidos de una red privada virtual, a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo

con el fin de proporcionar por lo menos una red privada virtual.

La llave de red de control doméstico de acuerdo con la invención que se va a conectar a la red privada virtual incluye un procesador, una memoria y un código de programa de ordenador almacenado en la misma, y se caracteriza por que el procesador, la memoria y el código de programa de ordenador almacenado en la misma están configurados para dar inicio con varios métodos conocidos de establecimiento de una red privada virtual a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo con el fin de proporcionar por lo menos una red privada virtual con el dispositivo de red doméstica de control.

El dispositivo de red de control doméstico de acuerdo con la invención, que se va a conectar a una red privada virtual, incluye un procesador, una memoria y un código de programa de ordenador almacenado en la misma, y está caracterizado por que el procesador, la memoria y el código de programa de ordenador almacenado en la misma están configurados para dar inicio, con varios métodos conocidos de establecimiento de una red privada virtual, a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual con la llave de red doméstica de control.

El servidor de red de control doméstico de acuerdo con la invención, comprende elementos de interfaz de red, los cuales comprenden medios de entrada/salida, un procesador y una memoria, la cual contiene código de programa de ordenador, y están caracterizados por que el procesador, la memoria y el código de programa de ordenador almacenado en la misma están configurados para:

- enviar al dispositivo de red de control doméstico información que indica una parte libre de un ciberespacio, y

- liberar la conexión de transferencia de datos con el par de terminales de red, cuando se ha establecido satisfactoriamente por lo menos una red privada virtual directa entre el par de terminales de red.

El producto de programa de ordenador según la invención, utilizado en una llave de red doméstica de control, está caracterizado por que comprende medios de código para dar inicio, con varios métodos conocidos de establecimiento de una red privada virtual, a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual con el dispositivo de red doméstica de control.

El producto de programa de ordenador según la invención, utilizado en un dispositivo de red doméstica de control, está caracterizado por que comprende medios de código para dar inicio, con varios métodos conocidos de establecimiento de una red privada virtual, a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual con la llave de red doméstica de control.

La invención se lleva a la práctica de acuerdo con las reivindicaciones independientes adjuntas.

En las reivindicaciones dependientes se presentan algunas formas de realización ventajosas de la invención.

La idea básica de la invención es la siguiente: para implementar un control remoto en cierta propiedad, se ha fabricado un par de dispositivos - un dispositivo de red de control doméstico y una llave (dispositivo) de red doméstica de control - donde por lo menos un dispositivo de red de control doméstico y por lo menos una llave (dispositivo) de red doméstica de control pueden establecer una conexión segura de transferencia de datos únicamente entre sí. Dicha llave (dispositivo) de red doméstica de control o bien puede ser un dispositivo electrónico independiente fabricado para esta finalidad o bien también puede ser algún dispositivo de procesado de datos, en el cual se ha instalado un programa de ordenador de acuerdo con la invención, implementando dicho programa las funciones de la llave de red doméstica de control.

El dispositivo de red de control doméstico en la propiedad a controlar remotamente está instalado en una red de intranet o red de Internet existente en la propiedad a controlar. Establece una subred -una red de intranet de control- en la red de intranet o Internet, conectándose a dicha red de intranet de control varios accionadores a controlar en la propiedad, con una conexión de transferencia de datos o bien por cable o bien inalámbrica.

En una forma de realización ventajosa de la invención, una llave individual de red doméstica de control o varias llaves de red doméstica de control pueden funcionar como el par de dispositivo de dos o más dispositivos de red doméstica de control en diferentes propiedades. Los códigos de identificación del dispositivo de red de control doméstico y la llave de red de control doméstico se almacenan en dichos dispositivos en relación con su fabricación, o dichos dispositivos cambian sus códigos de identificación cuando se conectan por primera vez, por ejemplo, por sus puertos USB. Usando los códigos de identificación, el dispositivo de red de control doméstico y la llave de red de control doméstico establecen una conexión de transferencia de datos segura y bidireccional entre ellos.

En relación con el arranque, los dos dispositivos determinan información de encaminamiento de los dispositivos desde su red de ubicación íntegramente hasta un terminal de red conectado a Internet, siendo necesaria dicha

información de encaminamiento para el establecimiento de la conexión. Esta información de encaminamiento se almacena en un servidor de red de control doméstico de acuerdo con la invención, conectado a Internet. Cuando la llave (dispositivo) de red doméstica de control desea establecer una conexión de transferencia de datos, por medio de Internet, con su par de dispositivo en alguna propiedad, recupera la información de encaminamiento del dispositivo de red de control doméstico que funciona como su par desde el servidor de red doméstica de control. Utilizando la información de encaminamiento obtenida, la llave de red de control doméstico inicia el proceso de establecimiento de una conexión de transferencia de datos directa de extremo-a-extremo, proceso por el cual se establece ventajosamente una red privada virtual (VPN) segura entre la llave de red de control doméstico y el dispositivo de red doméstica de control. En este establecimiento de la conexión de transferencia de datos se usan protocolos de transferencia de datos adecuados según se requiera.

Se puede intentar establecer una conexión de transferencia de datos de extremo-a-extremo ventajosamente, primero como una conexión de transferencia de datos basada en TCP o como una conexión de transferencia de datos basada en UDP, si así lo permiten los componentes de la red de transferencia de datos entre los dispositivos.

Si la conexión de transferencia de datos a establecer tiene componentes de red (por ejemplo, cortafuegos) que cambian sus puertos de origen y/o de destino ocasionalmente, con el fin de evitar ataques a la red, entonces se intenta establecer una conexión de transferencia de datos de extremo-a-extremo ventajosamente, además de lo mencionado anteriormente, también mediante el uso de un escaneo de puertos UDP. Además del escaneo de puertos UDP, se puede intentar establecer una conexión de transferencia de datos de extremo-a-extremo también utilizando el protocolo ICMP.

Si, por un u otro motivo, no puede establecerse una conexión de transferencia de datos directa de extremo-a-extremo con los protocolos antes mencionados, se establece un túnel seguro basado en el protocolo TCP a través de un servidor de red de control doméstico relacionado con la invención. En esta forma de realización, el servidor de red de control doméstico no cifra los mensajes seguros recibidos por él, sino que los traslada directamente, tal como están, al dispositivo receptor. Si, durante esta conexión de retransmisión de TCP establecida, se observa que resultaría posible establecer una conexión de transferencia de datos de VPN, entonces la transferencia de datos se cambia ventajosamente a esta otra conexión de transferencia de datos bidireccional de extremo-a-extremo.

Cuando se ha establecido o bien una conexión de transferencia de datos directa o bien una conexión de transferencia de datos, retransmitida a través del servidor de red doméstica de control, se ha establecido entonces una conexión de transferencia de datos de VPN directa entre la llave de red de control doméstico y el dispositivo de red de control doméstico en la propiedad.

Un dispositivo de red de control doméstico de acuerdo con la invención se instala en la red de transferencia de datos interna de una propiedad a controlar remotamente, entre una red de transferencia de datos interna existente relacionada con el control y la gestión de la propiedad y un terminal de red que retransmite tráfico desde la propiedad a Internet. Todos los dispositivos relacionados con el control de la propiedad se conectan a las entradas del dispositivo de red doméstica de control, y la salida del dispositivo de red de control doméstico se conecta a la entrada destinada al dispositivo de intranet del terminal de red que retransmite tráfico de Internet.

En un sistema de red doméstica de control de acuerdo con la invención, la llave de red de control doméstico es un dispositivo de un terminal de red y un dispositivo de procesado de datos adecuado, conectado o bien de manera inalámbrica o bien por medio de una conexión por cable.

En otra forma de realización de acuerdo con la invención, la llave de red de control doméstico se puede conectar a algún dispositivo de procesado de datos conectado a Internet. Posibles dispositivos de procesado de datos son, por ejemplo, un PC, un ordenador de tipo tableta o un teléfono inteligente. En esta forma de realización, la conexión de la llave de red de control doméstico con el dispositivo de procesado de datos se puede realizar, por ejemplo, con la ayuda de una interfaz de LAN (Red de Área Local), una interfaz de WLAN (LAN Inalámbrica), una interfaz de WAN (Red de Área Extensa), 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 llave de red de control doméstico se almacena en unos medios portátiles de almacenamiento de datos, por ejemplo, una unidad de memoria USB, desde los cuales pueden instalarse el programa de ordenador en un dispositivo adecuado de procesado de datos.

El programa instalado en el dispositivo de procesado de datos simula todas las funciones de la llave de red doméstica de control.

En lo sucesivo, se describirá la invención de forma detallada. En la descripción, se hace referencia a los dibujos adjuntos, en los cuales

la figura 1a muestra a título de ejemplo cómo puede establecerse una conexión de transferencia de datos bidireccional de acuerdo con la invención, entre un dispositivo de cliente que gestiona el control

remoto y un dispositivo de control o gestión individual de una propiedad,

la figura 1b muestra otro ejemplo de acuerdo con la invención, en el cual se puede establecer una conexión de transferencia de datos bidireccional entre un dispositivo de cliente que gestiona el control remoto y un dispositivo de control o gestión individual de una propiedad,

la figura 2 muestra, en forma de diagrama de flujo ejemplificativo, cómo se establece una conexión de transferencia de datos entre el dispositivo de cliente y el dispositivo en una propiedad,

la figura 3a muestra, a título de ejemplo, las etapas parciales incluidas en la etapa 201 de la figura 2,

la figura 3b muestra, a título de ejemplo, la etapa de establecimiento incluida en la etapa 206 de la figura 2,

la figura 4 muestra, a título de ejemplo, un dispositivo de red de control doméstico de acuerdo con la invención,

la figura 5a muestra, a título de ejemplo, una llave de red de control doméstico de acuerdo con la invención,

la figura 5b muestra, a título de ejemplo, otra llave de red de control doméstico según la invención,

la figura 6 muestra, a título de ejemplo, un servidor de red de control doméstico de acuerdo con la invención, y

la figura 7 muestra capas de conexión de acuerdo con la invención, utilizadas en el sistema de red doméstica de control.

Las formas de realización de la siguiente descripción se aportan únicamente como ejemplos, y aquellos versados en la materia pueden llevar a la práctica la idea básica de la invención también de alguna otra manera diferente a la descrita en la descripción. Aunque la descripción puede referirse a una cierta forma o formas de realización en varios lugares, esto no significa que la referencia remita a solamente una forma de realización descrita o que la característica descrita sea utilizable solamente en una forma de realización descrita. Las características individuales de dos o más formas de realización se pueden combinar, y, por lo tanto, pueden proporcionarse nuevas formas de realización de la invención.

Las figuras 1a y 1b muestran dos formas de realización ventajosas 1A y 1B del sistema de control remoto de acuerdo con la invención. En los ejemplos de las figuras 1a y 1b, una llave de red de control doméstico 42, 42b o un dispositivo de procesado de datos 41c, que se ha convertido por medio de software en una llave de red doméstica de control, se usa para establecer una conexión de transferencia de datos con un dispositivo de red de control doméstico 61 en cierta propiedad. La llave de red de control doméstico 42, 42b o el dispositivo de procesado de datos 41c convertido en llave de red de control doméstico de acuerdo con la invención, también puede funcionar ventajosamente, sin embargo, con dispositivos de red doméstica de control independientes en dos o más propiedades.

En las dos formas de realización de las figuras 1a y 1b, la red de transferencia de datos tiene principalmente la misma estructura de red básica. En las dos figuras, Internet se muestra con la referencia 2. Alguna red pública o una intranet, referencia 3, está conectada también a Internet 2. La red 3 puede ser una red de transferencia de datos fija o inalámbrica. En la figura 1a, una primera red de transferencia de datos 4, la red remota doméstica de control de la propiedad, está conectada a la red 3, pudiéndose conectar a dicha red remota doméstica de control el dispositivo de cliente que implementa el control remoto, referencia 41a. En la figura 1b, la llave de red de control doméstico 42b se conecta al dispositivo de procesado de datos 41c, el cual nuevamente se conecta a una red pública/red de intranet 3.

Cuando un dispositivo de red de control doméstico 61 o una llave de red de control doméstico 42, 42b se conecta a su propia red local de transferencia de datos, envía de vez en cuando una interrogación de sondeo (del inglés, “polling”) al servidor de red de control doméstico 21 perteneciente al sistema de control remoto, con el fin de averiguar si su propio dispositivo homólogo está conectado o no a la red. Si, a partir de la respuesta enviada por el servidor de red de control doméstico 21, resulta evidente que el dispositivo homólogo está conectado a su propia red de transferencia de datos, los dos miembros del par de dispositivos inician el proceso de establecimiento de una red privada virtual (conexión de transferencia de datos de VPN) por medio de procedimientos que se describen posteriormente.

La intranet doméstica en la propiedad a controlar remotamente se designa en las figuras 1a y 1b con la referencia 5. Una segunda red de transferencia de datos 6, que es una intranet doméstica de control, está conectada a la red de intranet doméstica 5. Los accionadores 62 a 65 que se van a controlar remotamente en la propiedad están conectados a la intranet doméstica de control.

Es evidente para alguien versado en la materia que también pueden existir más subredes entre el dispositivo de red de control doméstico 61 y/o la llave de red de control doméstico 42, 42b o 41c según la invención e Internet 2, en

comparación con lo que se muestra en las figuras 1a y 1b.

En los ejemplos de las figuras 1a y 1b, el segundo terminal de red de acuerdo con la invención, que es el dispositivo de red de control doméstico 61 (HCND), está conectado a la red de intranet doméstica 10.0.0.0/24, referencia 5. La red de intranet doméstica 5 está conectada a Internet 2 con el terminal de red 51. El terminal de red 51 puede ser un router, un módem o un cortafuegos, los cuales pueden incluir también un traductor de direcciones de red NAT. En los ejemplos de las figuras 1a y 1b, la intranet doméstica 5 está detrás de un cortafuegos FW1, referencia 51, que contiene una función de NAT. La dirección IP pública del cortafuegos FW1 es 240.1.1.2 en los ejemplos de las figuras 1a y 1b. En la intranet doméstica 5, la dirección IP interna del cortafuegos FW1 es 10.0.0.1. Otros dos dispositivos ejemplificativos de procesado de datos también están conectados a la red de intranet doméstica 5, cuyas direcciones IP en la red de intranet doméstica son 10.0.0.3 y 10.0.0.4.

La red de intranet doméstica de control 172.17.0.0/24 (HCI), referencia 6, está conectada a la red de intranet doméstica 5 por medio del dispositivo de red de control doméstico 61. La dirección IP del dispositivo de red de control doméstico 61 en la red de intranet doméstica de control es 172.17.0.1, y en la red de intranet doméstica 10.0.0.2. En los ejemplos de las figuras 1a y 1b, cuatro dispositivos/servidores ejemplificativos 62, 63, 64 y 65 están conectados a la intranet doméstica de control 6. Los dispositivos/servidores se pueden conectar a la intranet doméstica de control 6 ó bien con una conexión permanente o bien con una conexión de transferencia de datos inalámbrica.

La referencia 62 muestra un servidor web de control de iluminación, cuya dirección IP en la red de intranet doméstica de control es 172.17.0.5. Para un usuario remoto, el servidor web de control de iluminación 62 se ve como el dispositivo HCND4.

La referencia 63 muestra un servidor web de control de calefacción, cuya dirección IP en la red de intranet doméstica de control es 172.17.0.4. Para un usuario remoto, el servidor web de control de calefacción 63 se ve como el dispositivo HCND1.

La referencia 64 muestra un servidor web de cámaras de vigilancia, cuya dirección IP en la red de intranet doméstica de control es 172.17.0.3. Para un usuario remoto, el servidor web de cámaras de vigilancia 62 se ve como el dispositivo HCND2.

La referencia 65 muestra un servidor web de aire acondicionado, cuya dirección IP en la red de intranet doméstica de control es 172.17.0.2. Para un usuario remoto, el servidor web de aire acondicionado 65 se ve como el dispositivo HCND3.

En el ejemplo de la figura 1a, el primer terminal de red de acuerdo con la invención, que es la llave de red de control doméstico 42 (HCNK), está conectado a la red remota doméstica de control 172.17.0.0/24, referencia 4. La red remota doméstica de control 4 está detrás del cortafuegos FW1 de la intranet 3, referencia 31. La dirección IP pública del cortafuegos de NAT 31 es en este ejemplo 240.2.1.2, y la dirección IP interna del cortafuegos de NAT es 10.0.1.1.

La red remota doméstica de control 172.17.0.0/24 (HCRN), referencia 4, está conectada a la red de transferencia de datos 3 por medio de una llave de red de control doméstico 42 de acuerdo con la invención. La dirección IP de la llave de red de control doméstico 42 en la red de intranet es 10.0.1.2, y en la red remota doméstica de control 172.17.0.6. En los ejemplos de las figuras 1a y 1b, un dispositivo de procesado de datos ejemplificativo 41a se ha conectado a la red remota doméstica de control 4, siendo 172.17.0.7 la dirección IP de dicho dispositivo de procesado de datos en la red remota doméstica de control 4. Se usa este dispositivo de procesado de datos 41a/41b, cuando se desea controlar de forma remota dispositivos/servidores 62, 63, 64 ó 65 conectados a la red de intranet doméstica de control 6.

La llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 de acuerdo con la invención necesitan mutuamente información de encaminamiento del otro, para que puedan establecer entre ellos una conexión de transferencia de datos sobre la base o bien de una capa de enlace de datos o bien de una capa de red, en los ejemplos de las figuras 1a y 1b una conexión de transferencia de datos de VPN 55. La información de encaminamiento determinada es almacenada tanto por la llave de red de control doméstico 42 como por el dispositivo de red de control doméstico 61 de acuerdo con la invención, en un servidor de red de control doméstico 21 (HCNS) en Internet.

En el ejemplo de la figura 1a, los cortafuegos de NAT no restringen totalmente la comunicación de UDP saliente. Son los denominados cortafuegos de NAT en un estado y "con memoria", que tampoco cambian los números de puerto de origen de conexiones de UDP (Protocolo de Datagrama de Usuario) de manera impredecible, si no es necesario. En el ejemplo de la figura 1a, el objetivo es establecer en la capa de enlace de datos una conexión de nivel de Ethernet entre la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61.

Cuando, en el sistema de control remoto 1A de acuerdo con la figura 1a, se desea establecer una conexión de

transferencia de datos 55 perteneciente a una red privada virtual (VPN) entre los dispositivos, entonces ambos dispositivos 42 y 61 recuperan del servidor de red de control doméstico 21, la información de encaminamiento almacenada en el mismo por el dispositivo homólogo. Antes de entregar la información de encaminamiento, el servidor de red de control doméstico 21 comprueba que se trata realmente de un par permitido de llave de red doméstica de control/dispositivo de red doméstica de control. Con la ayuda de la información de encaminamiento recuperada, la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 establecen una conexión de VPN directa entre ellos. Cuando se completa la conexión de VPN 55, un dispositivo de procesado de datos 41a en la red remota doméstica de control 4 puede entrar en contacto con un dispositivo 62, 63, 64 ó 65 en la red doméstica de control 6.

Para que resulte posible establecer la conexión de transferencia de datos, la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 deben determinar su ruta de red desde su propia red por lo menos hasta Internet 2. Más adelante, a dicha información de ruta de red se le hace referencia con la expresión información de encaminamiento. Esta determinación de la ruta de red se puede realizar, por ejemplo, de las siguientes maneras, que son utilizadas ventajosamente por la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61.

En el ejemplo de la figura 1a, las rutas de red son determinadas por la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61. Estos dispositivos almacenan las rutas de red descubiertas en el servidor de red de control doméstico 21, que las almacena en su memoria.

La llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 de acuerdo con la invención también tienen ventajosamente una capacidad de determinar un ciberespacio libre. Dichos dispositivos están configurados para determinar para ellos mismos un ciberespacio disponible automáticamente, utilizando la información de ruta de red en el servidor de red de control doméstico 21. Dichos dispositivos solicitan al servidor de red de control doméstico 21 que conceda cierta parte libre del ciberespacio. El servidor de red de control doméstico 21 examina las rutas de red que ha recibido, y devuelve cierto bloque de la red, donde no se menciona ni siquiera una dirección en la ruta de red de ningún dispositivo conocido.

El dispositivo de red de control doméstico 61 también ofrece ventajosamente servicios de DHCP y de DNS en sus propias subredes 4 y 6 para dispositivos conectados a las mismas. Adicionalmente, la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 funcionan como pasarela por defecto para dispositivos conectados a la subred.

La figura 1b muestra otro sistema de control remoto 1B de acuerdo con la invención. En la figura 1b, el dispositivo de procesado de datos 41c utilizado por el usuario se conecta a una red de transferencia de datos representada con el número de referencia 3. La forma de realización de la figura 1b difiere con respecto a la forma de realización de la figura 1a, en que las funciones de la llave de red de control doméstico 42 de la figura 1a se sustituyen por una llave de red de control doméstico 42b que incluye una memoria USB 42e, la cual se puede conectar a un dispositivo de procesado de datos 41c utilizado por el cliente. En esta forma de realización, el dispositivo de procesado de datos 41c y el dispositivo 42b funcionan conjuntamente como llave de red doméstica de control.

En otra forma de realización ventajosa de la invención, el programa de ordenador que implementa las funciones de una llave de red de control doméstico de acuerdo con la invención se instala en el dispositivo de procesado de datos 41c. El programa de ordenador se puede almacenar ventajosamente en el dispositivo de procesado de datos 41c, por ejemplo, desde una unidad de memoria USB conectando la unidad de memoria USB a un puerto USB del dispositivo de procesado de datos 41c. Para aquellos versados en la materia, resulta evidente que, como medios de almacenamiento para el programa de ordenador, pueden usarse también algunos otros medios de almacenamiento de datos de la técnica anterior. En esta forma de realización, el dispositivo de procesado de datos 41c simula una llave de red de control doméstico de acuerdo con la invención, con un programa de ordenador instalado en el mismo.

En el ejemplo de la figura 1b, la llave de red de control doméstico 42 de la figura 1a se simula en su totalidad o parcialmente en el dispositivo de procesado de datos 41c del usuario. El usuario, con este software de simulación, entra en contacto con un navegador en su dispositivo de procesado de datos 41c, o alternativamente, el software de simulación abre una ventana de un navegador en el dispositivo de procesado de datos 41c. La simulación se inicia con el lanzamiento del programa de simulación de acuerdo con la invención en el dispositivo de procesado de datos 41c, implementando dicho programa de simulación todas las funciones de una llave física de red doméstica de control 42 por medio de software.

En esta forma de realización, todas las funcionalidades de la llave de red de control doméstico 42 de la figura 1a, comunicación, arranque y establecimiento de conexión, se implementan utilizando el dispositivo de procesado de datos 41c del usuario, con lo cual no es necesaria una llave de red de control doméstico 42 físicamente independiente de acuerdo con la figura 1a, para establecer una conexión con un par de dispositivos 61 en la propiedad.

Si, por algún motivo, el establecimiento del túnel de VPN directo antes descrito no resulta satisfactorio entre la llave de red de control doméstico 42, 42b o 41c y el dispositivo de red de control doméstico 61 presentados en las figuras 1a y 1b, o resulta satisfactorio solo ocasionalmente (por ejemplo, si los componentes de la red cambian ocasionalmente los puertos de origen y/o destino), las disposiciones de control remoto pueden utilizar otros protocolos de acceso descritos en relación con la figura 3b. También en este caso, para el usuario del dispositivo de cliente el sistema de control remoto funciona de la misma manera que en los sistemas de control remoto presentados en la figura 1a o la figura 1b.

El siguiente es un ejemplo del funcionamiento del sistema de control remoto 1A de acuerdo con la invención, en el ejemplo de la figura 1a.

Dispositivo de red de control doméstico 61:

El dispositivo de red de control doméstico 61 está conectado a la red 10.0.0.0/24 (la intranet doméstica 5) por ejemplo, conectando un cable al puerto WAN del dispositivo de red de control doméstico 61. El dispositivo de red de control doméstico 61 recupera automáticamente sus valores de configuración de IP con el procedimiento de DHCP. Un cortafuegos FW1 en la red de intranet doméstica 5 funciona ventajosamente como servidor de DHCP, proporcionando dicho cortafuegos al dispositivo de red de control doméstico 61 la dirección IP 10.0.0.2 en una máscara de red de 24 bits (255.255.255.0). El servidor de DHCP también proporciona la dirección del router por defecto 10.0.0.1 y la dirección del servidor de DNS 10.0.0.1.

El dispositivo de red de control doméstico 61 da inicio a la comunicación determinando, con la ayuda del servidor de DNS, la dirección IP del servidor de red de control doméstico 21 (HCNS, dirección DNS etahallinta.fi). El servidor de DNS 10.0.0.1 proporciona la dirección IP del servidor de red de control doméstico 21 como 240.1.1.1.

El dispositivo de red de control doméstico 61 entra en contacto 240.1.1.1 con el servidor de red de control doméstico 21 a través de Internet con un protocolo TCP o UDP. El dispositivo de red de control doméstico 61 autentica los derechos de funcionamiento mutuos con el servidor de red de control doméstico 21 con certificados y/o contraseñas determinados en relación con la fabricación. Esta conexión de transferencia de datos se cifra ventajosamente, por ejemplo, con un cifrado SSL/TLS. El servidor de red de control doméstico 21 ve, desde la conexión entrante, la dirección IP pública del dispositivo de red de control doméstico 61, que, en el ejemplo de la figura 1a, es 240.1.1.2. El dispositivo de red de control doméstico 61 notifica al servidor de red de control doméstico 21 su propia dirección y máscara de red (10.0.0.2/24). El servidor de red de control doméstico 21 almacena esta información en su base de datos Tosibox.

El dispositivo de red de control doméstico 61 también lleva a cabo ventajosamente una operación de *traceroute* hacia el servidor de red de control doméstico 21 y comunica la ruta de red descubierta al servidor de red de control doméstico 21. El servidor de red de control doméstico 21 almacena la ruta de red recibida del dispositivo de red de control doméstico 61 en su base de datos Tosibox.

A continuación, el dispositivo de red de control doméstico 61 también lleva a cabo ventajosamente una operación de Registro de Ruta de ICMP y comunica la ruta descubierta al servidor de red de control doméstico 21. El servidor de red de control doméstico 21 almacena la ruta recibida desde el dispositivo de red de control doméstico 61 en su base de datos Tosibox.

Después de esto, el dispositivo de red de control doméstico 61 efectúa una determinación automática de ciberespacio libre enviando una consulta al servidor de red de control doméstico 21. El servidor de red de control doméstico 21 devuelve al dispositivo de red de control doméstico 61, en los ejemplos de las figuras 1a y 1b, el ciberespacio 172.17.0.0/24.

El dispositivo de red de control doméstico 61 utiliza el ciberespacio para su intranet 6, y, como dirección IP propia, el dispositivo de red de control doméstico 61 adopta 172.17.0.1. El dispositivo de red de control doméstico 61 notifica al servidor de red de control doméstico 21 dicha utilización, y el servidor almacena la información en su base de datos Tosibox.

En las figuras 1a y 1b, el dispositivo de red de control doméstico 61 se muestra como su propio dispositivo independiente, que establece su propia subred para controlar dispositivos en una propiedad. Resulta evidente para aquellos versados en la materia que las funciones del dispositivo de red de control doméstico 61 se pueden integrar como parte de un dispositivo de ingeniería computarizado o doméstico, el cual tenga una capacidad de procesador y de memoria suficiente y medios de conexión para conectar diversos medios técnicos a los mismos o bien con una conexión de transferencia de datos por cable o bien con una conexión de transferencia de datos inalámbrica.

Llave de red de control doméstico 42:

En el ejemplo de la figura 1a, el puerto WAN de la llave de red de control doméstico 42 está conectado a la red 10.0.1.0/24 (red de transferencia de datos 3). La llave de red de control doméstico 42 recupera información de

direcciones IP a partir del servidor de DHCP, funcionando como tal un cortafuegos FW2, referencia 31. La llave de red de control doméstico obtiene la dirección IP 10.0.1.2. La dirección del router por defecto 31 de la llave de red de control doméstico 42 es 10.0.1.1, y la dirección del servidor de DNS 31 es 10.0.1.1, que se obtienen del servidor de DHCP.

La llave de red de control doméstico 42 da inicio a la comunicación determinando, con la ayuda del servidor de DNS, la dirección IP del servidor de red de control doméstico 21 (HCNS, dirección DNS hcns.fi). En los ejemplos de las figuras 1 y 2, el servidor de DNS 10.0.1.1 proporciona 240.1.1.1 como dirección IP del servidor de red de control doméstico 21.

Después de esto, la llave de red de control doméstico 42 entra en contacto con el servidor de red de control doméstico 21 en la dirección 240.1.1.1 a través de Internet fundamentalmente con un protocolo UDP, y en segundo lugar con un protocolo TCP. La llave de red de control doméstico 42 autentica los derechos de funcionamiento mutuos con el servidor de red de control doméstico 21 con certificados y/o contraseñas previamente distribuidos. La conexión de transferencia de datos se cifra ventajosamente, por ejemplo, con un cifrado SSL/TLS. El servidor de red de control doméstico 21 ve, desde la conexión entrante, la dirección IP pública 240.2.1.2 de la llave de red de control doméstico 42. La llave de red de control doméstico 42 notifica adicionalmente al servidor de red de control doméstico 21 su propia dirección y máscara de red 10.0.1.2/24. El servidor de red de control doméstico 21 almacena esta información en su base de datos Tosibox.

A continuación, la llave de red de control doméstico 42 efectúa una operación de *traceroute* y comunica la ruta de red descubierta al servidor de red de control doméstico 21, que almacena la información en su base de datos Tosibox.

La llave de red de control doméstico 42 también lleva a cabo ventajosamente una operación de registro de ruta de ICMP, y comunica la ruta de red descubierta al servidor de red de control doméstico 21, que almacena la información en su base de datos Tosibox.

El servidor de red de control doméstico 21 comprueba la información de encaminamiento recibida y, si se producen solapamientos, el servidor de red de control doméstico 21 los comunica a la llave de red de control doméstico 42, que, si es necesario, ejecuta la determinación automática de ciberespacio libre nuevamente.

Dispositivo de procesado de datos 41c como llave de red doméstica de control:

En la forma de realización 1B según la figura 1b, la llave de red de control doméstico 42 se puede sustituir o bien por una llave de red de control doméstico 42b o bien por un dispositivo de procesado de datos 41c del usuario, en donde se ha almacenado un programa de ordenador que comprende las funciones de la llave de red de control doméstico desde unos medios adecuados de almacenamiento de datos, por ejemplo, una unidad de memoria USB. Dicha llave de red de control doméstico 42b puede ser ventajosamente un denominado dispositivo electrónico que comprenda una conexión USB. En la forma de realización de la figura 1b, las funciones antes descritas de la llave de red de control doméstico 42 son ejecutadas por un programa de ordenador instalado en el dispositivo de procesado de datos 41c del usuario desde una unidad de memoria USB.

En la forma de realización de acuerdo con la figura 1b, el emparejamiento de la llave de red de control doméstico 42b y el dispositivo de red de control doméstico 61 se puede determinar o bien en relación con la fabricación o bien en el destino de utilización final. Si la determinación del par se realiza en el destino de utilización final, entonces, la llave de red de control doméstico 42b, en la forma de realización según la figura 1b, se conecta temporalmente al dispositivo de red de control doméstico 61. La conexión se implementa ventajosamente o bien por medio de los puertos USB de los dispositivos o bien a través de una red de radiocomunicaciones inalámbrica.

Con el acoplamiento, la llave de red de control doméstico 42b y el dispositivo de red de control doméstico 61 pueden recibir el código de identificación de su par de dispositivo y enviar su propio código de identificación a su par de dispositivo. Posteriormente, estos dos dispositivos pueden establecer una conexión de transferencia de datos únicamente entre ellos.

La transferencia de programa de ordenador de la llave de red de control doméstico al terminal de usuario 41c del usuario se implementa ventajosamente de la manera siguiente.

Cuando la llave de red de control doméstico 42b se enlaza momentáneamente mediante su conexión con el dispositivo de procesado de datos 41c, entonces el programa de ordenador contenido en la llave de red de control doméstico 42b con sus códigos de identificación individuales se instala en el dispositivo de procesado de datos 41c del usuario, referencia 42e. En relación con la instalación, se le pregunta al usuario del dispositivo de procesado de datos 41c si desea utilizar una función de protección del dispositivo y/o programa. Si se desea activar la función de protección, entonces, en este caso, el programa de instalación de la llave de red de control doméstico solicita que el usuario proporcione su contraseña o bien solamente al dispositivo de procesado de datos 41c del usuario o bien al programa instalado o bien, si lo desea, a ambos.

La llave de red de control doméstico con sus programas, códigos de identificación individuales y contraseñas también se puede almacenar, si se desea, por ejemplo, en un servidor de red interno bien protegido, desde el cual la misma, cuando sea necesario, se puede retornar a una nueva llave de red de control doméstico (por ejemplo, en caso de que el dispositivo de llave original se pierda o rompa).

En una forma de realización ventajosa de la invención, el programa contenido en la llave de red de control doméstico 42b con sus códigos de identificación, también se puede almacenar en varios dispositivos de procesado de datos 41c, que pueden funcionar, así, en paralelo con el primer dispositivo de procesado de datos.

En una forma de realización ventajosa de la invención, el programa de ordenador contenido en la llave de red de control doméstico 42b también se puede situar, por ejemplo, en un servidor en Internet, desde donde puede recuperarse el mismo. En esta forma de realización ventajosa, la propia llave física de red doméstica de control 42b puede comprender solamente el código de identificación necesario para identificar el par de dispositivos.

La figura 2 muestra, en forma de un diagrama de flujo ejemplificativo, las operaciones del método de control remoto de acuerdo con la invención, después de que se hayan emparejado entre sí la llave de red de control doméstico 42 o 42b y el dispositivo de red de control doméstico 61.

Cuando un dispositivo de red de control doméstico 61 o una llave de red de control doméstico 42, 42b se conecta a su propia red local de transferencia de datos, envía/envían ocasionalmente una interrogación de sondeo (el denominado *polling*) al servidor de red de control doméstico 21 perteneciente al sistema de control remoto, con el fin de averiguar si su propio par de dispositivo homólogo está conectado o no a la red. Si, a partir de la respuesta enviada por el servidor de red de control doméstico 21, resulta evidente que el par de dispositivo homólogo está conectado a su propia red de transferencia de datos, entonces los dos miembros del par de dispositivos dan inicio al proceso de establecimiento de una red privada virtual (conexión de transferencia de datos de VPN) a través de procedimientos que se describen posteriormente.

En la etapa 200, el dispositivo de red de control doméstico 61 se conecta a la red de intranet doméstica 5, y ventajosamente también la llave de red de control doméstico 42 o el dispositivo de procesado de datos 41c que soporta o simula la llave de red de control doméstico 4ab a la red de intranet 3. Todos los dispositivos que se van a controlar remotamente en la propiedad se conectan al dispositivo de red de control doméstico 61 o bien con una conexión permanente o bien con una conexión inalámbrica.

En la etapa 201, tanto el dispositivo de red de control doméstico 61 como la llave de red de control doméstico 42, 42b o el dispositivo de procesado de datos 41c que simula la llave de red de control doméstico 41c determinan su ruta de red hacia el servidor de red de control doméstico 21, en caso de que su información actual de ruta de red no esté actualizada. El procedimiento usado en la etapa 201 se muestra más detalladamente en la figura 3a.

En la etapa 302, el dispositivo de red de control doméstico y/o la llave de red de control doméstico 42, 42a o el dispositivo de procesado de datos 41c que simula la llave de red doméstica de control, almacenan sus rutas de red determinadas en el servidor de red de control doméstico 21, en caso de que se pudiera determinar la información de ruta de red actualizada.

En la etapa 203, los dispositivos 42, 42a ó 41c y 61 de acuerdo con la invención, que se van a utilizar en el control remoto, reciben la información de que su par de dispositivo se ha registrado en el servidor de red de control doméstico 21 o que falta el registro. Si falta la información actualizada de ruta de red del dispositivo 42, 42b, 41c ó 61 según la invención, perteneciente a uno de los pares de dispositivo, entonces el sistema de control remoto 1A ó 1B pasa, después de un retardo especificado 212, a la etapa de escucha y comprobación 213 de la conexión del servidor de red doméstica de control.

En el inicio del establecimiento de la conexión, tanto la llave de red de control doméstico 42/42b como el dispositivo de red de control doméstico 61 solicitan, en la etapa 204, la información actualizada de ruta de red de su homólogo, a partir del servidor de red de control doméstico 21. El servidor de red de control doméstico 21 comprueba que se trata de un par de dispositivo permitido, predeterminado, y, después de la comprobación, envía la información de ruta de red a los dos dispositivos en la etapa 205. Después de esto, el servidor de red de control doméstico 21 libera la conexión para ambos dispositivos 42/42b y 61, y, de este modo, ya no forma parte del túnel de VPN 55 que se está formando.

En la etapa 206, la llave de red de control doméstico 42/42b/41c y el dispositivo de red de control doméstico 61 forman entre ellos un túnel de VPN 55. Las etapas parciales incluidas en la etapa 206 se describen más detalladamente en la figura 3b.

En la etapa 207, tanto el dispositivo de cliente 41a ó 41c del usuario como el dispositivo de destino 62 a 65 de la propiedad se conectan a la red de VPN establecida.

En la forma de realización de la figura 1a, el dispositivo de cliente 41a del usuario se conecta a la red de VPN por medio de la llave de red de control doméstico 42. En la forma de realización de la figura 1b, la llave de red de control doméstico 42b conectada al dispositivo de procesado de datos 41c del usuario es uno de los puntos extremos de la red de VPN. El dispositivo 62 a 65 que se controlará remotamente en el destino se conecta a la red VPN por medio del dispositivo de red de control doméstico 61.

En la etapa 208, el dispositivo de cliente 41a ó 41c del usuario y el dispositivo 62 a 65 a controlar en la propiedad forman parte de la misma red VPN, con lo cual pueden intercambiar información entre sí. Después de un retardo especificado en el sistema de control remoto, la etapa 209 consiste en comprobar si la conexión de transferencia de datos entre el dispositivo de cliente 41a ó 41c y el dispositivo de destino 62 a 65 sigue todavía activa. Si la conexión de transferencia de datos está activa, el proceso vuelve a la etapa 208 y se permite continuar con la transferencia de datos.

Si, en la etapa 209, se observa que la conexión de VPN ya no está activa, entonces se toma una decisión en la etapa 210 con respecto a un posible intento nuevo de establecer una conexión.

Si, en la etapa 210, se decide realizar un nuevo intento de establecimiento de una conexión, entonces el proceso se ramifica a la etapa 214. En la etapa 214, se comprueba si los miembros conocen las rutas de red actualizadas del homólogo. Si la información de ruta de red está actualizada, el proceso se ramifica a la etapa 205, donde el servidor de red de control doméstico envía la información actualizada de ruta de red del homólogo a los dispositivos según la invención para establecer un túnel de VPN.

Si, en la etapa 214, se observa que falta uno de los detalles de la ruta de red o el mismo no está actualizado, el proceso vuelve a la etapa 201, donde se renueva la determinación de la información de ruta de red de uno o ambos de los dispositivos de acuerdo con la invención.

En esta alternativa, el proceso también incluye ventajosamente procedimientos necesarios para liberar la conexión de VPN, de manera que el propio proceso de establecimiento de la conexión de acuerdo con la invención se puede renovar satisfactoriamente. El establecimiento de la conexión se intenta según un número de veces predeterminado.

Si, en la etapa 210, se decide que ya no se realizará ningún nuevo intento de establecer una conexión de VPN, debido a que se ha alcanzado un número predeterminado de intentos de establecimiento de conexión o, por algún otro motivo, no se desea establecer una conexión de VPN, entonces el proceso pasa a la etapa 211. En la etapa 211, se libera la red usada de transferencia de datos de VPN. Esto es lo que ocurre, por ejemplo, cuando se apaga la llave de red doméstica de control.

Después de que se haya liberado la red de transferencia de datos de VPN, se produce a continuación un retardo predeterminado 212 en el proceso utilizado en el sistema de control remoto 1A ó 1B. Después del retardo 212, el proceso pasa a la función de escucha 213 del servidor de red doméstica de control. Allí, por lo menos el dispositivo de red de control doméstico 61 que tiene corriente envía ocasionalmente solicitudes de conexión al servidor de red de control doméstico 21.

El dispositivo de red de control doméstico 61 envía ventajosamente solicitudes de conexión hasta que el servidor de red de control doméstico 21 le envía a él la información actualizada de ruta de red. Cuando se ha recibido la información de ruta de red, el proceso de establecimiento de la conexión de VPN se pone en marcha en la etapa 201.

La ramificación hacia la etapa 212 también puede tener lugar desde la etapa 203. Esto ocurre cuando la información de ruta de red de uno o de los dos no se ha podido determinar y almacenar en el servidor de red doméstica de control. Además, esta rama del proceso vuelve, después de las etapas 231 y 214, a la etapa 201, donde por lo menos uno de los dispositivos que participan en el control remoto intenta determinar su información de ruta de red y almacenarla en el servidor de red de control doméstico 21.

Los procedimientos de búsqueda usados en la etapa 201 se describen más detalladamente en la figura 3a.

En la etapa 2011 se utiliza un protocolo DHCP (Protocolo de Configuración Dinámica del Anfitrión) con el que se pueden recuperar los valores de configuración de IP para la interfaz de red del dispositivo de procesado de datos. Los valores de configuración obtenibles con el procedimiento de DHCP incluyen por lo menos la dirección IP del dispositivo de procesado de datos, la máscara de red, la pasarela por defecto y el servidor de DNS (Sistema de Nombres de Dominio), que transforma los nombres de dominio en direcciones IP.

El procedimiento Traceroute utilizado en la etapa 2012 es una herramienta que usa el protocolo TCP/IP y que determina a través de qué vía o ruta de red se desplazan los paquetes a la máquina determinada. En el procedimiento Traceroute, un dispositivo de transferencia de datos conectado a la red establece la ruta de red incrementando el valor de Tiempo de Vida (TTL) de los paquetes que envía de uno en uno, comenzando desde cero.

El establecimiento de la ruta de red se produce típicamente de la siguiente manera. El dispositivo de procesado de datos envía a la pasarela por defecto un paquete IP con cierta dirección de destino en la red externa usando el valor de TTL "0". La pasarela por defecto responde a esto con un mensaje de expiración de TTL. A partir de este mensaje se revelan, por ejemplo, la dirección IP, el retardo, etcétera, de la pasarela por defecto.

Después de esto, el dispositivo de procesado de datos envía a la pasarela por defecto un paquete IP con cierta dirección de destino en la red externa usando el valor de TTL 1. Nuevamente, el router que sucede a la pasarela por defecto responde con un mensaje "expiración de TTL", a partir del cual queda clara la dirección IP de este router sucesivo (segundo). Se continúa con este proceso de transmisión/respuesta incrementando el valor de TTL hasta que se alcance el objetivo deseado. En el caso de Internet, el objetivo final se alcanza típicamente con un valor de TTL de 6 a 15. El resultado final es que el dispositivo de procesado de datos tiene conocimiento de la ruta de red al mundo exterior, por ejemplo, Internet.

En el establecimiento de direcciones externas se puede utilizar un protocolo de ICMP (Protocolo de Mensajes de Control de Internet). En el procedimiento de ICMP se usa un indicador (*flag*) de Registro de Ruta de un paquete de ICMP, de manera que dicho indicador solicita a los sistemas operativos de los dispositivos en la ruta de red que registren en el título del paquete de ICMP la dirección IP del router de transmisión.

La figura 3b muestra parte de los procedimientos de establecimiento de conexión 2060 a 2064 que posibilitan el establecimiento de un túnel de VPN y que se utilizan en la etapa 206 de la figura 2. En la figura 3b, los procedimientos alternativos de establecimiento de conexión se muestran como procesos paralelos que se utilizan de manera simultánea. No obstante, la invención no se limita a esta forma de realización, sino que también pueden implementarse procesos de establecimiento de conexión, en función de la aplicación, de una manera adecuada, como procesos de establecimiento de conexión sucesivos. En esta forma de realización, incluso después de un establecimiento de conexión de un túnel de VPN, no se intenta necesariamente utilizar otros métodos de establecimiento de conexión.

El ejemplo de la figura 3b muestra cinco métodos posibles de establecimiento de un túnel de VPN. Con la referencia 2060 se muestra el establecimiento de un túnel de VPN usando el protocolo TCP. Si los elementos de la red de comunicaciones entre el dispositivo de red de control doméstico y la llave de red de control doméstico permiten el establecimiento de la conexión, esto se averigua en la etapa 2060a. Si la conexión no puede establecerse, el establecimiento de la conexión se intenta nuevamente de forma ventajosa.

Con la referencia 2061, se muestra el establecimiento de un túnel de VPN usando el protocolo UDP. En la etapa 2061a se averigua si los elementos de la red de comunicación entre el dispositivo de red de control doméstico y la llave de red de control doméstico permiten el establecimiento de una conexión. Si la conexión no se puede establecer, el establecimiento de la conexión se intenta de forma ventajosa nuevamente.

Con la referencia 2062, se muestra el establecimiento de un túnel de VPN usando el escaneo de puertos UDP que se describe posteriormente. En la etapa 2062a se averigua si los elementos de la red de comunicación entre el dispositivo de red de control doméstico y la llave de red de control doméstico permiten el establecimiento de una conexión. Si la conexión no se puede establecer, el establecimiento de la conexión se intenta de forma ventajosa nuevamente.

Con la referencia 2063, se muestra el establecimiento de un túnel de VPN usando el procedimiento de ICMP que se describe posteriormente. En la etapa 2063a se averigua si los elementos de la red de comunicación entre el dispositivo de red de control doméstico y la llave de red de control doméstico permiten el establecimiento de una conexión. Si la conexión no se puede establecer, el establecimiento de la conexión se intenta de forma ventajosa nuevamente.

Con la referencia 2064, se muestra el establecimiento de un túnel de VPN usando el procedimiento de retransmisión de TCP que se describe posteriormente. De forma ventajosa, este procedimiento se utiliza cuando los elementos de la red de comunicaciones entre el dispositivo de red de control doméstico y la llave de red de control doméstico no permiten el establecimiento de un túnel directo de VPN de extremo-a-extremo. También en este procedimiento se averigua en la etapa 2062a si se estableció satisfactoriamente una conexión segura de transferencia de datos entre el dispositivo de red de control doméstico y la llave de red doméstica de control. Si la conexión no puede establecerse, el establecimiento de la conexión se intenta de forma ventajosa nuevamente.

Cada procedimiento de establecimiento de conexión 2060 a 2064 puede proporcionar una conexión de transferencia de datos de VPN entre el dispositivo de red de control doméstico 61 y la llave de red de control doméstico 42 o 42b. En la etapa 2069, se selecciona/seleccionan el túnel de VPN o los túneles de VPN que se usa/usan como conexión de transferencia de datos.

Todas las etapas del proceso mostradas en las figuras 2, 3a y 3b se implementan con órdenes de programa, las cuales se ejecutan en un procesador adecuado de propósito general o de propósito específico. Las órdenes del

programa se almacenan en un soporte de almacenamiento utilizado por el dispositivo de red de control doméstico 61 y la llave de red de control doméstico 42, tal como memorias, a partir de las cuales el procesador las puede recuperar e implementar. Las referencias a un soporte legible por ordenador también pueden contener, por ejemplo, componentes especiales, tales como memorias *Flash* USB programables, matrices lógicas (FPLA), circuitos integrados de aplicación específica (ASIC) y procesadores de señal (DSP).

Ejemplo de establecimiento de un túnel de VPN usando un protocolo UDP, referencia 2061, en la disposición de la figura 1a:

La llave de red de control doméstico 42 comienza el proceso de emparejamiento. Notifica al servidor de red de control doméstico 21 que desea establecer una conexión de transferencia de datos con el dispositivo de red de control doméstico 61 ventajosamente usando el protocolo UDP. El servidor de red de control doméstico 21 decide que la conexión de transferencia de datos solicitada se debería establecer con los siguientes números de puerto:

- llave de red doméstica de control: puerto de origen de UDP 10500, puerto de destino de UDP 10501, dirección IP de destino 240.1.1.2

- dispositivo de red doméstica de control: puerto de origen de UDP 10501, puerto de destino de UDP 10500, dirección IP de destino 240.2.1.2

El servidor de red de control doméstico 21 comunica esta información a la llave de red de control doméstico 42 y al dispositivo de red de control doméstico 61.

Después de esto, la llave de red de control doméstico 42 envía el paquete de UDP a la dirección 240.1.1.2 con puerto de origen 10500 al puerto de destino 10501. El paquete enviado atraviesa el cortafuegos FW2, que contiene una función de NAT, debido a que el tráfico saliente no está restringido fuertemente. El cortafuegos FW2 31 recuerda el paquete de UDP como una conexión durante los siguientes X segundos con la información de contacto 10.0.0.2, 240.1.1.2, 10500 y 10501.

El paquete de UDP llega al cortafuegos FW1 51, delante del dispositivo de red de control doméstico 61, no permitiendo dicho cortafuegos tráfico entrante y rechazando el paquete. El paquete no llega a la dirección 10.0.0.2.

El dispositivo de red de control doméstico 61 envía un paquete de UDP a la dirección 240.2.1.2 con puerto de origen 10501 al puerto de destino 10500. El paquete de UDP enviado pasa a través del cortafuegos de NAT FW1 51, ya que el tráfico saliente no está restringido. El cortafuegos FW1 51 recuerda el paquete de UDP como una conexión durante los X segundos siguientes, con la información de contacto 10.0.0.2, 240.2.1.2, 10501 y 10500.

El paquete de UDP llega al cortafuegos FW2 31. El cortafuegos FW2 31 recuerda que la dirección IP 10.0.1.2 había establecido una conexión de UDP con la dirección 240.1.1.2 con puerto de origen 10500 y puerto de destino 10501. Debido a que el paquete de UDP proviene de dicha dirección de origen 240.2.1.2, con puerto de origen 10501 y al puerto de destino 10500, el cortafuegos FW2 31 interpreta el paquete como una comunicación de retorno relacionada con la conexión establecida por el dispositivo 10.0.1.2. Después de esto, el cortafuegos FW2 efectúa una operación de cambio de dirección. Cambia la dirección de destino del paquete de UDP a 10.0.1.2. Después de esto, el cortafuegos FW2 31 encamina el paquete de UDP a la dirección 10.0.1.2. A continuación, la llave de red de control doméstico 42 recibe un mensaje desde el dispositivo de red de control doméstico 61. En este momento existe una conexión de transferencia unidireccional de datos desde el dispositivo de red de control doméstico 61 a la llave de red de control doméstico 42.

A continuación, la llave de red de control doméstico 42 envía el paquete de UDP a la dirección 240.1.1.2 con puerto de origen 10500 al puerto de destino 10501. El paquete de UDP llega al cortafuegos FW1 51. El cortafuegos FW1 51 recuerda que la dirección IP 10.0.1.2 había establecido una conexión UDP con la dirección 240.2.1.2 con puerto de origen 10501 y puerto de destino 10500. Debido a que el paquete de UDP proviene de dicha dirección de origen 240.2.1.2, con puerto de origen 10501 y al puerto de destino 10500, el cortafuegos FW2 51 interpreta el paquete recibido como una comunicación de retorno relacionada con la conexión establecida por el dispositivo 10.0.0.2. El cortafuegos FW1 51 lleva a cabo un cambio de dirección, es decir, cambia la dirección de destino del paquete a 10.0.0.2. Después de esto, el cortafuegos FW1 51 encamina el paquete a la dirección 10.0.0.2.

En este momento, existe una conexión UDP bidireccional entre la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61. Estos dispositivos pueden comunicarse entre sí bidireccionalmente. El dispositivo de red de control doméstico 61 y la llave de red de control doméstico 42 forman ventajosamente un túnel de VPN de nivel de capa de enlace de datos entre ellos, usando, por ejemplo, el software OpenVPN.

El dispositivo de red de control doméstico 61 puentea ventajosamente el túnel de VPN creado 55, con la red remota doméstica de control 172.17.0.0 /24, referencia 6, que administra. De la misma forma, la llave de red de control doméstico 42 puentea el túnel de VPN creado 55 con su puerto LAN, con lo que es posible proporcionar 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

remota doméstica de control 4 y la intranet doméstica de control 6 forman una red VPN privada a través de Internet 2.

Ejemplo de establecimiento de un túnel de VPN usando el escaneo de puertos UDP, referencia 2062, en la disposición de la figura 1a:

El escaneo de puertos UDP puede utilizarse si un elemento en la red de transferencia de datos cambia ocasionalmente los puertos o bien de origen o bien de destino. Las etapas del método que se describe a continuación difieren entre sí en función del hecho de si el elemento que cambia ocasionalmente los puertos de origen o de destino está delante del miembro emisor o receptor.

1. Escaneo sobre puertos de origen:

El cortafuegos 51 que está delante del dispositivo de red de control doméstico 61 cambia solamente la dirección de origen de los paquetes enviados, el puerto de origen no se cambia.

El dispositivo de red de control doméstico 61 inicia el envío de paquetes de UDP con la siguiente información: puerto de origen 5000, IP de origen 10.0.0.2, IP de destino 5.5.5.5, puertos de destino, por ejemplo, entre 1024 -> 1054 (30 puertos de origen diferentes). Los datos (carga útil) de cada paquete de UDP incluyen el puerto de destino seleccionado, por ejemplo, 1024. Por medio de esto, se sabe en el extremo receptor a qué puerto fue el paquete enviado a través del cortafuegos 31.

La frecuencia de envío de los paquetes de UDP es ventajosamente 200 milisegundos. En primer lugar, por ejemplo se envía un paquete de UDP con puerto de origen 1024, en 200 ms otro paquete de UDP con puerto de origen 1025, etcétera. Después de que se haya enviado el paquete de UDP con el último puerto de origen 1054 (después aproximadamente de 6 segundos), el dispositivo de red de control doméstico 61 envía nuevamente paquetes de UDP en el mismo orden comenzando desde el puerto de origen 1024.

Después de esto, también la llave de red de control doméstico 42 comienza a enviar paquetes de UDP con la siguiente información: IP de origen 10.0.1.2, IP de destino 6.6.6.6, puerto de destino 5000, puertos de origen, por ejemplo, entre 1024 -> 65535 (64.511 puertos de origen diferentes). La frecuencia de envío de los paquetes de UDP es ventajosamente 50 milisegundos. Es decir, primero se envía, por ejemplo, un paquete de UDP con puerto de origen 1024, en 50 ms otro paquete de UDP con puerto de origen 1025, etcétera. La carga útil de cada paquete de UDP incluye el puerto de origen usado, por ejemplo, 1024. Esta información se puede usar para reconocer cuál de los puertos de origen usados cambia y a qué puerto de origen cambia cuando pasa a través del cortafuegos de NAT 51.

El objetivo es que, durante esta etapa, el paquete de UDP enviado por la llave de red de control doméstico 42 pase a través del cortafuegos 51, o que el paquete de UDP enviado por el dispositivo de red de control doméstico 61 pase a través del cortafuegos 31 de la llave de red de control doméstico 42. Cuando uno u otro de los dispositivos ve que el paquete de UPD está allí, se responde a ese paquete de UDP con el mismo puerto de origen del cual se indicó que venía el paquete de UDP. Después de esto, puede iniciarse el establecimiento de la conexión de VPN.

El envío de los paquetes continúa hasta que se consigue que la conexión funcione o hasta que se cancele el establecimiento de la conexión.

2. Escaneo sobre puertos de destino:

El cortafuegos de NAT 31 que está delante de la llave de red de control doméstico 42 cambia la dirección de origen y el puerto de origen de los paquetes de datos enviados. Típicamente, el puerto de origen cambia ocasionalmente, por ejemplo el puerto de origen 1024 puede cambiar por ejemplo, al puerto de origen 16431.

La llave de red de control doméstico 42 inicia el envío de paquetes de UDP con la siguiente información: puerto de origen 5000, IP de origen 10.0.1.2, puerto de destino 6.6.6.6, puertos de origen, por ejemplo, entre 1024 -> 1054 (30 puertos de origen diferentes). Los datos (carga útil) de cada paquete de UDP incluyen un puerto de origen, por ejemplo, 1024. Por medio de esto, se sabe en el extremo receptor desde qué puerto de origen se envió el paquete de UDP que pasó a través del cortafuegos 31.

La frecuencia de envío de los paquetes de UDP es ventajosamente 200 milisegundos. En primer lugar, por ejemplo se envía un paquete de UDP con puerto de origen 1024, en 200 ms un paquete de UDP con puerto de origen 1025, etcétera. Después de que se haya enviado el paquete de UDP con el último puerto de origen 1054 (después aproximadamente de 6 segundos), la llave de red de control doméstico 42 envía nuevamente paquetes de UDP en el mismo orden comenzando desde el puerto de origen 1024.

Después de esto, el dispositivo de red de control doméstico 61 comienza a enviar paquetes de UDP con la siguiente información: IP de origen 10.0.0.2, IP de destino 5.5.5.5, puerto de origen 5000, puertos de destino, por ejemplo,

entre 1024 -> 65535 (64.511 puertos de destino diferentes). La frecuencia de envío de los paquetes es ventajosamente 50 milisegundos. Primero se envía un paquete de UDP con puerto de destino 1024, en 50 ms con puerto de destino 1025, etcétera. La carga útil de cada paquete de UDP incluye el puerto de destino usado por el paquete, por ejemplo, 1024. Esta información se puede usar para reconocer cuál de los puertos de destino usados cambia a qué puerto de destino cuando pasa a través del cortafuegos de NAT 31.

El objetivo es que, durante esta etapa, el paquete de UDP enviado por la llave de red de control doméstico 42 pase a través del cortafuegos 51 de delante del dispositivo de red de control doméstico 61, o que el paquete de UDP enviado por el dispositivo de red de control doméstico 61 pase a través del cortafuegos 31 de delante de la llave de red de control doméstico 42. Cuando uno de los dispositivos ve el paquete de UPD pasando a través, se responde a ese paquete con el mismo puerto de origen del cual parece estar viniendo el paquete.

El envío de los paquetes continúa hasta que se consigue que la conexión funcione o hasta que se cancele el establecimiento de la conexión.

En los dos casos antes mencionados, el establecimiento de la conexión de VPN se puede iniciar de la manera siguiente:

Trío de puertos usado con la conexión de VPN:

- puerto de origen usado por el dispositivo de red de control doméstico 61 (host1_real_source_port).

- puerto de origen transformado por el cortafuegos de NAT 51 del dispositivo de red doméstica de control, que es el mismo que el puerto de destino (host1_translated_source_port) usado por la llave de red de control doméstico 42

- puerto de destino (host2_real_source_port) usado por la llave de red de control doméstico 42.

El dispositivo de red de control doméstico 61 abre la conexión de VPN:

- IP de destino 6.6.6.6
- puerto de origen host1_real_source_port
- puerto de origen host2_real_source_port

La llave de red de control doméstico 42 abre la conexión de VPN:

- IP de destino 5.5.5.5
- puerto de origen host2_real_source_port
- puerto de destino host1_translated_source_port

Los dos cortafuegos de NAT 31 y 51 creen que la conexión se estableció desde su propia intranet, con lo cual la conexión de UDP se encamina a través de los cortafuegos de NAT 31 y 51.

Ejemplos de establecimiento de un túnel de VPN usando un protocolo ICMP, referencia 2063, en la disposición de la figura 1a:

El protocolo de control del protocolo IP puede utilizarse si el elemento de red en la red de transferencia de datos permite la comunicación para paquetes de tipo ICMP ECHO e ICMP ECHO REPLY.

Método de ICMP 1: ICMP ECHO ID permanente:

Esta forma de realización es posible cuando el(los) cortafuegos en la(las) red(es) de transferencia de datos no reacciona(n) a mensajes de expiración del TTL.

La llave de red de control doméstico 42 envía un paquete de IP por medio del router 10.0.1.1 con la siguiente información: IP de destino 6.6.6.6, IP de origen 10.0.1.2, TTL1, tipo ICMP, tipo de ICMP ECHO REQUEST, ID 1234, secuencia 1 y la carga útil del paquete está vacía.

El paquete enviado pasa a través del cortafuegos de NAT 31, con lo cual la IP de origen del paquete cambia -> 5.5.5.5, el TTL del paquete cambia 1 -> 0. El cortafuegos de NAT 31 recuerda que con el número de ID 1234, la IP de origen 10.0.1.2 cambió a 1 solicitud de eco.

El router en Internet 2 (no mostrado en la figura 1a), cuya dirección IP ejemplificativa es 3.1.1.1, recibe un paquete de IP, cuyo TTL es 0. Este router responde con un mensaje “expiración de tiempo de vida TTL de ICMP” al cortafuegos 31.

El cortafuegos 31 recibe un mensaje “expiración de tiempo de vida TTL de ICMP”, aunque, sin embargo, no reacciona al mismo.

El dispositivo de red de control doméstico 61 envía un paquete de IP a través del router 10.0.0.1 con la siguiente información: IP de destino 5.5.5.5, IP de origen 10.0.0.2, TTL 255, tipo ICMP, tipo de ICMP ECHO REPLY, ID 1234, Secuencia 1 y la carga útil del paquete incluye ventajosamente 30-1.400 bytes de comunicación de VPN.

El paquete enviado ICMP ECHO pasa a través del cortafuegos 51, con lo cual la IP de origen del paquete cambia -> 6.6.6.6. El paquete de ICMP llega al cortafuegos 31. El cortafuegos 31 recuerda que anteriormente se envió una solicitud con número de ICMP ECHO ID 1234. El cortafuegos 31 recuerda que el emisor de la solicitud fue el dispositivo 10.0.1.2. El cortafuegos 51 encamina al paquete adicionalmente a la dirección 10.0.1.2. La IP de destino del paquete cambia 5.5.5.5 -> 10.0.1.2.

La llave de red de control doméstico 42 recibe el paquete ICMP ECHO y, así, el dispositivo de red de control doméstico 61 ha enviado satisfactoriamente un paquete de datos en formato libre a la llave de red de control doméstico 42.

La llave de red de control doméstico 42 continúa enviando paquetes ICMP ECHO REQUEST, y el dispositivo de red de control doméstico 61 continúa enviando mensajes ICMP ECHO REPLY, respectivamente. La llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 han constituido entre ellos una conexión unidireccional de transferencia de datos.

A continuación, la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 forman también otra conexión de ICMP inversa. La conexión se establece tal como se ha descrito anteriormente. Solamente cambia la dirección del establecimiento de la conexión. Al final del proceso de establecimiento de la conexión, el dispositivo de red de control doméstico 61 recibe el paquete de ICMP enviado por la llave de red de control doméstico 42, incluyendo la carga útil de dicho paquete ventajosamente 30-1.400 bytes de comunicación de VPN.

La llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 continúan enviando solicitudes mutuamente tal como se ha descrito anteriormente. De este modo, en este momento existe una conexión bidireccional entre la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61. Los mensajes ECHO REPLY comprenden comunicación, cifrada por TLS, de la conexión de VPN, de manera que se ha formado satisfactoriamente una conexión de VPN directa que penetra en los cortafuegos de NAT 31 y 51, entre la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61.

Método de ICMP 2: ICMP ECHO ID variable:

La conexión de transferencia de datos puede tener un elemento de red, por ejemplo, un cortafuegos, que gestiona los mensajes de TTL (expiración de Tiempo de Vida) de tal manera que es necesaria una nueva ICMP ECHO REQUEST, con lo que seguiría una ICMP ECHO REPLY. Así, cada mensaje “expiración de TTL” se “come” el lugar de un paquete ICMP ECHO REPLY. Cuando este tipo de elemento de red ve un mensaje “expiración de TTL”, ya no encamina ningún mensaje “ICMP ECHO REPLY” al destino.

La diferencia de este método con respecto al caso de un ICMP ECHO ID permanente es que un ICMP ECHO ID es diferente en cada par de paquetes ICMP ECHO REQUEST e ICMP ECHO REPLY. El envío de un par de paquetes ICMP ECHO REQUEST e ICMP ECHO REPLY tiene lugar sincronizado en el tiempo, de manera que ICMP ECHO REQUEST e ICMP ECHO REPLY se envían de manera sustancialmente simultánea. De este modo, el ICMP ECHO REQUEST sale del cortafuegos de NAT del miembro emisor, antes de que el ICMP ECHO REPLY del otro dispositivo llegue al mismo cortafuegos.

Ventajosamente, como valor de TTL se usa un valor elevado, de manera que el paquete de ICP ECHO REQUEST permanezca en su camino el mayor tiempo posible antes de que el cortafuegos reciba o bien una “expiración de TTL” o bien una ICMP ECHO REPLY “incorrecta” del cortafuegos del otro extremo.

A continuación un ejemplo de este método de ICMP ECHO en el caso de la figura 1a:

La llave de red de control doméstico 42 envía un paquete de IP por medio del router 10.0.0.1 con la siguiente información: IP de destino 6.6.6.6, IP de origen 10.0.1.2, TTL 255, tipo ICMP, tipo de ICMP ECHO REQUEST, ID 1000, Secuencia 1 y la carga útil del paquete está vacía.

Simultáneamente, el dispositivo de red de control doméstico 61 envía un paquete de IP con la siguiente información: IP de destino 5.5.5.5, IP de origen 10.0.0.2, TTL 255, tipo ICMP, tipo de ICMP ECHO REPLY, ID 1000, Secuencia 1. La carga útil del paquete incluye en su inicio el número “2.000”, tras lo cual sigue la frecuencia de envío solicitada (por ejemplo 500 ms) del ICMP ECHO REQUEST, y, después de esto, comunicación de VPN en formato libre, ventajosamente 30-1.400 bytes.

El paquete de ICMP ECHO REQUEST enviado por la llave de red de control doméstico 42 pasa a través del cortafuegos de NAT 31. Así, la IP de origen del paquete cambia -> 5.5.5.5. El cortafuegos de NAT 31 recuerda que, con el número de ID 1000, la IP de origen 10.0.0.2 se convirtió en un ICMP ECHO REQUEST.

Simultáneamente, el paquete de ICMP ECHO REQUEST enviado por el dispositivo de red de control doméstico 61 pasa a través del cortafuegos de NAT 51. De este modo, la IP de origen del paquete cambia -> 6.6.6.6. El cortafuegos de NAT 51 recuerda que, con el número de ID 1000, la IP de origen 10.0.0.2 se convirtió en ICMP ECHO REQUEST.

Los paquetes enviados de ICMP ECHO REQUEST se “cruzan” en Internet 2, es decir, los dos paquetes están de camino en la red del operador al mismo tiempo.

El paquete de ICMP ECHO REQUEST llega al cortafuegos 51, y el cortafuegos 51 responde al mismo. El resultado de la respuesta no es significativo, ya que el ICMP ECHO REPLY enviado por el dispositivo de red de control doméstico 61 se ha enviado antes que el paquete de ICMP ECHO REPLY enviado por el cortafuegos 51. Tampoco es importante que el cortafuegos 51 no responda al paquete de ICMP ECHO REQUEST.

El paquete de ICMP ECHO REPLY enviado por el dispositivo de red de control doméstico 61 llega al cortafuegos 31. El cortafuegos 31 recuerda que anteriormente se envió un paquete de ICMP ECHO con número de ID 1000. El cortafuegos 31 recuerda que el emisor de la solicitud fue el dispositivo 10.0.1.2. El cortafuegos 31 encamina el paquete adicionalmente a la dirección 10.0.1.2 cambiando la IP de destino del paquete 5.5.5.5 -> 10.0.1.2.

La llave de red de control doméstico 42 recibe el paquete de ICMP y, de este modo, el dispositivo de red de control doméstico 61 ha enviado satisfactoriamente un paquete de ICMP de datos en formato libre a la llave de red de control doméstico 42.

A continuación, la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 forman también otra conexión de ICMP inversa. La conexión se establece tal como se ha descrito anteriormente. Únicamente cambia la dirección del establecimiento de la conexión. Al final del proceso de establecimiento de la conexión, la llave de red de control doméstico 42 recibe un paquete, cuya carga útil incluye comunicación de VPN ventajosamente de 30-1.400 bytes.

El dispositivo de red de control doméstico 61 y la llave de red de control doméstico 42 continúan enviando pares de paquetes de ICMP ECHO REQUEST e ICMP ECHO REPLY, de manera que cada par de paquetes de ICMP tiene un ECHO ID diferente. Así, los mensajes de ICMP ECHO REPLY o de tiempo de vida TTL superado, enviados por los cortafuegos 31 y 51 no impiden la comunicación.

El dispositivo de red de control doméstico 61 y la llave de red de control doméstico 42 llegan a un acuerdo entre ellos sobre los números de los ECHO ID y la frecuencia de envío, ventajosamente en primer lugar por medio de un servidor de red de control doméstico 21 independiente, y, tras el establecimiento de la conexión de transferencia de datos, directamente entre ellos en el comienzo de la carga útil de los paquetes de ICMP ECHO REPLY. En el inicio de los paquetes de ICMP REPLY, se notifican en cada paquete el ECHO REQUEST ID previo, enviado por el dispositivo respectivo, y la frecuencia de envío solicitada por el dispositivo para los paquetes de ECHO REQUEST. Así, los dos dispositivos conocen qué ECHO ID es necesario enviar en el siguiente paquete de ECHO REQUEST, y cuándo es necesario enviar el siguiente ECHO REQUEST. Si, por ejemplo, en el paquete de ECHO REPLY, la frecuencia de envío solicitada es 500 ms, el dispositivo envía su paquete de ECHO REQUEST siempre que el tiempo que va desde el momento del establecimiento de la conexión en milisegundos sea divisible por 500.

Ejemplos de establecimiento de un túnel de VPN usando un protocolo TCP, referencia 2064, en la disposición de la figura 1a:

Una conexión de retransmisión de TCP asistida funciona, en el sentido de la seguridad de los datos, de forma correspondiente a cualquier otra conexión, por ejemplo, una conexión de UDP directa normal entre dos dispositivos. La conexión de VPN no se abre con un servidor de retransmisión de TCP que se esté utilizando, sino que el cifrado tiene lugar en los dispositivos terminales que establecen la conexión. Una vulneración en el servidor de retransmisión de TCP no puede vulnerar la conexión de VPN establecida, y no se puede engañar a la llave de red de control doméstico según la invención para que se conecte a un dispositivo incorrecto.

Ejemplo de establecimiento de una conexión de retransmisión de TCP:

La dirección IP pública de la llave de red de control doméstico 42 es 5.5.5.5, la dirección IP pública del dispositivo de red de control doméstico 61 es 6.6.6.6, y la dirección IP pública del servidor de retransmisión de TCP (servidor de red de control doméstico 21) es 7.7.7.7.

La llave de red de control doméstico 42 realiza una conexión de TCP con la dirección 7.7.7.7, y con su puerto 443. El servidor de retransmisión de TCP ve la conexión solicitada y la acepta. Tiene lugar la señalización de entrada en

contacto de TCP, y se abre el canal de TCP. La llave de red de control doméstico 42 envía información exclusiva de la conexión por el canal de TCP (por ejemplo, ID de Conexión) al servidor de retransmisión de TCP.

El servidor de retransmisión de TCP recibe la información y, por medio de esto, puede enlazar posteriormente la conexión recibida con el dispositivo de red de control doméstico 61 correcto.

El dispositivo de red de control doméstico 61 realiza una conexión de TCP con la dirección 7.7.7.7, en el puerto 443. El servidor de retransmisión de TCP ve la conexión solicitada y la acepta. Tiene lugar la señalización de entrada en contacto de TCP, y se abre el canal de TCP. El dispositivo de red de control doméstico 61 envía información exclusiva de la conexión por el canal de TCP (por ejemplo, ID de Conexión) al servidor de retransmisión de TCP.

El servidor de retransmisión de TCP recibe la información y, por medio de esto, el servidor de retransmisión de TCP sabe posteriormente a qué llave de red de control doméstico 42 se va a conectar el dispositivo de red de control doméstico 61.

El servidor de retransmisión de TCP comienza a transmitir mensajes entre la llave de red de control doméstico 42 y el dispositivo de red de control doméstico 61 entre las conexiones de TCP. El servidor de retransmisión de TCP lee datos de la conexión de TCP proveniente de la llave de red de control doméstico 42, y transmite los datos, tal como están, a la conexión de TCP del dispositivo de red de control doméstico 61. Por consiguiente, el servidor de retransmisión de TCP lee datos de la conexión del dispositivo de red de control doméstico 61, y transmite los datos leídos, tal como están, a la conexión de TCP de la llave de red de control doméstico 42. Se continúa con la transmisión de datos de manera bidireccional hasta que se interrumpe la otra conexión de TCP. Cuando se interrumpe la otra conexión de TCP, el servidor de retransmisión de TCP interrumpe también la otra conexión de TCP.

La figura 4 muestra las partes principales funcionales del dispositivo de red de control doméstico 61 de acuerdo con la invención. El dispositivo de red de control doméstico 61 tiene una fuente de alimentación 621. Puede ser un acumulador o una fuente de alimentación con corriente de la red eléctrica. Todos los componentes eléctricos del dispositivo de red de control doméstico obtienen su voltaje de funcionamiento a partir de la fuente de alimentación 621.

El dispositivo de red de control doméstico 61 tiene uno o más procesadores 622. El procesador o medios de procesador pueden comprender una unidad lógica aritmética, un grupo de diferentes registros, y circuitos de control. Una disposición de almacenamiento de datos 623, tal como una unidad de memoria o medios de memoria, en donde se puede almacenar información legible por ordenador o programas o información de usuario, se ha conectado a los medios de procesador. Los medios de memoria 623 contienen típicamente unidades de memoria, que permiten funciones tanto de lectura como de escritura (Memoria de Acceso Aleatorio, RAM), y unidades de memoria que contienen memoria no volátil, desde la cual únicamente se pueden leer datos (Memoria de Solo Lectura, ROM). En los medios de memoria se almacenan ventajosamente el registro del dispositivo, certificados a utilizar en el establecimiento de la conexión de VPN, la información de ruta de red actual y todos los programas necesarios para el funcionamiento del dispositivo de red de control doméstico 61.

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

El dispositivo de red de control doméstico 61 también comprende elementos de interfaz, los cuales comprenden una entrada/salida o medios de entrada/salida 624, 625, 626, 627 y 628 para recibir o enviar información. La información recibida con los medios de entrada se transfiere para que sea procesada por los medios de procesador 622 del dispositivo de red de control doméstico 61. Los elementos de interfaz del dispositivo de red de control doméstico transfieren información o bien a la red de transferencia de datos o bien a dispositivos de procesado de datos externos. Los elementos de interfaz del dispositivo de red de control doméstico 61 son ventajosamente un puerto WAN 624, uno o más puertos LAN 625, un puerto de antena 626, un puerto USB 627 y un puerto de control 628. El emparejamiento del dispositivo de red de control doméstico 61 y la llave de red de control doméstico 42 o 41c se puede realizar ventajosamente, por ejemplo, por medio del puerto USB 627.

Resulta evidente para alguien versado en la materia, que las funciones del dispositivo de red de control doméstico 61 se pueden integrar como parte de un dispositivo computarizado o de ingeniería doméstica, el cual tenga una capacidad de procesador y de memoria suficiente, y medios de conexión para conectar al mismo diversos medios técnicos, o bien con una conexión de transferencia de datos por cable o bien con una conexión de transferencia de datos inalámbrica. Este dispositivo computarizado, en el cual están integradas las funciones del dispositivo de red doméstica de control, se conecta a alguna red de transferencia de datos 5, desde la cual se tiene acceso a la Internet pública.

La figura 5a muestra las partes principales funcionales de la llave de red de control doméstico 42 de acuerdo con la invención. El dispositivo de red de control doméstico 42 tiene una fuente de alimentación 421. Puede ser un acumulador o una fuente de alimentación con corriente de la red eléctrica. Todos los componentes eléctricos del dispositivo de red de control doméstico obtienen su voltaje de funcionamiento de la fuente de alimentación 421.

La llave de red de control doméstico 42 puede comprender uno o varios procesadores 422. El procesador o medios de procesador pueden comprender una unidad lógica aritmética, un grupo de diferentes registros, y circuitos de control. Una disposición de almacenamiento de datos 423, tal como una unidad de memoria o medios de memoria, en donde se puede almacenar información legible por ordenador o programas o información de usuario, se ha conectado a los medios de procesador. Los medios de memoria 423 contienen típicamente unidades de memoria, que permiten funciones tanto de lectura como de escritura (Memoria de Acceso Aleatorio, RAM), y unidades de memoria que contienen memoria no volátil, desde la cual únicamente se pueden leer datos (Memoria de Solo Lectura, ROM). Los certificados a utilizar en el establecimiento de la conexión de VPN, la información de ruta de red actual, y todos los programas necesarios para el funcionamiento del dispositivo de red de control doméstico 42 se almacenan ventajosamente en los medios de memoria.

Algunos ejemplos de programas almacenados en la memoria de la llave de red de control doméstico 42 son un sistema operativo (por ejemplo, Linux), programas de TCP/IP, un programa de VPN (por ejemplo, OpenVPN), un programa de servidor/dispositivo de cliente de DHCP (por ejemplo, ISC DHCP), un programa de servidor de DNS (por ejemplo, dnsmasq), un programa de base de datos (por ejemplo, SQLite), un programa de control remoto (por ejemplo, OpenSSH), un programa de confirmación/gestión de certificados (por ejemplo, GPG) y una biblioteca de interfaz de usuario (por ejemplo, LuCI).

La llave de red de control doméstico 42 también comprende elementos de interfaz, los cuales comprenden una entrada/salida o medios de entrada/salida 424, 425, 426, 427 y 428 para recibir o enviar información. La información recibida con los medios de entrada se transfiere para que sea procesada por los medios de procesador 422 de la llave de red de control doméstico 42. Los elementos de interfaz del dispositivo de red de control doméstico transfieren información o bien a la red de transferencia de datos o bien a dispositivos de procesado de datos externos. Los elementos de interfaz del dispositivo de red de control doméstico 42 son ventajosamente un puerto WAN 424, un puerto o puertos LAN 425, un puerto de antena 426, un puerto USB 427 y un puerto de control 428.

La figura 5b muestra las partes principales funcionales de una llave de red de control doméstico 42b de acuerdo con una segunda forma de realización de la invención. La llave de red de control doméstico 42b según esta forma de realización puede comprender uno o varios criptoprocesadores 422b. El procesador o medios de procesador pueden comprender una unidad lógica aritmética, un grupo de diferentes registros y circuitos de control. Un criptoprocesador 422b comprende ventajosamente una unidad de memoria interna, en la cual se ha almacenado una clave criptográfica privada individual.

Una disposición de almacenamiento de datos 423b, tal como una unidad de memoria *Flash* o medios de memoria, en donde se puede almacenar información legible por ordenador o programas o información de usuario, se ha conectado a los medios de procesador. Los medios de memoria 423b contienen típicamente unidades de memoria, que permiten funciones tanto de lectura como de escritura (Memoria de Acceso Aleatorio, RAM), y unidades de memoria que contienen memoria no volátil, desde la cual únicamente se pueden leer datos (Memoria de Solo Lectura, ROM). La información de identificación de la llave de red de control doméstico 42b, su ruta de red actual, los certificados a utilizar en el establecimiento de la conexión de VPN, la información de ruta de red actual, la información de identificación del dispositivo de red de control doméstico 61 que funciona como sus pares de dispositivo y todos los programas necesarios para el funcionamiento de la llave de red de control doméstico 42b se almacenan ventajosamente en los medios de memoria.

Algunos ejemplos de programas almacenados en la memoria de la llave de red de control doméstico 42b son un sistema operativo (por ejemplo, Linux), programas de TCP/IP, un programa de VPN (por ejemplo, OpenVPN), un programa de servidor/dispositivo de cliente de DHCP (por ejemplo, ISC DHCP), un programa de base de datos (por ejemplo, SQLite), un programa de confirmación/gestión de certificados (por ejemplo, GPG) y una biblioteca de interfaz de usuario (por ejemplo, LuCI).

La llave de red de control doméstico 42 comprende también elementos de interfaz, los cuales comprenden una entrada/salida o medios de entrada/salida 426b para recibir o enviar información. La información recibida con los medios de entrada se transfiere para que sea procesada por los medios de procesador 422b de la llave de red de control doméstico 42b. Los elementos de interfaz del dispositivo de red de control doméstico se usan ventajosamente para transferir información desde la memoria 423b de la llave de red doméstica de control, o bien a un dispositivo de procesado de datos externo 41c o bien al dispositivo de red de control doméstico 61. De forma correspondiente, se puede recibir información u órdenes, por medio de los elementos de interfaz, por ejemplo, desde el dispositivo de procesado de datos, al cual está conectada la llave de red de control doméstico 42b.

Con respecto a sus niveles de derechos de acceso, existen por lo menos dos niveles para las llaves de red

doméstica de control 42 ó 42b antes descritas, por ejemplo dispositivos de llave de nivel administrador y de nivel usuario básico. Un usuario/propietario de un dispositivo de llave con un nivel de derechos de acceso superior (por ejemplo, un administrador) tiene derecho de control sobre todos los objetivos de control de usuarios de llaves de red doméstica de control de un nivel inferior (tales como usuarios básicos). Por otro lado, un propietario de un dispositivo de llave con un nivel de derechos de acceso inferior no tiene acceso a ningún otro objetivo de control de nivel superior de derechos de acceso que no sea sus propios objetivos.

La figura 6 muestra las partes principales funcionales del servidor de red de control doméstico 21. El servidor de red de control doméstico 21 funciona ventajosamente también como servidor de retransmisión de TCP. El servidor de red de control doméstico 21 comprende una fuente de alimentación 611. Puede ser un acumulador o una fuente de alimentación con corriente de la red eléctrica. Todos los componentes eléctricos del servidor de red de control doméstico 21 obtienen su voltaje de funcionamiento de la fuente de alimentación 611.

El servidor de red de control doméstico 21 tiene uno o más procesadores 212. El procesador o medios de procesador pueden comprender una unidad lógica aritmética, un grupo de diferentes registros, y circuitos de control. Una disposición de almacenamiento de datos 613, tal como una unidad de memoria o medios de memoria, en donde se puede almacenar información legible por ordenador o programas o información de usuario, se ha conectado a los medios de procesador. Los medios de memoria 613 contienen típicamente unidades de memoria, que permiten funciones tanto de lectura como de escritura (Memoria de Acceso Aleatorio, RAM), y unidades de memoria que contienen memoria no volátil, desde la cual únicamente se pueden leer datos (Memoria de Solo Lectura, ROM). La información de identificación de los pares de los dispositivos en el sistema de control remoto (registro Tosibox), la información de ruta de red actual de cada par de dispositivo, todos los programas necesarios para establecer la conexión de transferencia de datos de VPN que se establecerá entre los pares de dispositivos y la base de datos Tosibox se almacenan ventajosamente en los medios de memoria.

Algunos ejemplos de programas almacenados en la memoria del servidor de red de control doméstico 21 son un sistema operativo (por ejemplo, Linux), programas de TCP/IP, un programa de servidor/dispositivo de cliente de DHCP (por ejemplo, ISC DHCP), un programa de servidor de DNS (por ejemplo, *bind*) un programa de base de datos (por ejemplo, SQLite), un programa de confirmación/gestión de certificados (por ejemplo, GPG) y una biblioteca de interfaz de usuario (por ejemplo, LuCI).

El servidor de red de control doméstico 21 también comprende elementos de interfaz, los cuales comprenden una entrada/salida o medios de entrada/salida 614 para recibir o enviar información. La información recibida con los medios de entrada se transfiere para que sea procesada por los medios de procesador 612 del dispositivo de red de control doméstico 21. Los elementos de interfaz del servidor de red de control doméstico transfieren información o bien a la red de transferencia de datos o bien a dispositivos de procesado de datos externos. El elemento de interfaz del servidor de red de control doméstico 21 es ventajosamente un puerto WAN 614.

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

La figura 7 muestra las capas de enlace de datos (capas de Tosibox) utilizadas en la transferencia de datos entre el dispositivo de red de control doméstico 61, la llave de red de control doméstico 42, 42b y el servidor de red de control doméstico 21.

La capa física de Tosibox comprende alternativas para establecer una conexión física de transferencia de datos entre dos dispositivos que participan en el control remoto. Puede establecerse una conexión de transferencia de datos, por ejemplo, acoplando los dispositivos por sus puertos de Ethernet a la red Ethernet local, que tiene conexión con Internet. Alternativamente, la conexión de transferencia de datos se puede establecer en la red WLAN local, desde la cual se tiene conexión con Internet. La tercera alternativa consiste en formar una conexión de transferencia de datos 2G ó 3G. En esta forma de realización, un dispositivo terminal que establece una conexión 2G ó 3G se conecta al puerto USB del dispositivo de red de control doméstico y/o a la llave de red doméstica de control.

La capa de enlace de datos de Tosibox comprende procedimientos de establecimiento de conexión que se pueden utilizar en una conexión de transferencia de datos por paquetes junto con la VPN. Procedimientos alternativos o paralelos de establecimiento de conexiones incluyen una conexión directa de transferencia de datos de TCP entre los miembros, una conexión directa de transferencia de datos de UDP entre los miembros, una conexión de transferencia de datos establecida mediante el uso de escaneo de puertos, una conexión de transferencia de datos basada en mensajes ICMP ECHO entre los miembros, o una conexión de transferencia de datos con retransmisión, establecida a través del servidor de red de control doméstico (miembro de retransmisión del TCP).

La capa de cifrado de VPN comprende los procedimientos de cifrado (clave criptográfica privada, individual, y una clave criptográfica pública de la llave de red doméstica de control) conocidos por el dispositivo de red de control doméstico 61, y los procedimientos de cifrado (clave criptográfica privada, individual, y la clave pública del

dispositivo de red doméstica de control) conocidos por la llave de red de control doméstico 42, 42b. Con estos procedimientos de cifrado, el dispositivo de red de control doméstico 61 y la llave de red de control doméstico 42, 42b pueden establecer una conexión segura de transferencia de datos de VPN usando un procedimiento de cifrado PKI (Infraestructura de Clave Pública).

Anteriormente se han descrito algunos procedimientos utilizados en el establecimiento de la conexión de transferencia de datos de VPN del sistema de control remoto según la invención. Además, se han descrito formas de realización ventajosas de componentes que implementan estos procedimientos en el sistema de control remoto. La invención no se limita a las soluciones antes descritas, sino que la idea de la misma se puede aplicar de múltiples maneras dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Método para proporcionar una red privada virtual (55, VPN) entre una llave de red de control doméstico (42, 42b) y un dispositivo de red de control doméstico (61) de los accionadores del sistema de control remoto en una propiedad, que comprende:

- tanto la llave de red de control doméstico (42, 42b) como el dispositivo de red de control doméstico (61) que forman un par predeterminado de terminales de red, a cuyos miembros se les permite comunicarse solamente entre sí y con un servidor de red de control doméstico (21), envían ocasionalmente una interrogación de sondeo al servidor de red de control doméstico (21), en la cual se le pregunta si el otro dispositivo del par de terminales de red está conectado a la red de transferencia de datos, y si es el caso, entonces

- tanto la llave de red de control doméstico (42, 42b) como el dispositivo de red de control doméstico (61) realizan una conexión (201) con el servidor de red de control doméstico (21), con el fin de establecer una red privada virtual y de solicitar (204) del servidor de red de control doméstico (21) la información de encaminamiento, con el fin de establecer una conexión de transferencia de datos de extremo-a-extremo entre dicho par de terminales de red;

- el servidor de red de control doméstico (21) comprueba si tanto la llave de red de control doméstico (42, 42b) como el dispositivo de red de control doméstico (61) son el par predeterminado de terminales de red; y

- el servidor de red de control doméstico (21) envía (205) tanto a la llave de red de control doméstico (42, 42b) como al dispositivo de red de control doméstico (61), la información de encaminamiento solicitada (205) si el servidor de red de control doméstico (21) ha comprobado que la llave de red de control doméstico (42, 42b) y el dispositivo de red de control doméstico (61) son el par predeterminado de terminales de red,

en el que la llave de red de control doméstico (42, 42b) y el dispositivo de red de control doméstico (61) dan inicio, con varios métodos conocidos de establecimiento de una red privada virtual, a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual (55).

2. Método de control remoto según la reivindicación 1, en el que la red privada virtual se establece como una conexión directa de transferencia de datos de TCP entre los terminales de red (2060, 2060a), como una conexión directa de transferencia de datos de UDP entre los terminales de red (2061, 2061a), usando un escaneo de puertos de UDP entre los terminales de red (2062, 2062a), utilizando unos mensajes ICMP ECHO del protocolo de control de IP (2063, 2063a), o con una conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21).

3. Método según la reivindicación 2, en el que se libera por lo menos la conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21), si la red privada virtual (55) se ha establecido también con otro método de establecimiento de una red privada virtual.

4. Llave de red de control doméstico (42, 42b) para accionadores en una propiedad, que comprende:

- unos elementos de interfaz de red, que comprenden unos medios de entrada/salida (424, 425, 426, 426b, 427, 428) para unas interfaces de red (3, 4);

- un procesador (422, 422b), y

- una memoria (423, 423b), que contiene un código de programa de ordenador, estando el procesador, la memoria y el código de programa de ordenador almacenado en la misma configurados para:

  - enviar ocasionalmente una interrogación de sondeo a un servidor de red de control doméstico (21), en la cual se le pregunta si un dispositivo de red de control doméstico (61) que se ha predeterminado para ser un par de terminales de red de la llave de red de control doméstico (42, 42b), de manera que la llave de red de control doméstico (42, 42b) solamente tiene permiso para comunicarse con dicho dispositivo de red doméstica de control, esté conectado a la red de transferencia de datos, y si es el caso, entonces

  - realizar una conexión (201) con el servidor de red de control doméstico (21) y solicitar (204) del servidor de red de control doméstico (21) la información de encaminamiento del dispositivo de red de control doméstico (61), con el fin de establecer una red privada virtual con el dispositivo de red de control doméstico (61)

  - recibir del servidor de red de control doméstico (21) la información de encaminamiento del dispositivo de red de control doméstico (61), si el servidor de red de control doméstico (21) comprueba que la llave de

red de control doméstico (42, 42b) y el dispositivo de red de control doméstico (61) son el par predeterminado de terminales de red,

en el que el procesador, la memoria y el código de programa de ordenador almacenado en la misma están configurados además para dar inicio con varios métodos conocidos de establecimiento de una red privada virtual a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual (55) con el dispositivo de red de control doméstico (61).

5. Llave de red de control doméstico según la reivindicación 4, configurada además para establecer una red privada virtual como una conexión directa de transferencia de datos de TCP (2060, 2060a) con el dispositivo de red de control doméstico (61), como una conexión directa de transferencia de datos de UDP (2061, 2061a) con el dispositivo de red de control doméstico (61), usando un escaneo de puertos de UDP (2062, 2062a) con el dispositivo de red de control doméstico (61), utilizando unos mensajes ICMP ECHO del protocolo de control de IP (2063, 2063a) con el dispositivo de red de control doméstico (61) o para establecer una conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21) con el dispositivo de red de control doméstico (61).

6. Llave de red de control doméstico según la reivindicación 5, configurada además para liberar por lo menos la conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21) si la red privada virtual (55) se ha establecido también con otro método de establecimiento de una red privada virtual.

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

- unos elementos de interfaz de red, que comprenden unos medios de entrada/salida (624, 625, 626, 627, 628) para la interfaz de red (5);

- un procesador (622), y

- una memoria (623), que contiene un código de programa de ordenador, estando el procesador, la memoria y el código de programa de ordenador almacenado en la misma configurados para:

  - enviar ocasionalmente una interrogación de sondeo a un servidor de red de control doméstico (21), en la cual se le pregunta si una llave de red de control doméstico (42, 42b) que se ha predeterminado para ser un par de terminales de red del dispositivo de red de control doméstico (61), de manera que el dispositivo de red de control doméstico (61) solamente tiene permiso para comunicarse con dicha llave de red doméstica de control, está conectada a la red de transferencia de datos, y si es el caso;

  - realizar una conexión (201) con el servidor de red de control doméstico (21) y solicitar (204) del servidor de red de control doméstico (21) la información de encaminamiento de la llave de red de control doméstico (42, 42b), con el fin de establecer una red privada virtual con la llave de red de control doméstico (42, 42b)

  - recibir la información de encaminamiento de la llave de red de control doméstico (42, 42b) del servidor de red de control doméstico (21), si el servidor de red de control doméstico (21) comprueba que la llave de red de control doméstico (42, 42b) y el dispositivo de red de control doméstico (61) son el par predeterminado de terminales de red,

en el que el procesador, la memoria y el código de programa de ordenador almacenado en la misma están configurados además para dar inicio con varios métodos conocidos de establecimiento de una red privada virtual a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual (55) con la llave de red de control doméstico (42, 42b).

8. Dispositivo de red de control doméstico según la reivindicación 7, configurado además para establecer una red privada virtual como una conexión directa de transferencia de datos de TCP (2060, 2060a) con la llave de red de control doméstico (42, 42b), como una conexión directa de transferencia de datos de UDP (2061, 2061a) con la llave de red de control doméstico (42, 42b), usando un escaneo de puertos de UDP (2062, 2062a) con la llave de red de control doméstico (42, 42b), utilizando unos mensajes ICMP ECHO del protocolo de control de IP (2063, 2063a) con la llave de red de control doméstico (42, 42b) o para establecer una conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21) con la llave de red de control doméstico (42, 42b).

9. Dispositivo de red de control doméstico según la reivindicación 8, configurado además para liberar por lo menos la conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21), si la red privada virtual (55) se ha establecido también con otro método de establecimiento de una red privada virtual.

10. Servidor de red de control doméstico (21), que comprende:

- unos elementos de interfaz de red, que comprenden unos medios de entrada/salida (614);
- un procesador (612), y
- una memoria (613), que contiene un código de programa de ordenador,
- estando la memoria y el código de programa de ordenador almacenado en la misma configurados para:
  - almacenar en la memoria (613) del servidor de red de control doméstico (21) una información de identificación de un par de terminales de red formado por una llave de red de control doméstico (42, 42b) y un dispositivo de red de control doméstico (61) usados para el control remoto de una propiedad;
  - recibir del par de terminales de red la información de ruta de red determinada por ellos;
  - recibir de la llave de red de control doméstico (42, 42a) la solicitud de información de encaminamiento de su par de terminales de red;
  - comprobar cuál es el dispositivo de red de control doméstico (61) que funciona como el par de terminales de red predeterminado de la llave de red de control doméstico (42, 42b) que realizó la solicitud de información de encaminamiento, y que a la llave de red de control doméstico (42, 42a) se le permite comunicarse solamente con el mismo, basándose en la información de identificación del par de terminales de red almacenada en la memoria (613) del servidor de red de control doméstico (21), y
  - enviar la información de encaminamiento del par de terminales de red tanto a la llave de red de control doméstico (42, 42a) como al dispositivo de red de control doméstico (61), si tanto la llave de red de control doméstico (42, 42a) como el dispositivo de red de control doméstico (61) están conectados a la red de transferencia de datos y si se comprueba que la llave de red de control doméstico (42, 42a) y el dispositivo de red de control doméstico (61) son el par de terminales de red predeterminado,

  configurados además para:

  - enviar información que indica una parte libre de un ciberespacio al dispositivo de red de control doméstico (61), y
  - liberar la conexión de transferencia de datos para el par de terminales de red cuando se ha establecido satisfactoriamente por lo menos una red privada virtual directa (55) entre el par de terminales de red.

11. Producto de programa de ordenador que comprende unos medios de código de programa de ordenador adaptados para llevar a cabo las siguientes etapas de código de programa cuando dicho programa se ejecuta en un ordenador, con el fin de proporcionar unas funciones de llave de red doméstica de control, que comprende:

- unos medios de código para determinar la información de encaminamiento desde una llave de red de control doméstico (42, 42b) a Internet (2);
- unos medios de código para enviar ocasionalmente una interrogación de sondeo a un servidor de red de control doméstico (21), en la cual se le pregunta si un dispositivo de control doméstico (61) con el cual la llave de red de control doméstico (42, 42a) forma un par predeterminado de terminales de red, y a cuyos miembros se les permite comunicarse únicamente entre sí, está conectado a la red de transferencia de datos, y si es el caso, entonces;
- unos medios de código para realizar una conexión (201) con el servidor de red de control doméstico (21) y para solicitar (204) del servidor de red de control doméstico (21) la información de encaminamiento del dispositivo de red de control doméstico (61), con el fin de establecer una red privada virtual con el dispositivo de red de control doméstico (61);
- unos medios de código para recibir del servidor de red de control doméstico (21) la información de encaminamiento del dispositivo de red de control doméstico (61), si el servidor de red de control doméstico (21) comprueba que la llave de red de control doméstico (42, 42b) y el dispositivo de red de control doméstico (61) son el par predeterminado de terminales de red,

en el que el programa de ordenador además comprende unos medios de código para dar inicio con varios métodos conocidos de establecimiento de una red privada virtual a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual (55)

con el dispositivo de red de control doméstico (61).

12. Producto de programa de ordenador según la reivindicación 11, que además comprende unos medios de código que están configurados para establecer una red privada virtual como una conexión directa de transferencia de datos de TCP (2060, 2060a) con el dispositivo de red de control doméstico (61), como una conexión directa de transferencia de datos de UDP (2061, 2061a) con el dispositivo de red de control doméstico (61), usando un escaneo de puertos de UDP (2062, 2062a) con el dispositivo de red de control doméstico (61), utilizando unos mensajes ICMP ECHO del protocolo de control de IP (2063, 2063a) con el dispositivo de red de control doméstico (61) o para establecer una conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21) con el dispositivo de red de control doméstico (61).

13. Producto de programa de ordenador según la reivindicación 12, que comprende unos medios de código que están configurados para liberar por lo menos la conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21), si la red privada virtual (55) se ha establecido también con otro método de establecimiento de una red privada virtual.

14. Programa de ordenador que comprende unos medios de código de programa de ordenador adaptados para llevar a cabo las siguientes etapas de código de programa cuando dicho programa se ejecuta en un ordenador para proporcionar funciones de dispositivo de red doméstica de control, que comprende:

- unos medios de código para determinar la información de encaminamiento desde un dispositivo de red de control doméstico (61) a Internet (2);

- unos medios de código para enviar ocasionalmente una interrogación de sondeo a un servidor de red de control doméstico (21), en la cual se le pregunta si una llave de control doméstico (42, 42b) con la cual el dispositivo de red de control doméstico (61) forma un par predeterminado de terminales, y a cuyos miembros se les permite comunicarse únicamente entre sí, está conectada a la red de transferencia de datos, y si es el caso, entonces;

- unos medios de código para realizar una conexión (201) con el servidor de red de control doméstico (21) y para solicitar (204) del servidor de red de control doméstico (21) la información de encaminamiento de la llave de red de control doméstico (42, 42b), con el fin de establecer una red privada virtual con la llave de red de control doméstico (42, 42b);

- unos medios de código para recibir del servidor de red de control doméstico (21) la información de encaminamiento de la llave de red de control doméstico (42, 42b), si el servidor de red de control doméstico (21) comprueba que la llave de red de control doméstico (42, 42b) y el dispositivo de red de control doméstico (61) son el par predeterminado de terminales de red,

en el que el programa de ordenador además comprende unos medios de código para dar inicio con varios métodos conocidos de establecimiento de una red privada virtual a un proceso de establecimiento de una conexión de transferencia de datos de extremo-a-extremo, con el fin de proporcionar por lo menos una red privada virtual (55) con la llave de red de control doméstico (42, 42b).

15. Producto de programa de ordenador según la reivindicación 14, que además comprende unos medios de código que están configurados para establecer una red privada virtual como una conexión directa de transferencia de datos de TCP (2060, 2060a) con la llave de red de control doméstico (42, 42b), como una conexión directa de transferencia de datos de UDP (2061, 2061a) con la llave de red de control doméstico (42, 42b), usando un escaneo de puertos de UDP (2062, 2062a) con la llave de red de control doméstico (42, 42b), utilizando unos mensajes ICMP ECHO del protocolo de control de IP (2063, 2063a) con la llave de red de control doméstico (42, 42b) o para establecer una conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21) con la llave de red de control doméstico (42, 42b).

16. Producto de programa de ordenador según la reivindicación 15, que comprende unos medios de código que están configurados además para liberar por lo menos la conexión de transferencia de datos de TCP (2064, 2064a) retransmitida por medio del servidor de red de control doméstico (21), si la red privada virtual (55) se ha establecido también con otro método de establecimiento de una red privada virtual.

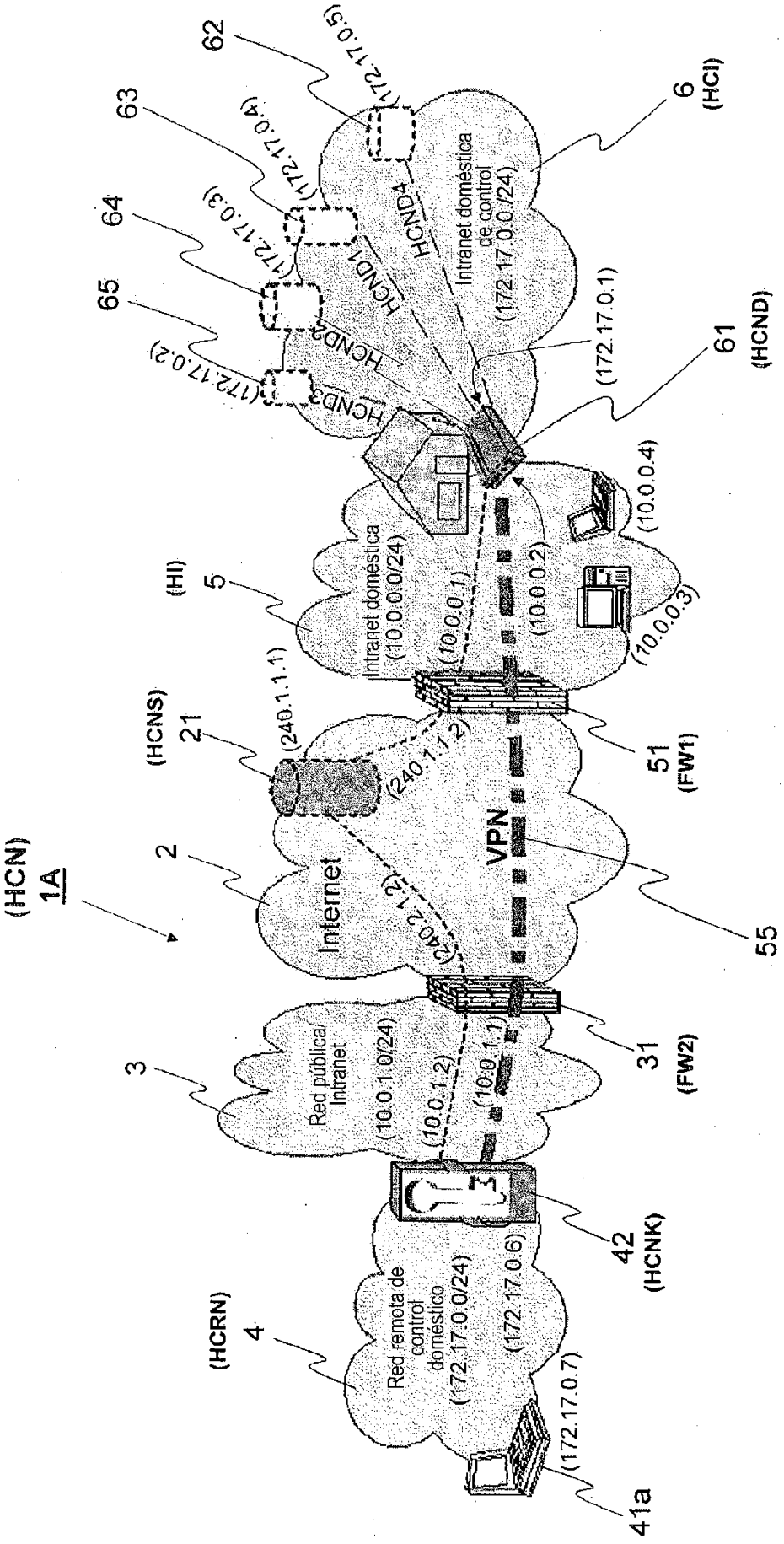

(HCN)
1A
2
Internet
(240.1.1.2)
(240.1.1.1)
(HCNS)
21
VPN
55
3
Red pública Intranet
(10.0.1.0/24)
(10.0.1.2)
(10.0.1.1)
31
(FW2)
42
(HCNK)
4
(HCRN)
Red remota de control doméstico
(172.17.0.0/24)
(172.17.0.6)
(172.17.0.7)
41a
5
(HI)
Intranet doméstica
(10.0.0.0/24)
(10.0.0.1)
(10.0.0.2)
(10.0.0.3)
(10.0.0.4)
51
(FW1)
61
(HCND)
(172.17.0.1)
6
(HCI)
Intranet doméstica de control
(172.17.0.0/24)
HCND4
HCND1
HCND2
HCND3
62
63
64
65
(172.17.0.5)
(172.17.0.4)
(172.17.0.3)
(172.17.0.2)

Fig. 1a

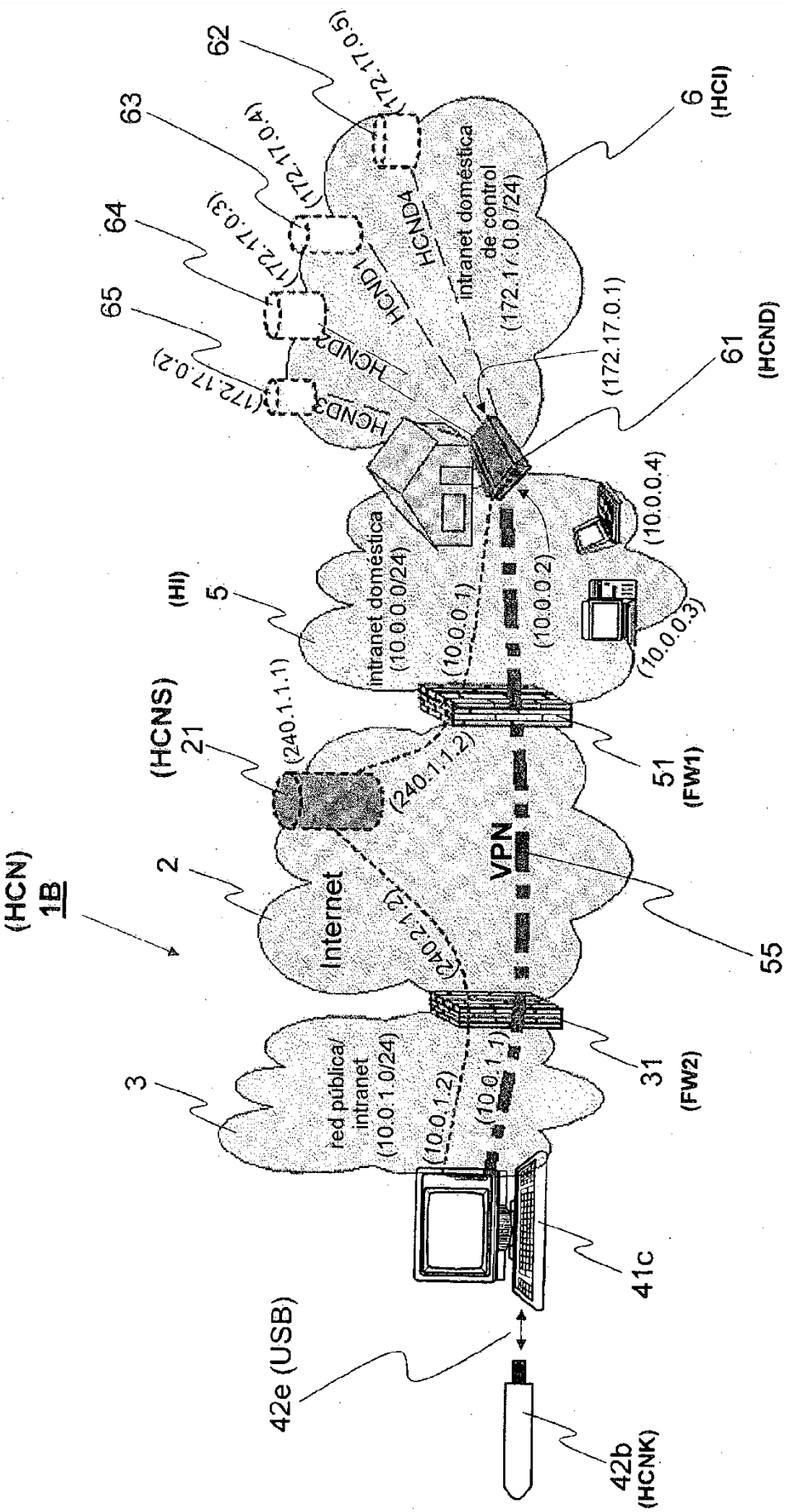
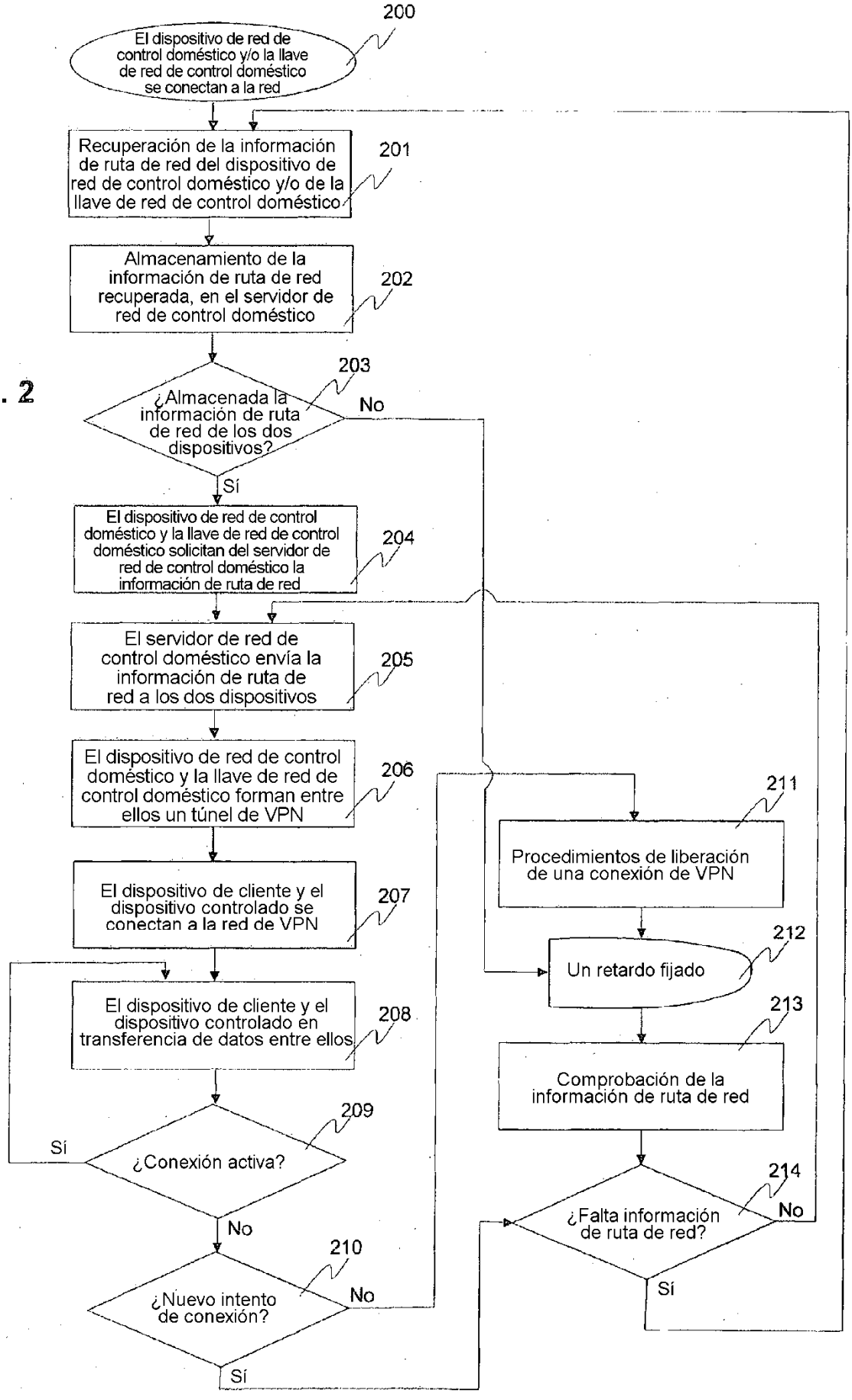

(HCN)
1B
2
Internet
3
red pública/
intranet
(10.0.1.0/24)
(10.0.1.2)
(10.0.1.1)
31
(FW2)
55
VPN
(HCNS)
21
(240.1.1.1)
(240.1.1.2)
(240.1.2.1)
(240.1.2.2)
5
(HI)
intranet doméstica
(10.0.0.0/24)
(10.0.0.1)
(10.0.0.2)
(10.0.0.3)
(10.0.0.4)
51
(FW1)
61
(HCND)
(172.17.0.1)
6
(HCI)
intranet doméstica
de control
(172.17.0.0/24)
HCND4
HCND1
HCND2
HCND3
62
63
64
65
(172.17.0.5)
(172.17.0.4)
(172.17.0.3)
(172.17.0.2)
41c
42e (USB)
42b
(HCNK)

Fig. 1b

Fig. 2


200
El dispositivo de red de control doméstico y/o la llave de red de control doméstico se conectan a la red
Recuperación de la información de ruta de red del dispositivo de red de control doméstico y/o de la llave de red de control doméstico
201
Almacenamiento de la información de ruta de red recuperada, en el servidor de red de control doméstico
202
¿Almacenada la información de ruta de red de los dos dispositivos?
203
No
Sí
El dispositivo de red de control doméstico y la llave de red de control doméstico solicitan del servidor de red de control doméstico la información de ruta de red
204
El servidor de red de control doméstico envía la información de ruta de red a los dos dispositivos
205
El dispositivo de red de control doméstico y la llave de red de control doméstico forman entre ellos un túnel de VPN
206
El dispositivo de cliente y el dispositivo controlado se conectan a la red de VPN
207
El dispositivo de cliente y el dispositivo controlado en transferencia de datos entre ellos
208
¿Conexión activa?
209
Sí
No
¿Nuevo intento de conexión?
210
No
Sí
Procedimientos de liberación de una conexión de VPN
211
Un retardo fijado
212
Comprobación de la información de ruta de red
213
¿Falta información de ruta de red?
214
No
Sí

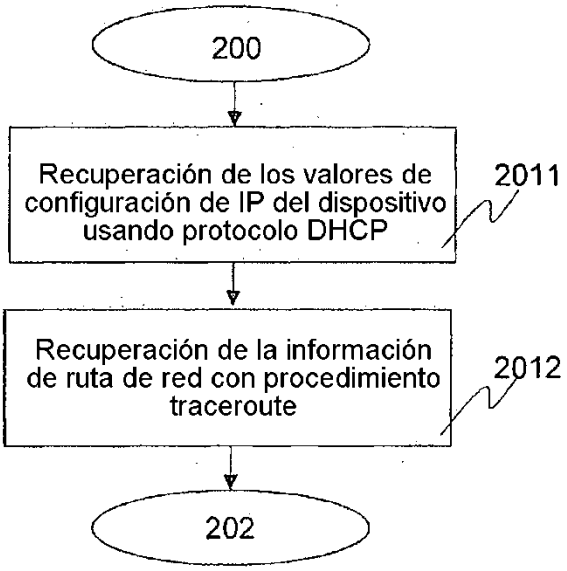

200
Recuperación de los valores de configuración de IP del dispositivo usando protocolo DHCP
2011
Recuperación de la información de ruta de red con procedimiento traceroute
2012
202

Fig. 3a

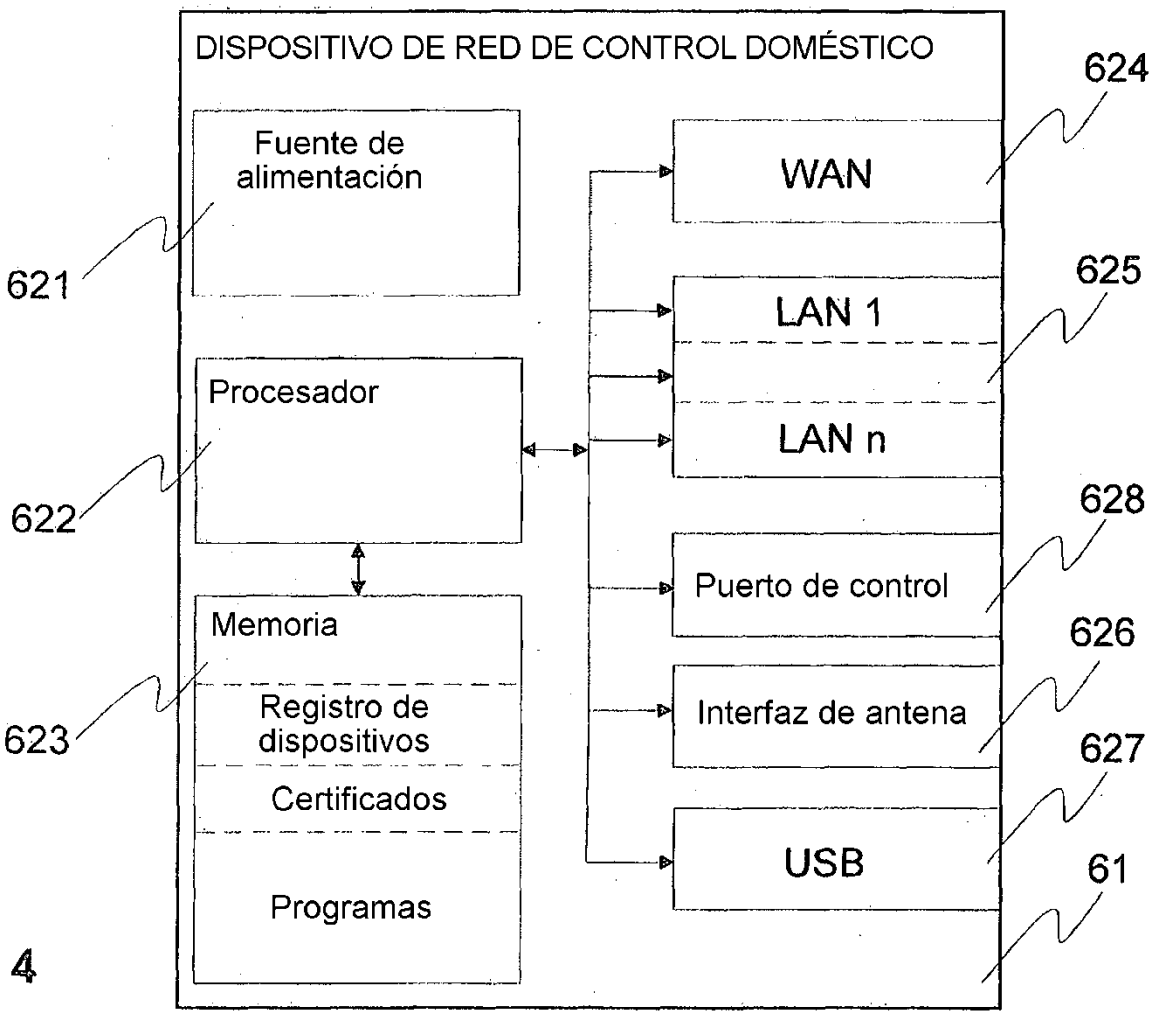

DISPOSITIVO DE RED DE CONTROL DOMÉSTICO
624
Fuente de alimentación
621
WAN
625
LAN 1
LAN n
Procesador
622
628
Puerto de control
626
Interfaz de antena
Memoria
623
Registro de dispositivos
Certificados
627
USB
Programas
61

Fig. 4

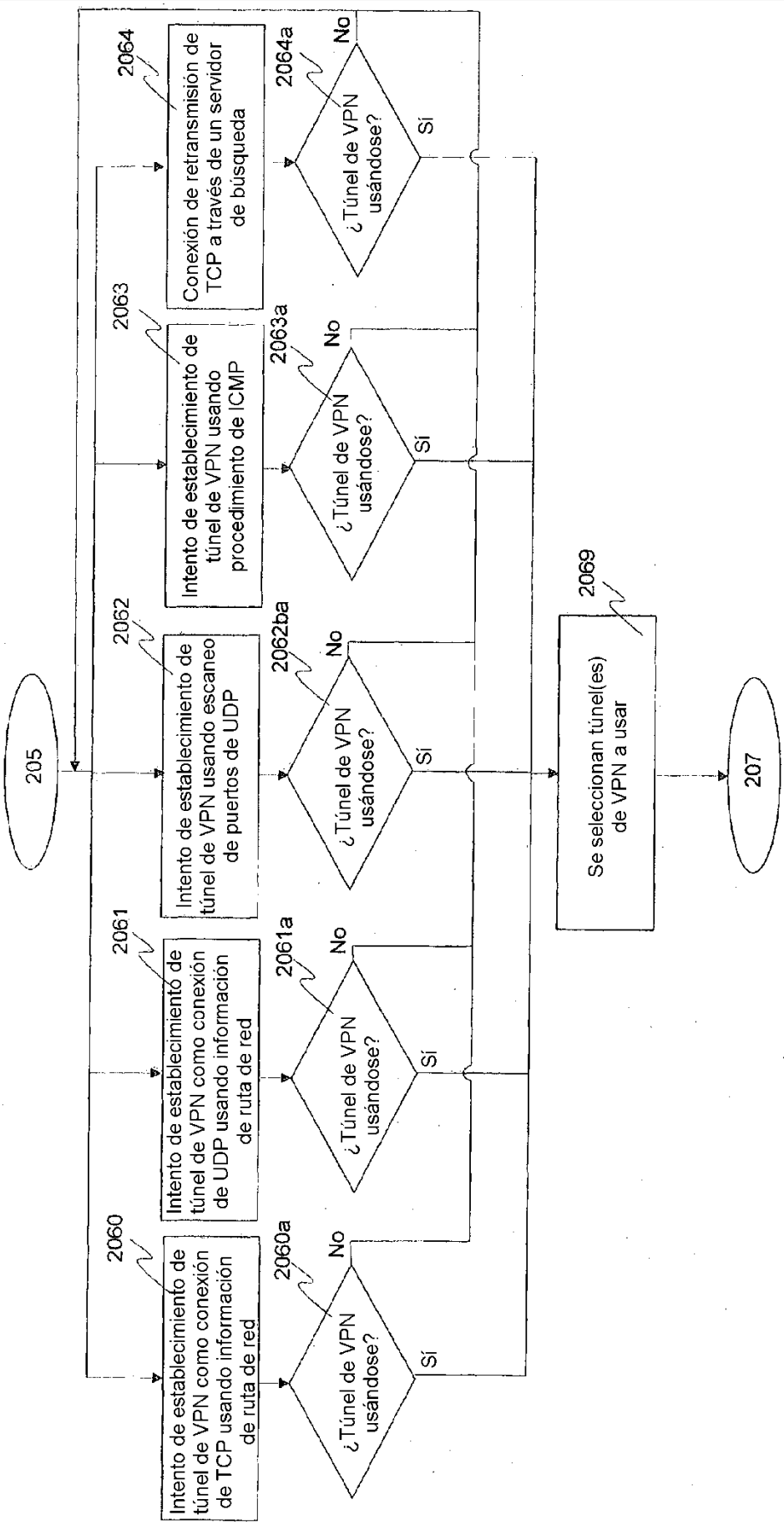

205
2060
Intento de establecimiento de túnel de VPN como conexión de TCP usando información de ruta de red
2060a
¿Túnel de VPN usándose?
No
Sí
2061
Intento de establecimiento de túnel de VPN como conexión de UDP usando información de ruta de red
2061a
¿Túnel de VPN usándose?
No
Sí
2062
Intento de establecimiento de túnel de VPN usando escaneo de puertos de UDP
2062ba
¿Túnel de VPN usándose?
No
Sí
2063
Intento de establecimiento de túnel de VPN usando procedimiento de ICMP
2063a
¿Túnel de VPN usándose?
No
Sí
2064
Conexión de retransmisión de TCP a través de un servidor de búsqueda
2064a
¿Túnel de VPN usándose?
No
Sí
2069
Se seleccionan túnel(es) de VPN a usar
207

Fig. 3b

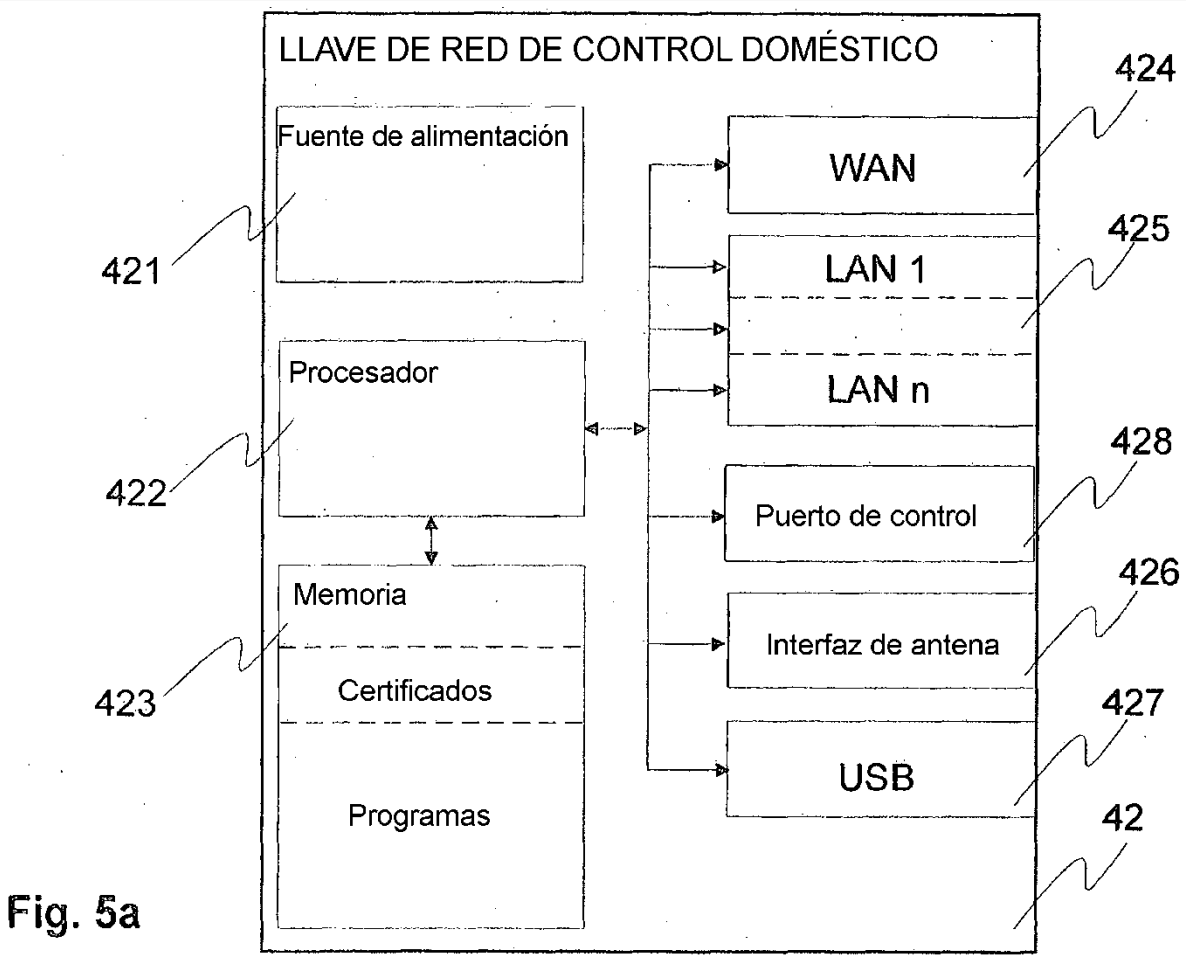

LLAVE DE RED DE CONTROL DOMÉSTICO
Fuente de alimentación
421
Procesador
422
Memoria
423
Certificados
Programas
WAN
424
LAN 1
425
LAN n
Puerto de control
428
Interfaz de antena
426
USB
427
42

Fig. 5a

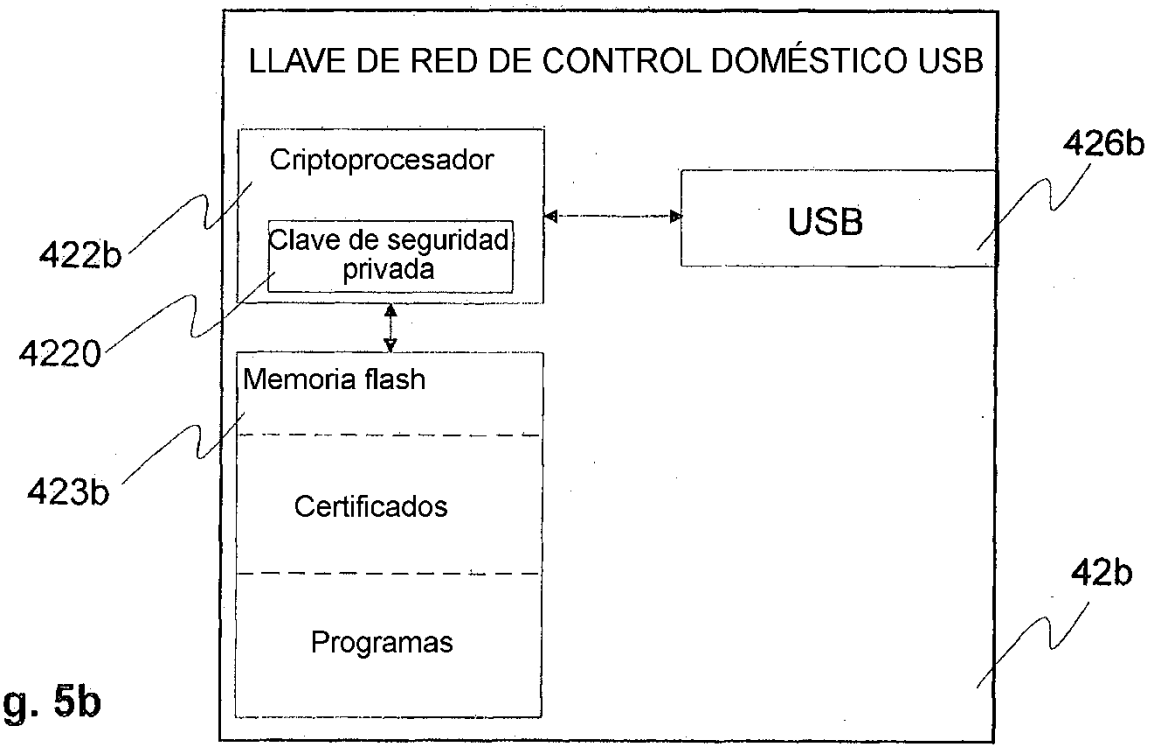

LLAVE DE RED DE CONTROL DOMÉSTICO USB
Criptoprocesador
422b
Clave de seguridad privada
4220
Memoria flash
423b
Certificados
Programas
USB
426b
42b

Fig. 5b

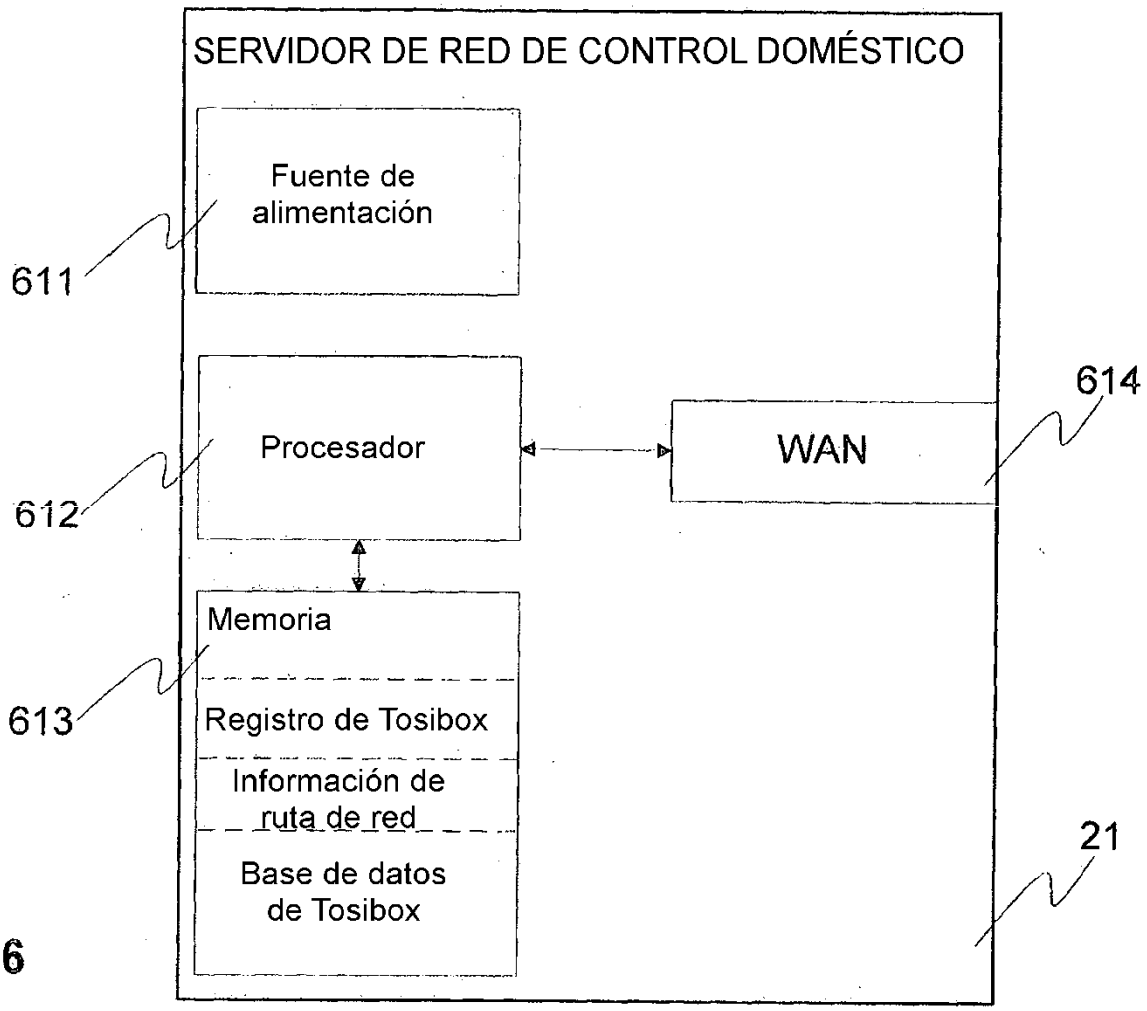

SERVIDOR DE RED DE CONTROL DOMÉSTICO
Fuente de alimentación
611
Procesador
612
WAN
614
Memoria
613
Registro de Tosibox
Información de ruta de red
Base de datos de Tosibox
21
X

Fig. 6

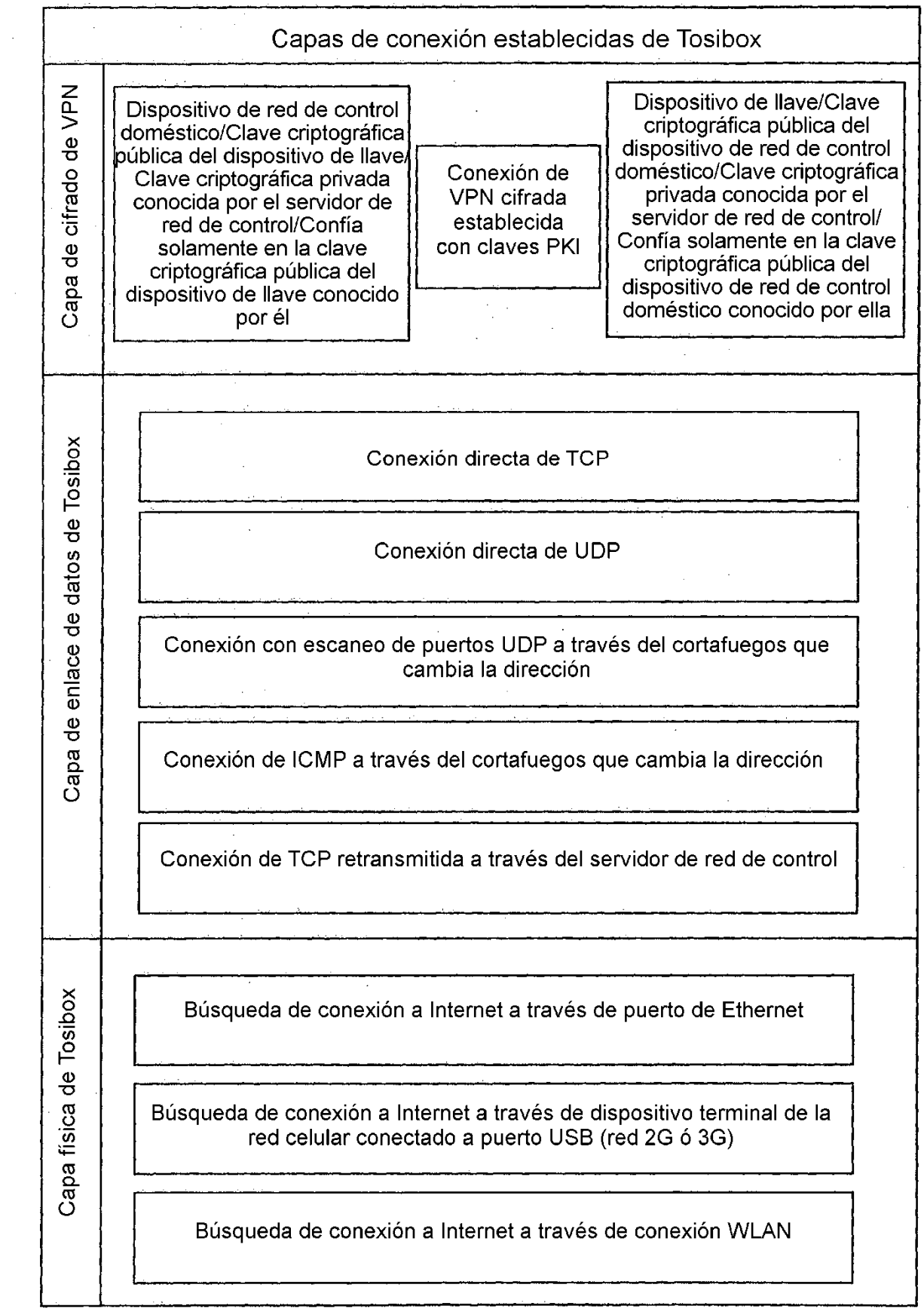

Capas de conexión establecidas de Tosibox
Capa de cifrado de VPN
Dispositivo de red de control doméstico/Clave criptográfica pública del dispositivo de llave/ Clave criptográfica privada conocida por el servidor de red de control/Confía solamente en la clave criptográfica pública del dispositivo de llave conocido por él
Conexión de VPN cifrada establecida con claves PKI
Dispositivo de llave/Clave criptográfica pública del dispositivo de red de control doméstico/Clave criptográfica privada conocida por el servidor de red de control/ Confía solamente en la clave criptográfica pública del dispositivo de red de control doméstico conocido por ella
Capa de enlace de datos de Tosibox
Conexión directa de TCP
Conexión directa de UDP
Conexión con escaneo de puertos UDP a través del cortafuegos que cambia la dirección
Conexión de ICMP a través del cortafuegos que cambia la dirección
Conexión de TCP retransmitida a través del servidor de red de control
Capa física de Tosibox
Búsqueda de conexión a Internet a través de puerto de Ethernet
Búsqueda de conexión a Internet a través de dispositivo terminal de la red celular conectado a puerto USB (red 2G ó 3G)
Búsqueda de conexión a Internet a través de conexión WLAN

Fig. 7