

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 655 675**

51 Int. Cl.:

H04L 29/06 (2006.01)

H04L 12/24 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **19.06.2013** **PCT/GB2013/051590**

87 Fecha y número de publicación internacional: **27.12.2013** **WO13190289**

96 Fecha de presentación y número de la solicitud europea: **19.06.2013** **E 13735362 (9)**

97 Fecha y número de publicación de la concesión europea: **11.10.2017** **EP 2865156**

54 Título: **Aparato y procedimiento para conectar redes informáticas**

30 Prioridad:

20.06.2012 GB 201210907
20.06.2012 GB 201210922

45 Fecha de publicación y mención en BOPI de la
traducción de la patente:
21.02.2018

73 Titular/es:

DEEP-SECURE LIMITED (100.0%)
1 Nimrod House Sandy's Road
Malvern WR14 1JJ, GB

72 Inventor/es:

WISEMAN, SIMON ROBERT

74 Agente/Representante:

AZNÁREZ URBIETA, Pablo

ES 2 655 675 T3

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

DESCRIPCIÓN

Aparato y procedimiento para conectar redes informáticas

Campo técnico de la invención

- 5 La presente invención se refiere a un aparato y a un procedimiento para conectar redes informáticas y en particular para proporcionar una conexión segura entre redes informáticas.

Antecedentes de la invención

- 10 Con frecuencia es necesario controlar el flujo de datos que entra en una red informática o que sale de la misma para proteger la red y los datos almacenados en la misma. Por ejemplo, cuando dos redes conectadas almacenan datos con diferentes clasificaciones de seguridad, es deseable impedir que los datos con una mayor clasificación de seguridad almacenados en la red sean transferidos a la red con una menor clasificación de seguridad. Aunque, en principio, los datos de la red con menor clasificación de seguridad pueden transferirse a la red de mayor clasificación de seguridad, puede ser deseable asegurar que no se transfieran datos que puedan afectar a la integridad de los datos de mayor clasificación almacenados en la red o perjudicar de otro modo a dicha red.

- 15 Una manera de proteger las redes informáticas es el uso de los llamados diodos de datos, según se describe en el documento US5703562. Un diodo de datos proporciona una conexión de datos unidireccional, de manera que es posible restringir el flujo de datos para que sólo entre o salga de una red. Aunque esto es útil para proteger la confidencialidad o la integridad de la información almacenada por la red, impedir la comunicación bidireccional con la red causa problemas.

- 20 Un problema es el de controlar el flujo de datos a través del diodo de datos. La parte receptora del diodo no puede informar a la parte transmisora de la velocidad óptima a la que enviar datos y no es posible la recuperación automática de errores o fallos de transmisión de la lógica receptora, ya que la lógica receptora no puede informar de ningún problema a la lógica transmisora.

- 25 Otro problema es que necesariamente un diodo de datos tiene, a cada lado del enlace unidireccional que éste proporciona, un equipo que requiere mantenimiento, en el sentido de que debe configurarse y necesitará informar de la actividad con fines de control de seguridad. Sin embargo, si el equipo de cada lado del enlace está conectado a un sistema de gestión, esto proporciona una derivación del enlace unidireccional que podría introducir una comunicación bidireccional entre las dos redes. La única manera de que pueda conservarse la propiedad unidireccional es utilizar sistemas de gestión separados para cada lado del diodo, lo que resulta caro y es propenso a errores durante el funcionamiento.

- 30 Un problema relacionado es que el sistema de gestión mismo habitualmente es un sistema sensible que requiere protección de las redes de datos y del equipo de comunicaciones que está gestionando. El diodo de datos que está siendo gestionado no ofrece protección alguna para el sistema de gestión, de manera que se necesita un equipo adicional para ello. Este equipo adicional puede incluir un diodo de datos, en cuyo caso también debe gestionarse éste sin introducir una derivación del diodo de datos. Para evitar esta recurrencia, es usual gestionar tal equipo desde varios puntos, lo que resulta en un aumento en la escala de gastos generales de gestión.

- 35 Con el fin de abordar problemas causados por la imposición de un flujo unidireccional de datos entre redes, pero manteniendo la seguridad de la red, se ha propuesto conectar dos redes con dos conexiones de datos unidireccionales separadas dispuestas para transmitir datos en direcciones opuestas entre ellas. Cada conexión comprende una comprobadora de contenido dispuesta en serie entre un par de diodos de datos que limitan respectivamente la transmisión de datos a y de la comprobadora de contenido. La función de las comprobadoras de contenido es permitir solo la transmisión de datos aceptables de una red a otra y la seguridad de la conexión depende principalmente de las comprobadoras de contenido. Los diodos de datos proporcionan protección a las comprobadoras de contenido.

- 40 Si bien esta disposición permite una comunicación bidireccional controlada entre redes, aún está lejos de ser ideal. Aunque las aplicaciones que se ejecuten en cada red pueden comunicarse entre sí, para hacerlo deben coordinarse para proporcionar el control de flujo y la recuperación de errores requeridos. Por ejemplo, una primera aplicación que se ejecute en un ordenador en una primera red puede necesitar enviar datos a una segunda aplicación que se ejecute en un ordenador en una segunda red conectada. La primera aplicación puede enviar datos a través de un enlace unidireccional, pero entonces debe escuchar para recibir un mensaje

de acuse de recibo enviado desde la segunda aplicación a través del segundo enlace unidireccional opuesto antes de enviar otro mensaje. Este enfoque contrasta con los protocolos de comunicaciones de redes informáticas estándar que están dispuestos en una pila con control de flujo y recuperación de errores normalmente implementados en múltiples niveles de la pila. Como resultado, las aplicaciones no necesitan preocuparse del control de flujo y la recuperación de errores, dado que de ello se ocupa la pila de red. La necesidad de aplicaciones para implementar protocolos a medida para el control de flujo y la recuperación de errores, al nivel de la aplicación, es gravosa y limita la utilidad del enfoque.

Este enfoque tampoco permite gestionar el equipo a cada lado de los diodos de datos mediante un solo sistema sin derivar los diodos de datos y/o las comprobadoras de contenido.

10 Las formas de realización de la presente invención se han hecho teniendo en cuenta estos problemas.

El documento US 7 992 209 B1 describe una disposición para la comunicación bilateral utilizando múltiples enlaces de datos de un solo sentido. La disposición comprende un primer nodo, un segundo nodo, dos enlaces direccionales opuestos de un solo sentido entre los nodos para la transferencia unidireccional y dos aplicaciones de transferencia de datos, una para cada enlace de un solo sentido, para administrar la transferencia unidireccional.

El documento US 2010/299742 A1 da a conocer una pasarela bidireccional con un nivel de seguridad mejorado entre una red de comunicación de alta seguridad y una red de comunicación de baja seguridad. El camino de avance desde la red de alta seguridad hasta la red de baja seguridad es un camino monodireccional, mientras que el camino de retorno desde la red de baja seguridad hasta la red de alta seguridad comprende un enlace de baja velocidad provisto de una capa de enlace según un protocolo que difiere de los protocolos utilizados en las capas de enlace tanto en la red de alta seguridad como en la red de baja seguridad. La capa de enlace del enlace de baja velocidad tiene un protocolo de autenticación que garantiza el origen de los datos.

Sumario de la invención

25 Según un aspecto de la presente invención, se proporciona un aparato para conectar tres o más redes informáticas, comprendiendo el aparato:

tres o más máquinas de interfaz de red, cada una de ellas dispuesta para conectarse a una red informática respectiva con un enlace de comunicaciones bidireccional que permite a la máquina de interfaz de red recibir datos y transmitirlos desde y a la red informática;

30 al menos dos comprobadoras de contenido conectadas junto con las tres o más máquinas de interfaz de red y configuradas para permitir que se transmitan datos desde una máquina de interfaz de red a otra;

estando cada máquina de interfaz de red conectada a una primera comprobadora de contenido asociada, por medio de un primer enlace de comunicaciones unidireccional respectivo configurado para permitir que se transmitan datos desde la máquina de interfaz de red a la primera comprobadora de contenido asociada, pero no que los reciba la máquina de interfaz de red desde la primera comprobadora de contenido asociada;

40 estando cada máquina de interfaz de red conectada a una segunda comprobadora de contenido asociada, por medio de un segundo enlace de comunicaciones unidireccional respectivo configurado para permitir que se transmitan datos desde la segunda comprobadora de contenido asociada a la máquina de interfaz de red, pero no que los reciba la segunda comprobadora de contenido asociada desde la máquina de interfaz de red;

45 estando el aparato configurado de manera que los datos transmitidos desde cada máquina de interfaz de red a cualquier otra máquina de interfaz de red deben ser transmitidos desde la máquina de interfaz de red transmisora a su primera comprobadora de contenido asociada a través de su primer enlace de comunicaciones unidireccional respectivo, y los datos transmitidos a cada máquina de interfaz de red desde cualquier otra máquina de interfaz de red deben ser transmitidos a la máquina de interfaz de red receptora desde su segunda comprobadora de contenido asociada a través de su segundo enlace de comunicaciones unidireccional respectivo; y

50 estando cada máquina de interfaz de red dispuesta para transmitir datos de control de flujo a otra máquina de interfaz de red para regular así la transmisión de datos entre las máquinas de interfaz de red.

Así, el control del flujo de datos entre las máquinas de interfaz de red puede ser gestionado por las máquinas de interfaz de red mediante la transmisión de datos de control de flujo, que también son comprobados por la comprobadora de contenido o por cada comprobadora de contenido, sin utilizar recursos de redes o aplicaciones conectadas entre las que se están transfiriendo datos.

- 5 La o cada comprobadora de contenido puede estar configurada para pasar datos sólo si éstos no van a dañar la integridad o la disponibilidad de los servicios ofrecidos por su destinatario. Alternativa o adicionalmente, la o cada comprobadora de contenido puede estar configurada para no pasar información que vaya a causar una relevación perjudicial.

- 10 Otro aspecto de la invención proporciona un procedimiento para proporcionar una comunicación bidireccional entre tres o más redes informáticas utilizando el aparato, comprendiendo el procedimiento los pasos de:

conectar cada red informática a una máquina de interfaz de red respectiva con un enlace de comunicaciones bidireccional;

recibir datos desde una red informática en una primera máquina de interfaz de red;

- 15 pasar los datos recibidos desde la primera máquina de interfaz de red a una primera comprobadora de contenido asociada, que está asociada a la primera máquina de interfaz de red a través de un primer enlace de comunicaciones unidireccional respectivo que conecta a la primera comprobadora de contenido asociada la primera máquina de interfaz de red;

- 20 pasar los datos recibidos a una segunda máquina de interfaz de red desde una segunda comprobadora de contenido asociada, que está asociada a la segunda máquina de interfaz de red a través de un segundo enlace de comunicaciones unidireccional respectivo que conecta a la segunda máquina de interfaz de red la segunda comprobadora de contenido asociada;

entregar los datos recibidos por la segunda máquina de interfaz de red a otra red informática a la que la misma está conectada a través de un enlace de comunicaciones bidireccional; y

- 25 pasar datos de control de flujo entre al menos la primera y la segunda máquinas de interfaz de red a través de al menos una comprobadora de contenido para regular la transmisión de datos entre las máquinas.

- 30 Las máquinas de interfaz de red pueden estar dispuestas para comunicarse con las redes informáticas respectivas utilizando una pila de protocolo bidireccional. El enlace de comunicaciones unidireccional puede estar formado en cada caso por un transmisor comprendido en cada máquina de interfaz de red que esté conectado a través de un conducto a un receptor comprendido en la comprobadora de contenido asociada.

- 35 Dos o más máquinas de interfaz de red pueden estar conectadas a la misma comprobadora de contenido mediante unos enlaces unidireccionales respectivos, que permitan una transmisión de datos desde las máquinas de interfaz de red a la comprobadora de contenido. Una comprobadora de contenido puede estar conectada a dos o más máquinas de interfaz de red mediante unos enlaces de comunicaciones unidireccionales respectivos, que permitan una transmisión de datos desde la comprobadora de contenido a una de las máquinas de interfaz de red conectadas seleccionada o a ambas.

- 40 Puede preverse el mismo número o un número mayor de comprobadoras de contenido que de máquinas de interfaz de red, estando las comprobadoras de contenido conectadas entre sí mediante enlaces de comunicaciones unidireccionales en una formación anular y estando cada máquina de interfaz de red conectada a una comprobadora de contenido con un enlace de comunicaciones unidireccional que le permite transmitir datos a la comprobadora de contenido y a otra comprobadora de contenido con un enlace de comunicaciones unidireccional que le permite recibir datos desde la comprobadora de contenido. Con esta disposición, cada comprobadora de contenido puede estar conectada mediante enlaces de comunicaciones unidireccionales de configuración opuesta respectivos a sólo dos máquinas de interfaz de red.

- 45 Dos o más comprobadoras de contenido de configuración diferente pueden estar conectadas en serie mediante enlaces de comunicaciones unidireccionales, de manera que los datos recibidos por la primera comprobadora de contenido en la serie deban pasar a través de cada otra comprobadora de contenido antes de su transmisión posterior a otro componente.

- 50 El aparato comprende al menos tres máquinas de interfaz de red, una de las cuales puede denominarse máquina de interfaz de red de gestión, configurada para pasar información de control y de gestión entre una red a la que está conectada a través de un enlace de comunicaciones bidireccional y cada una de las otras

máquinas de interfaz de red del aparato. Así, todas las máquinas de interfaz de red pueden comunicarse con una sola red o máquina de gestión sin comprometer la seguridad.

- 5 El aparato puede estar dispuesto de manera que al menos una máquina de interfaz de red pueda transmitir datos a cualquier otra máquina de interfaz de red sin que los datos pasen a través de una tercera máquina de interfaz de red.

Descripción detallada de la invención

Con el fin de que la invención pueda comprenderse más claramente, a continuación se describirán formas de realización de la misma sólo a modo de ejemplo, en referencia a las figuras adjuntas, en los cuales:

- 10 Figura 1: vista general de un aparato según la invención;
 Figura 2: muestra una primera forma de realización de un aparato de conexión;
 Figura 3: muestra una segunda forma de realización de un aparato de conexión;
 Figura 4: muestra una tercera forma de realización de un aparato de conexión; y
 Figura 5: muestra una cuarta forma de realización de un aparato de conexión.

- 15 En referencia a las figuras, la figura 1 muestra tres redes informáticas, una red externa 101, una red protegida 102 y una red de gestión 103, conectadas entre sí mediante un aparato de conexión 104 según la invención. Cada red, 101, 102 y 103 está conectada al aparato de conexión 104 mediante un enlace de comunicaciones bidireccional 105, 106, 107 convencional respectivo que soporta un protocolo de comunicación de red informática convencional que emplea una pila de protocolo bidireccional, tal como TCP/IP a través de *Ethernet* o *Frame Relay* (retransmisión de tramas). Cada enlace bidireccional permite que se transfieran datos en cualquier dirección entre las redes que conecta y el aparato de conexión 104. Puede comprender cualquier conexión adecuada formada por uno o más conductos adecuados, tales como cables eléctricos o fibras ópticas, y podría emplear dos conductos que sirvan para pasar datos en sólo una dirección dispuestos para pasar datos en direcciones opuestas respectivas para establecer un enlace bidireccional.

- 20 El aparato de conexión permite que se transfieran sólo tipos especificados de datos entre las redes con el fin de proteger la integridad y/o la confidencialidad de los datos almacenados en las redes, o proteger éstas de otro modo. Las referencias a datos que se están almacenando en una red concreta incluyen datos almacenados en uno o más ordenadores u otros aparatos incluidos en la red.

- 25 La figura 2 muestra una forma de realización del aparato de conexión 104 adecuada para el uso en la disposición ilustrada en la figura 1. En referencia a la figura 2, el aparato comprende una primera, una segunda y una tercera máquinas de interfaz de red 201, 202, 203 para la conexión respectiva a las redes externa 101, protegida 102 y de gestión a través de enlaces bidireccionales 105, 106 y 107 que permiten una transferencia de datos desde cada red a su máquina de interfaz de red asociada y viceversa.

- 30 Cada máquina de interfaz de red comprende un ordenador programado que incluye un software y/o hardware apropiado para implementar la pila de protocolo bidireccional para la comunicación con una red informática a través de un enlace de comunicaciones bidireccional. Cada máquina de interfaz de red podría comprender uno o más componentes interconectados. En particular, cada máquina de interfaz de red podría construirse a partir de equipo informático de uso general estándar, tal como un procesador Intel™ o Arm™, y ejecutar un sistema operativo comercial, tal como Microsoft™ Windows™ o Linux™. Para establecer una comunicación bidireccional con una red informática, las máquinas de interfaz pueden comprender dispositivos de conexión de redes informáticas comerciales, tales como tarjetas de interfaz de red *Ethernet*.

- 35 El software de aplicación ejecutado en estas máquinas funciona como un *proxy* de protocolo, terminando conexiones de ordenadores cliente conectados a una red a la que las máquinas están conectadas, o estableciendo conexiones a ordenadores servidor en la red. Para protocolos de correo electrónico podrían utilizarse como *proxy* aplicaciones tales como el software de transferencia de mensajes *sendmail*. Para aplicaciones web podría utilizarse un servidor web tal como Apache™.

- 40 Cada máquina de interfaz comprende también un transmisor 204, 205, 206 para transmitir datos y un receptor 207, 208, 209 para recibir datos. Pueden utilizarse cualesquiera transmisores y receptores adecuados, pero normalmente éstos serán eléctricos u ópticos. Cada máquina de interfaz de red está dispuesta para transmitir datos recibidos a través del enlace de comunicaciones bidireccional y está destinada a transmitirlos posteriormente a otro dispositivo a través de su transmisor, conformando un enlace de datos unidireccional con el otro dispositivo, junto con datos de control de flujo relativos a la transmisión de datos entre máquinas de interfaz de red. Estos datos de control de flujo podrían comprender, por ejemplo, un acuse de recibo de que se han recibido datos desde otra máquina de interfaz de red o una indicación de que la máquina está lista para recibir más datos. Cada máquina de interfaz de red está dispuesta también para transmitir datos recibidos por

su receptor desde otro dispositivo (formando así un enlace de datos unidireccional con ese dispositivo) y está destinada a una transmisión posterior, a través del enlace de comunicaciones bidireccional, y a transmitir datos de control de flujo comprendidos en los datos recibidos o relativos a éstos a través de su transmisor, por ejemplo un acuse de recibo de datos o una señal para pedir la transmisión de más datos.

- 5 En cada máquina de interfaz de red se ejecutan copias separadas de los *proxies* y éstas se comunican a través de un software adicional que intercambia datos a través de los enlaces unidireccionales. Los protocolos utilizados por este software podrían estar basados en estándares tales como Ethernet, que funcionen naturalmente de manera unidireccional. El software podría escribirse en cualquier lenguaje de programación de sistemas, tal como C++.
- 10 El aparato de conexión comprende además una primera y una segunda máquinas comprobadoras de contenido 210, 211. Cada máquina comprobadora de contenido puede comprender un ordenador programado. Las comprobadoras de contenido pueden construirse a partir de hardware informático de uso general y sistemas operativos comerciales, aunque es probable que éstos se instalen en una configuración mínima para evitar introducir vulnerabilidades de seguridad en software sin utilizar. El software de gestión de protocolo y de comprobación de contenido puede escribirse en C++.

Alternativamente, la comprobadora de contenido puede implementarse utilizando hardware especializado, tal como el desarrollado para implementar unidades codificadoras. Éstas son normalmente una combinación de interfaces externas, procesadores y componentes lógicos programables dedicados, tales como un arreglo de puertas programable in situ (*Field Programmable Gate Array* (FPGA) adecuadamente programado. La función de la comprobación de contenido está entonces dividida, con su funcionalidad de interconexión implementada mediante lógica alrededor de las interfaces, su funcionalidad de gestión de protocolo implementada en software ejecutado en los procesadores y su función de validación de datos implementada en procesadores adicionales o en lógica dentro de un componente FPGA.

- 25 La primera máquina comprobadora de contenido 210 comprende dos receptores 212, 213 y un solo transmisor 214. La segunda máquina comprobadora de contenido 211 comprende dos transmisores 215, 216 y un solo receptor 217.

La primera máquina comprobadora de contenido 210 funciona para recibir datos en cualquiera de sus dos receptores, para comprobar los datos y para, de los datos recibidos, transmitir sólo aquellos apropiados a través de su transmisor.

- 30 La segunda máquina comprobadora de contenido 211 funciona para recibir datos en su receptor, para comprobar los datos y para separar los datos de gestión de otros datos y entonces transmitir sólo aquellos datos de gestión apropiados a través de un transmisor y sólo otros datos apropiados a través del otro transmisor.

Cada transmisor de una máquina de interfaz de red está conectado a través un conducto 219 adecuado, tal como un cable eléctrico o una fibra óptica, a un receptor respectivo de una máquina comprobadora de contenido, conformando así un enlace de comunicaciones unidireccional entre la interfaz de red conectada y las máquinas comprobadoras de contenido que permite transmitir datos sólo desde cada máquina de interfaz de red a una máquina comprobadora de contenido. Cada receptor de una máquina de interfaz de red está conectado, a través de un conducto 220 adecuado, al transmisor de la máquina comprobadora de contenido que no es a la que está conectado el transmisor de la máquina de interfaz de red, permitiendo sólo la transmisión de datos desde esa máquina comprobadora de contenido a la máquina de interfaz de red conectada. Específicamente, los transmisores de la primera y la tercera máquinas de interfaz de red están conectados a los receptores de la primera máquina comprobadora de contenido y el transmisor de la segunda máquina de interfaz de red está conectado al receptor de la segunda máquina comprobadora de contenido.

45 Asimismo, los receptores de la primera y la tercera máquinas de interfaz de red están conectados a los transmisores de la segunda máquina comprobadora de contenido y el receptor de la segunda máquina de interfaz de red está conectado al transmisor de la primera máquina comprobadora de contenido.

- 50 El aparato permite que se pasen datos entre las tres máquinas de interfaz de red, permitiendo así una comunicación bidireccional entre redes informáticas respectivas conectadas a las tres máquinas de interfaz de red. Los datos que pasan entre las máquinas de interfaz de red deben pasar siempre a través de una comprobadora de contenido, que permite que pasen sólo datos apropiados y sirve para proteger las redes frente a una transferencia de datos inadecuados, por ejemplo una transmisión de datos no deseados, como un virus informático, desde la red externa a la red protegida y una transmisión de datos sensibles desde una red protegida a una red externa. Los enlaces de comunicación de datos entre las máquinas de interfaz de red y las máquinas comprobadoras de contenido son todos unidireccionales, cada máquina de interfaz de red transmitiendo datos a una máquina comprobadora de contenido y recibiendo datos de otra. Estos enlaces

unidireccionales sirven para proteger las máquinas comprobadoras de contenido y las máquinas a las que éstas pasan datos frente a un ataque externo que pueda tener como objetivo vulnerabilidades en el receptor, tales como desbordamientos de memoria intermedia (*buffer*).

5 En uso, cuando se deben transferir datos desde una red externa a una red protegida, éstos son recibidos por la primera máquina de interfaz de red 201, que a continuación los transmite, junto con datos de control de flujo apropiados, a la segunda máquina de interfaz de red 202 a través de la primera comprobadora de contenido 210. La segunda máquina de interfaz de red 202 envía de vuelta datos de control de flujo relevantes en respuesta a la primera máquina de interfaz de red 201 a través de la segunda comprobadora de contenido 211. Así, la transmisión de datos recibidos desde la red externa por el camino unidireccional entre la primera y la
10 tercera máquinas de control de red es coordinada entre la primera y la tercera máquinas de interfaz de red, superando los problemas de transmisión con diodos de datos existentes y sin tener que implicar aplicaciones ejecutadas en redes en la coordinación de la transmisión de datos. Asimismo, pueden transmitirse datos desde una red protegida a la red externa a través de la segunda comprobadora de contenido 211, pasando adicionalmente datos de control desde la primera máquina de interfaz de red 201 a la segunda máquina de
15 interfaz de red 202 a través de la primera máquina comprobadora de contenido 210.

La primera y la segunda máquinas de interfaz de red 201, 202 y las máquinas comprobadoras de contenido 210, 211 pueden también cada una transmitir datos a la tercera máquina de interfaz de red 203 y recibir datos de la misma y así intercambiar datos con una red de gestión. Los datos que se deban transmitir a la tercera máquina de interfaz de red 203 deben ser transmitidos a esa máquina por la segunda máquina comprobadora de contenido 211. Los datos procedentes de la primera interfaz de red 201 y la primera máquina comprobadora de contenido 210 deben pasar a la segunda máquina de interfaz de red 202 para una transmisión a la segunda máquina comprobadora de contenido 211. Los datos que deben ser recibidos desde la tercera máquina de interfaz de red 203 se transmiten a la primera máquina comprobadora de contenido 210, desde la cual pueden, si se desea, pasar a la segunda máquina de interfaz de red 202, desde ésta a la segunda máquina
20 comprobadora de contenido 211 y desde ésta a la primera máquina de interfaz de red 201.

Los datos enviados a una red de gestión y recibidos desde la misma a través de la tercera máquina de interfaz de red 203 pueden comprender información sobre la salud de la máquina fuente o detalles de los datos que está manejando. Además, la primera y la segunda máquinas de interfaz de red 201, 202 pueden intercambiar datos con la tercera máquina de interfaz de red 203 relacionados con el flujo de datos entre las máquinas de
30 interfaz de red.

Dado que todos los datos enviados a una red de gestión y recibidos desde la misma deben pasar a través de una comprobadora de contenido, una red de gestión no proporciona una conexión no segura entre redes externas y protegidas. Es importante el hecho de que la tercera máquina de interfaz de red 203 está conectada para recibir datos directamente desde la segunda comprobadora de contenido 211, de manera que los datos
35 recibidos por la segunda máquina de interfaz de red desde una red protegida pueden transmitirse a la tercera máquina de gestión de red 203, y desde ésta a una red de gestión, sin que tengan que pasar a través de la primera máquina de interfaz de red, lo que podría suponer un peligro debido a la conexión a la red externa.

La disposición permite que cada máquina se comunique con las otras máquinas para una comunicación bidireccional entre una red externa y una red protegida, proporcionar información de registro a una máquina de interfaz de red de gestión y recibir instrucciones de configuración desde la misma. Las máquinas también pueden intercambiar mensajes relativos al control de flujo de su comunicación.

Así, la disposición proporciona una comunicación bidireccional entre una red externa y una red protegida con las ventajas de seguridad de utilizar enlaces unidireccionales, siendo al mismo tiempo capaz de gestionar la falta de fiabilidad inherente de los enlaces unidireccionales y capaz de operar y administrar el equipo desde un
45 solo punto.

En la figura 3 se muestra una variación de la disposición mostrada en la figura 2, utilizándose números iguales para identificar componentes iguales. La disposición mostrada en la figura 3 se diferencia de la de la figura 2 por la adición de una tercera máquina comprobadora de contenido 221, conectada en serie entre la primera máquina comprobadora de contenido 210 y la segunda máquina de interfaz de red 202. La tercera máquina comprobadora de contenido 221 tiene un receptor 222 conectado mediante un conducto 223 al transmisor de la primera máquina comprobadora de contenido 210 y un transmisor 224 conectado mediante un conducto 225 al receptor 208 de la segunda máquina de interfaz de red 202, de manera que se establecen caminos de comunicación unidireccional de la primera máquina comprobadora de contenido 210 a la tercera máquina comprobadora de contenido 221 y de la tercera máquina comprobadora de contenido a la segunda máquina
50 de interfaz de red 202.

La previsión de la máquina comprobadora de contenido adicional en el camino de los datos a la segunda máquina de interfaz de red proporciona a la red protegida a la que esa máquina está conectada un nivel adicional de protección contra la recepción de datos inadecuados o un ataque externo. Lo ideal es que la primera y la tercera máquinas comprobadoras de contenido estén hechas con diseños diferentes, para evitar modos de fallo comunes. La probabilidad de que ambos medios comprobadores de contenido permitan el paso de datos inadecuados o sean deshabilitados por un atacante se reduce enormemente en comparación con una sola máquina.

En cualquier realización, una sola máquina comprobadora de contenido podría sustituirse por dos o más máquinas comprobadoras de contenido conectadas en serie mediante una conexión de datos unidireccional.

La figura 4 muestra otra variación de la disposición mostrada en la figura 2, utilizándose de nuevo números de referencia iguales para identificar componentes iguales. La disposición de la figura 2 se ha modificado para permitir que dos redes externas se comuniquen con una red protegida y una red de gestión, dotando la primera máquina comprobadora de contenido 210 de un tercer receptor 225 y dotando la segunda máquina de contenido 211 de un tercer transmisor 226, lo que permite que una cuarta máquina de interfaz de red 227, que está conectada mediante un enlace bidireccional 228 a una segunda red externa, se conecte a la primera comprobadora de contenido 210 de la misma manera que, y en paralelo a, la primera máquina de interfaz de red 201. Así, la cuarta máquina de interfaz de red 227 puede comunicarse con la segunda y la tercera máquinas de interfaz 202, 203 exactamente de la misma manera que la primera máquina de interfaz de red 201. Pueden transmitirse datos entre las dos redes externas haciéndolos pasar a través de la segunda máquina de interfaz de red, en la que, dado que está conectada a una red protegida, puede confiarse para que no revele o modifique datos inadecuadamente. En cambio, gracias a la conexión paralela, pueden transmitirse datos entre cualquiera de las dos redes externas y la red protegida sin pasar a través de una máquina de conexión de red que esté conectada a otra red externa. En esta disposición, la segunda máquina comprobadora de contenido 211 está dispuesta para enrutar selectivamente información recibida para la transmisión posterior a sólo una cualquiera de las dos máquinas de conexión de red primera y cuarta 201, 227 o a ambas.

La figura 5 muestra otra forma de realización del aparato de conexión de red adecuada para conectar redes mutuamente sospechosas. En esta disposición se emplea el mismo número de comprobadoras de contenido 501 que de máquinas de interfaz de red 502. Cada comprobadora de contenido tiene dos receptores 504, 508 y dos transmisores 503, 505. Un transmisor 503 de cada comprobadora de contenido está conectado mediante un conducto al receptor 504 de otra comprobadora de contenido para formar un anillo alrededor del cual los datos pueden pasar sólo en una dirección. El otro transmisor 505 de cada comprobadora de contenido está conectado mediante un conducto al receptor 506 de una máquina de interfaz de red 502, y un transmisor 507 de esa máquina de interfaz de red está conectado mediante un conducto al receptor 508 de la siguiente comprobadora de contenido en el anillo en la dirección del flujo de datos. Cada máquina de interfaz de red está conectada a una red a través de un enlace bidireccional convencional 509. En el ejemplo mostrado hay cuatro máquinas de interfaz de red y cuatro comprobadoras de contenido. Una máquina de interfaz de red puede estar conectada a una red de gestión y las otras a redes mutuamente sospechosas. De este modo pueden conectarse un mínimo de tres máquinas de interfaz de red y comprobadoras de contenido y la disposición puede adaptarse para incluir cualquier número mayor.

En esta disposición, además de que todos los datos que pasan entre máquinas de interfaz de red pasan a través de al menos una máquina comprobadora de contenido, los datos pueden pasar de una máquina de interfaz de red cualquiera a otra máquina de interfaz de red cualquiera sin pasar a través de ninguna otra máquina de interfaz de red.

En esta forma de realización, cada máquina comprobadora de contenido puede transmitir selectivamente datos recibidos a cualquiera de las dos máquinas de interfaz de red o a ambas y a la comprobadora de contenido siguiente en el anillo.

Así, por ejemplo, los datos recibidos desde una red conectada a la primera máquina de interfaz de red para la transmisión a la red conectada a la tercera máquina de interfaz de red se transmitirán a la primera, la segunda y la tercera comprobadoras de contenido sucesivamente y desde la tercera comprobadora de contenido a la tercera máquina de interfaz de red. Entonces pueden transmitirse datos de control de flujo desde la tercera máquina de interfaz de red, a través de la cuarta comprobadora de contenido, y a continuación de vuelta a la primera máquina de interfaz de red.

Las formas de realización anteriores se han descrito sólo a modo de ejemplo. Son posibles muchas variaciones sin apartarse del alcance de la invención, tal como está definido en las reivindicaciones adjuntas.

Reivindicaciones

1. Aparato para conectar tres o más redes informáticas (101, 102, 103), comprendiendo el aparato:
 - a. tres o más máquinas de interfaz de red (201, 202, 203), cada una de ellas dispuesta para conectarse a una red informática respectiva con un enlace de comunicaciones bidireccional (105, 106, 107) que permite a la máquina de interfaz de red recibir datos desde la red informática y transmitir datos a la red informática;
 - b. al menos dos comprobadoras de contenido (210, 211) conectadas junto con las tres o más máquinas de interfaz de red y configuradas para permitir que se transmitan datos desde una máquina de interfaz de red a otra;
 - c. estando cada máquina de interfaz de red conectada a una primera comprobadora de contenido asociada mediante un primer enlace de comunicaciones unidireccional respectivo configurado para permitir que se transmitan datos desde la máquina de interfaz de red a la primera comprobadora de contenido asociada, pero no que los reciba la máquina de interfaz de red desde la primera comprobadora de contenido asociada;
 - d. estando cada máquina de interfaz de red conectada a una segunda comprobadora de contenido asociada mediante un segundo enlace de comunicaciones unidireccional respectivo configurado para permitir que se transmitan datos desde la segunda comprobadora de contenido asociada a la máquina de interfaz de red, pero no que los reciba la segunda comprobadora de contenido asociada desde la máquina de interfaz de red;
 - e. estando el aparato configurado de manera que los datos transmitidos desde cada máquina de interfaz de red a cualquier otra máquina de interfaz de red deben ser transmitidos desde la máquina de interfaz de red transmisora a su primera comprobadora de contenido asociada a través de su primer enlace de comunicaciones unidireccional respectivo, y los datos transmitidos a cada máquina de interfaz de red desde cualquier otra máquina de interfaz de red deben ser transmitidos a la máquina de interfaz de red receptora desde su segunda comprobadora de contenido asociada a través de su segundo enlace de comunicaciones unidireccional respectivo; y
 - f. estando cada máquina de interfaz de red dispuesta para transmitir datos de control de flujo a otra máquina de interfaz de red para regular así la transmisión de datos entre las máquinas de interfaz de red.
2. Aparato según la reivindicación 1, donde las máquinas de interfaz de red están dispuestas para comunicarse con una red informática utilizando una pila de protocolo bidireccional.
3. Aparato según cualquiera de las reivindicaciones anteriores, donde el enlace de comunicaciones unidireccional está formado por un transmisor (204, 205, 206) comprendido en cada máquina de interfaz de red, conectado a través de un conducto (219) a un receptor (212, 213, 217), comprendido en una comprobadora de contenido.
4. Aparato según cualquiera de las reivindicaciones anteriores, donde dos o más máquinas de interfaz de red están conectadas a la misma comprobadora de contenido mediante unos enlaces unidireccionales respectivos, que permiten una transmisión de datos desde las máquinas de interfaz de red a la comprobadora de contenido, y/o una comprobadora de contenido está conectada a dos o más máquinas de interfaz de red mediante unos enlaces de comunicaciones unidireccionales respectivos, que permiten una transmisión de datos desde la comprobadora de contenido a una de las máquinas de interfaz de red conectadas seleccionada, a dos de las máquinas de interfaz de red conectadas o a todas ellas.
5. Aparato según cualquiera de las reivindicaciones anteriores, que tiene el mismo número o un número mayor de comprobadoras de contenido que de máquinas de interfaz de red, estando las comprobadoras de contenido conectadas entre sí mediante enlaces de comunicaciones unidireccionales en una formación anular y estando cada máquina de interfaz de red conectada a una comprobadora de contenido con un enlace de comunicaciones unidireccional que le permite transmitir datos a la comprobadora de contenido, y a otra comprobadora de contenido con un enlace de comunicaciones unidireccional que le permite recibir datos desde la comprobadora de contenido.
6. Aparato según la reivindicación 5, donde cada comprobadora de contenido está conectada mediante enlaces de comunicaciones unidireccionales de configuración opuesta respectivos a no más de dos máquinas de interfaz de red.
7. Aparato según cualquiera de las reivindicaciones anteriores, donde dos o más comprobadoras de contenido de configuración diferente están conectadas en serie mediante dos o más enlaces de comunicaciones unidireccionales, de manera que los datos recibidos por la primera comprobadora de

contenido en la serie deben pasar a través de cada otra comprobadora de contenido antes de su transmisión posterior a otro componente.

- 5 **8.** Aparato según cualquiera de las reivindicaciones anteriores, donde una máquina de interfaz de red está designada como máquina de interfaz de red de gestión configurada para pasar información de control y de gestión entre una red, a la que está conectada, y cada una de las otras máquinas de interfaz de red del aparato.
- 9.** Aparato según cualquiera de las reivindicaciones anteriores, dispuesto de manera que al menos una máquina de interfaz de red puede transmitir datos a cualquier otra máquina de interfaz de red sin que los datos pasen a través de ninguna tercera máquina interfaz de red.
- 10 **10.** Aparato según cualquiera de las reivindicaciones anteriores, donde la o cada comprobadora de contenido está configurada para pasar datos sólo si los datos no van a dañar la integridad o la disponibilidad de servicios ofrecidos por su destinatario.
- 11.** Aparato según cualquiera de las reivindicaciones anteriores, donde la o cada comprobadora de contenido está configurada para no pasar información que vaya a causar una revelación perjudicial.
- 15 **12.** Sistema que comprende una pluralidad de redes informáticas y un aparato según cualquiera de las reivindicaciones anteriores, estando la pluralidad de redes informáticas conectadas entre sí mediante el aparato, estando cada red conectada a una máquina de interfaz de red respectiva mediante un enlace de comunicaciones bidireccional.
- 20 **13.** Procedimiento para proporcionar una comunicación bidireccional entre tres o más redes informáticas utilizando un aparato según cualquiera de las reivindicaciones 1 a 11, comprendiendo el procedimiento los pasos de:
 - a) conectar cada red informática a una máquina de interfaz de red respectiva con un enlace de comunicaciones bidireccional;
 - 25 b) recibir datos desde una red informática en una primera máquina de interfaz de red;
 - c) pasar los datos recibidos desde la primera máquina de interfaz de red a una primera comprobadora de contenido asociada, que está asociada con la primera máquina de interfaz de red, a través de un primer enlace de comunicaciones unidireccional respectivo que conecta a la primera comprobadora de contenido asociada la primera máquina de interfaz de red;
 - 30 d) pasar los datos recibidos a una segunda máquina de interfaz de red desde una segunda comprobadora de contenido asociada, que está asociada con la segunda máquina de interfaz de red, a través de un segundo enlace de comunicaciones unidireccional respectivo que conecta a la segunda máquina de interfaz de red la segunda comprobadora de contenido asociada;
 - e) entregar los datos recibidos por la segunda máquina de interfaz de red a otra red informática a la que la misma está conectada a través de un enlace de comunicaciones bidireccional; y
 - 35 f) pasar datos de control de flujo entre al menos la primera y la segunda máquinas de interfaz de red a través de al menos una comprobadora de contenido para regular la transmisión de datos entre las máquinas.
- 40 **14.** Procedimiento según la reivindicación 13, donde los datos pasados entre máquinas de interfaz de red se pasan, a través de un primer enlace de comunicaciones unidireccional, a una comprobadora de contenido y, a través de un segundo enlace de comunicaciones unidireccional, desde la comprobadora de contenido a una máquina de conexión de red receptora.

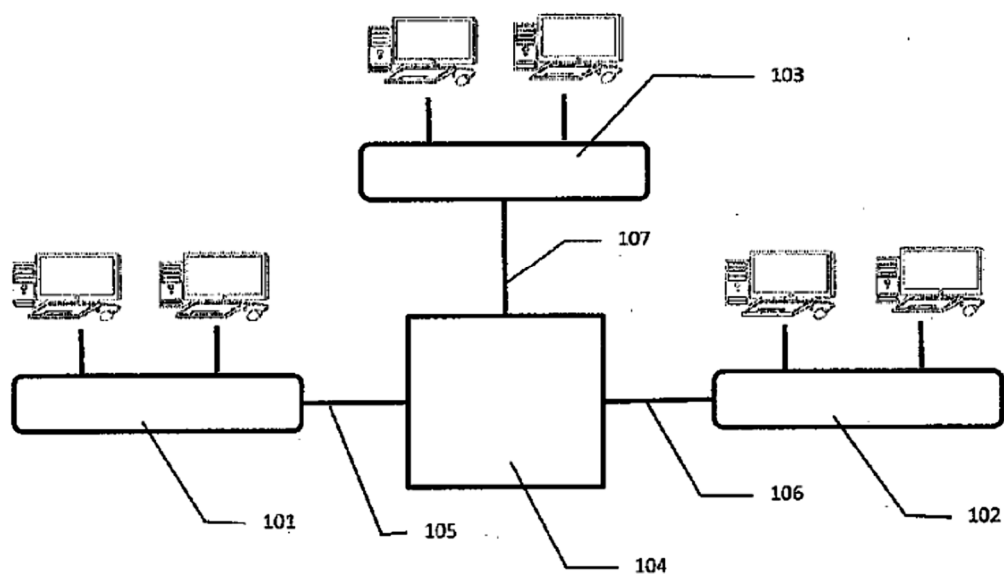


Fig. 1

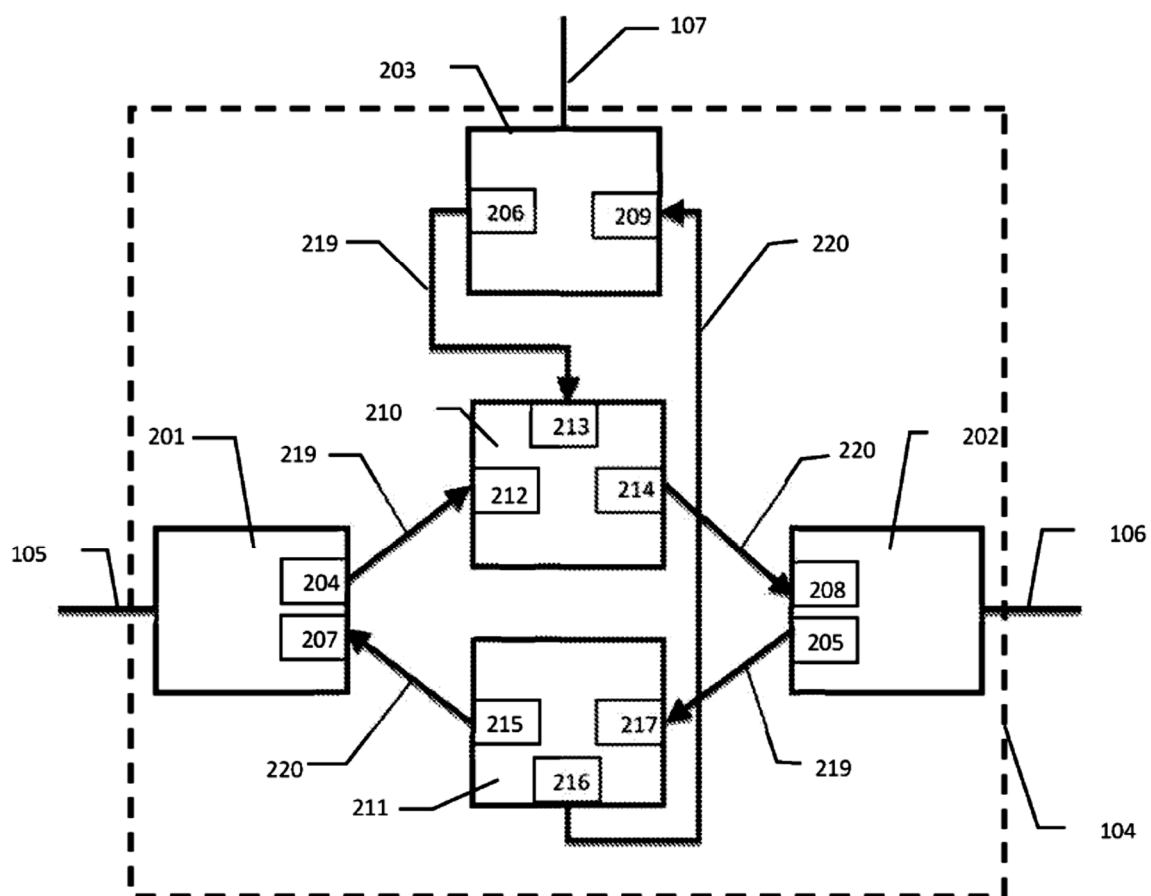


Fig. 2

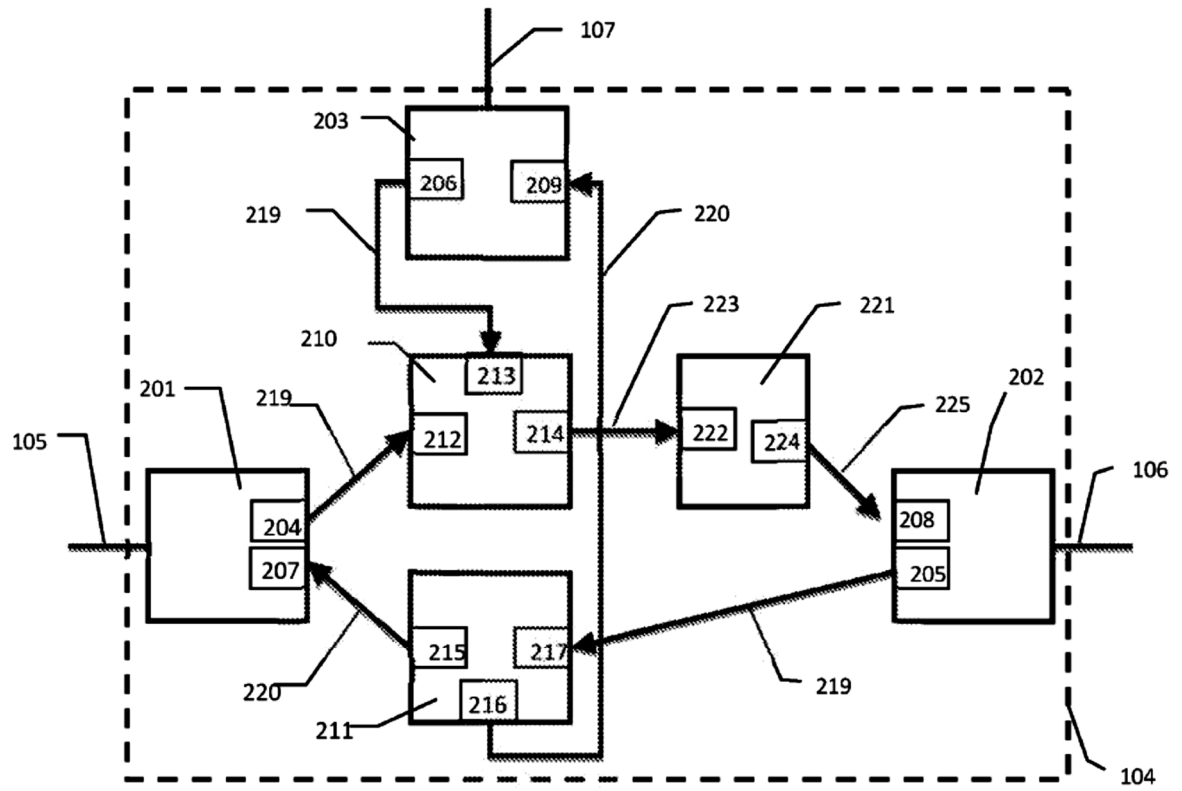


Fig. 3

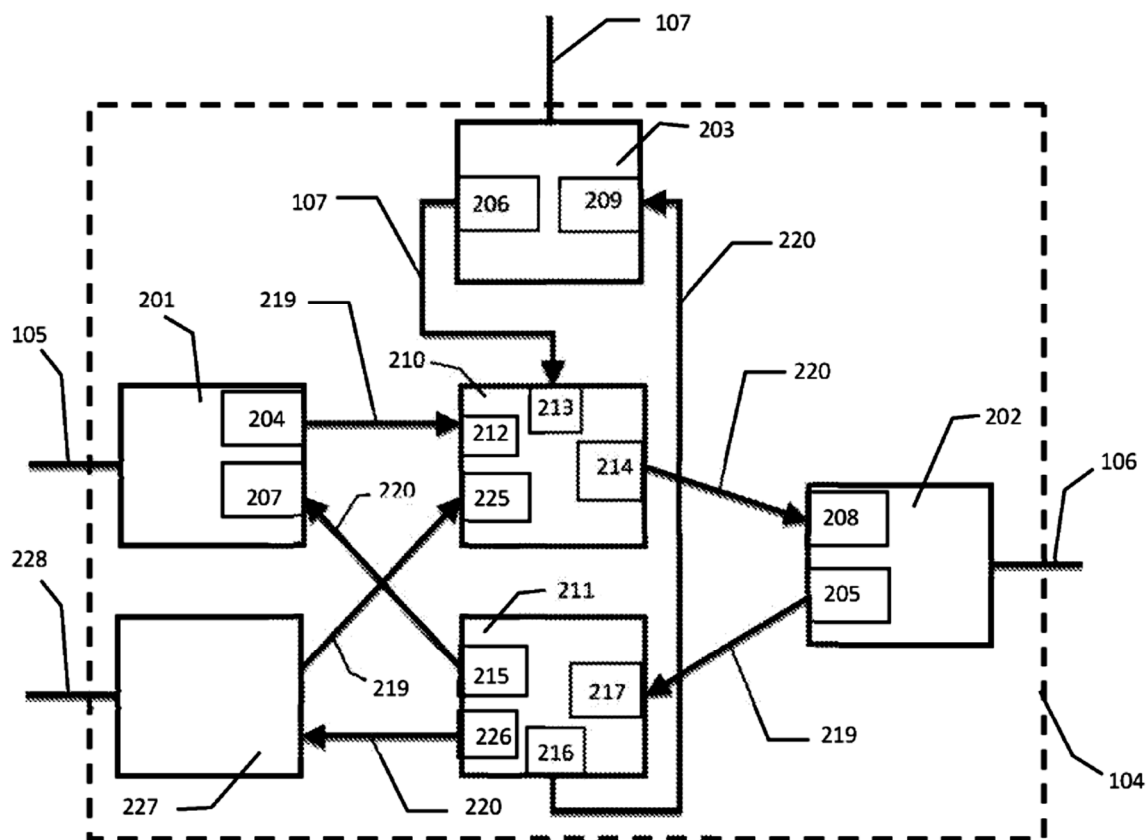


Fig. 4

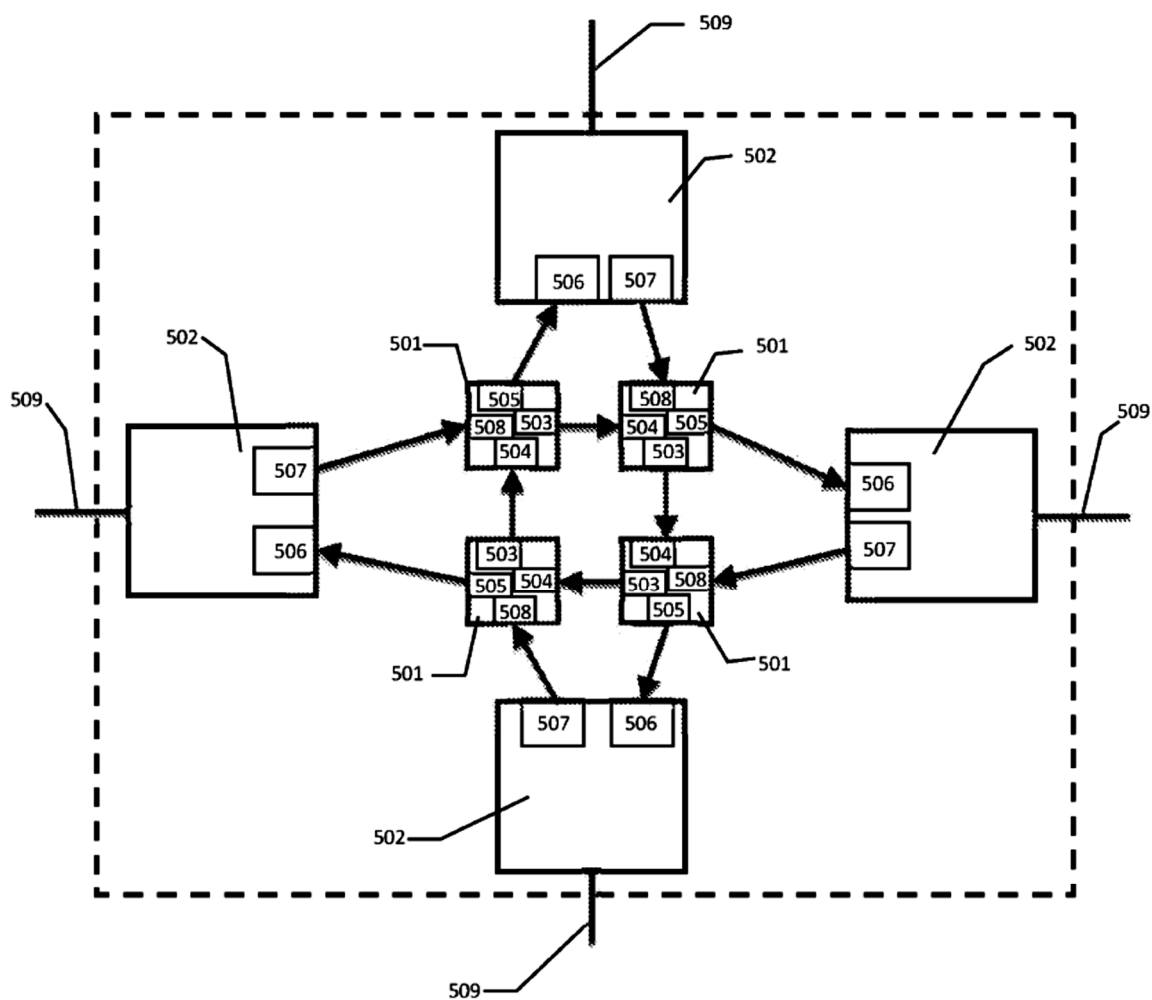


Fig. 5