(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 654 165**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.03.2015 E 15161362 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.10.2017 EP 3073701**

(54) Título: **Entidad de protección de red y método para proteger una red de comunicación contra mensajes fraudulentos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.02.2018

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

VAN DEN BERGE, FRIDTJOF

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Entidad de protección de red y método para proteger una red de comunicación contra mensajes fraudulentos

Campo técnico

La presente divulgación se refiere a una entidad de protección de red para proteger una red de comunicación contra los mensajes fraudulentos y a un método para proteger una red de comunicación contra los mensajes fraudulentos.

Antecedentes

Los mensajes fraudulentos contra las redes de comunicación han aumentado de manera constante durante las últimas décadas. Actualmente, hay alrededor de 195 países o estados soberanos en todo el mundo con un potencial para crecer en número a medida que surgen conflictos étnicos y políticos en las últimas décadas en todo el mundo. El número de redes tanto de proveedores como de destino está creciendo continuamente, ya que, por ejemplo, las nubes de datos se inician en parte por nuevos conglomerados. El crecimiento del tráfico IP generado y/o destinado a dispositivos móviles aumentará drásticamente en los próximos años. Como la seguridad en los dispositivos de mano es muy propensa a los ataques, muchos de los (nuevos) ataques se producen de nuevas maneras y en personas y/o institutos que tienen plena confianza en no ser blanco de ataques en sus cuentas. Solo en los últimos cinco años, el aumento de la criminalidad IP en Alemania aumentó en un 50 por ciento. Debido, por ejemplo, al anonimato HTTP existente en IPv4, respectivamente en la RFC 4941 para las extensiones de privacidad de las direcciones IPv6 sin estado no se establecen “guardianes” ni puede esperarse una mejora. Ni la transparencia en las direcciones IP, ni una prevención total o incluso el seguimiento de la criminalidad IP por parte de la fiscalía nacional se esperan en un futuro cercano.

El documento US 2012/0023593 A1 describe un sistema y un método para filtrar el contenido de Internet y el bloqueo de sitios web no deseados mediante un dispositivo de red segura.

Existe una necesidad de una mejor protección de las redes de comunicación contra los mensajes fraudulentos de los usuarios criminales.

Sumario

Es el objeto de la invención proporcionar tal protección de las redes de comunicación contra los mensajes fraudulentos.

Este objeto se logra mediante las características de las reivindicaciones independientes. Otras formas de implementación son evidentes a partir de las reivindicaciones dependientes, la descripción y las figuras.

La idea esencial de la invención es evitar fraudes IP y de puerto a partir de atacar una red de comunicación proporcionando a una entidad de protección de red, por ejemplo, una pasarela o un encaminador periférico de proveedor de la red de comunicación que recolecta su propia inteligencia en qué direcciones IP y números de puerto de los mensajes de comunicación para un destino dentro de la red de recepción (es decir, la red de comunicación mencionada anteriormente de la que es responsable la pasarela o el encaminador periférico de proveedor) entrarían normalmente la pasarela o el encaminador periférico de proveedor en qué interfaces y troncales. Los detalles de estos mensajes de comunicación pueden almacenarse en tablas dentro del almacenamiento de la entidad de protección de red para detectar los mensajes fraudulentos y evitar que estos mensajes fraudulentos entren en la red de comunicación. Las tablas pueden renovarse en intervalos de tiempo para permitir alteraciones en las configuraciones de direcciones IP dinámicas. Las tablas mencionadas anteriormente se establecerán enviando todas las combinaciones posibles de direcciones IP y números de puerto con un campo de tiempo de vida que se establece en uno, por lo tanto, hasta el próximo salto. Con este principio, la entidad de protección de red establecerá la interfaz y el enlace troncal adecuados para cada dirección IP y número de puerto específicos en su tabla. Todos los paquetes para una conexión, es decir, la dirección IP con el número de puerto de un origen a una dirección IP y el número de puerto del destino siempre usan la misma ruta, tanto entrando como saliendo.

Cuando se usa una configuración de este tipo de la entidad de protección de red o método con preferencia en la periferia del proveedor de su red, el fraude IP realizado de cualquier manera anónima y por lo tanto difícil de juzgar mediante un enjuiciamiento extranjero en la mayoría de los casos, se extinguiría como una forma de enviar software perjudicial, tal como un virus, a usuarios no conscientes, ya que todo el tráfico IP que no entre en la interfaz y el troncal correctas de la entidad de protección de red se eliminará en consecuencia y por lo tanto no entra en la red de destino para el tráfico. Al implementar estas entidades de protección de red o los métodos correspondientes en las redes, las transferencias de IP intencionalmente maliciosas a otros usuarios solo pueden realizarse con éxito usando puertos y direcciones IP reales. Como tal sería el caso, cada daño individual, de cualquier forma, puede investigarse más fácilmente y llevarse más rápido y con una mayor probabilidad de éxito a la justicia, como es ahora el caso en general.

Con el fin de describir la invención en detalle, se usarán los siguientes términos, abreviaturas y notaciones:

HPLMN: red móvil terrestre pública doméstica
IP: protocolo de Internet
ISO: organización de normalización internacional
ISP: proveedor de servicios de Internet
OSI: modelo de interconexión de sistemas abiertos
PE: periferia de proveedor; la periferia de una red
TTL: tiempo de vida

Los métodos y dispositivos de acuerdo con la divulgación pueden estar configurados para proporcionar una inspección OSI capa 2 de paquetes de datos o tramas de datos. El modelo de referencia OSI capa 2 (oficialmente conocido como norma ISO 1984, 7498-1:1994 y norma CCITT X.200) fue desarrollado por la Junta de arquitectura de Internet y redactado por el IETF. OSI capa 2, especifica la capa de enlace de datos para una transmisión de datagramas segura y sin fallos de datagramas. En esta capa, los paquetes de datos se codifican y decodifican en bits. Proporciona conocimiento y gestión del protocolo de transmisión y maneja los errores en la capa física, el control de flujo y la sincronización de tramas. La capa de enlace de datos se divide en dos subcapas: la capa de control de acceso al medio (MAC) y la capa de control de enlace lógico (LLC). La subcapa MAC controla cómo un ordenador en la red obtiene acceso a los datos y permiso para transmitirlos. La capa LLC controla la sincronización de tramas, el control de flujo y la comprobación de errores.

Los métodos y dispositivos de acuerdo con la divulgación pueden usar una tabla apropiada (o simplemente una tabla) para indicar una dirección de origen dedicada y un número de puerto dedicado a la interfaz física y al troncal de conexión asociado a un destino dentro de la red de recepción. En lo sucesivo en el presente documento, como medio apropiado puede usarse cualquier tabla que sea apropiada o adecuada o adaptada para almacenar una dirección de origen dedicada y un número de puerto dedicado para la interfaz física y el troncal de conexión asociado. La tabla puede ordenarse como una matriz dinámica, como una tabla simple que incluye columnas y filas o como cualquier otro tipo de estructura de memoria utilizable para ese fin. La tabla puede adaptarse para almacenar un mapeo de la dirección de origen dedicada y el número de puerto dedicado a la interfaz física y al troncal de conexión asociado.

Lo siguiente se escribe sin la adición de que un mensaje enviado a la red de recepción está destinado a la recepción por una dirección IP y un número de puerto del destino.

Todos los paquetes para una conexión, es decir, la dirección IP con el número de puerto de un origen para una dirección IP y un número de puerto de destino siempre usan la misma ruta, tanto entrando como saliendo.

De acuerdo con un primer aspecto, la invención se refiere a una entidad de protección de red para proteger una red de comunicación contra los mensajes fraudulentos, comprendiendo el elemento de protección de red: una interfaz física y una línea de conectividad con sus posiblemente varios troncales definidos asociados a la interfaz física y configurada para recibir un mensaje de comunicación, comprendiendo el mensaje de comunicación una dirección de origen de mensaje y un número de puerto. La entidad de protección de red incluye además un almacenamiento para el almacenamiento de la tabla apropiada mencionada anteriormente, la tabla apropiada indica solo una dirección de origen dedicada con un puerto a la interfaz física con un troncal de la entidad de protección de red; y un procesador configurado para recuperar la al menos una dirección de origen permitida con el número de puerto del almacenamiento y para comparar la dirección de origen de mensaje y su puerto con la única dirección IP de origen dedicada con un puerto dedicado, en el que el procesador está además configurado para descartar el mensaje de comunicación si la dirección de origen de mensaje y el puerto difieren de la entidad de entrada almacenada de la interfaz y el troncal para la dirección IP y el puerto específicos, bajo los que entró el datagrama en la entidad de protección de red.

Esto se consigue proporcionando a la entidad de protección de red, por ejemplo, una pasarela o encaminador en la periferia del proveedor de la red de comunicación que recolecta su propia inteligencia en qué direcciones de origen de mensaje y puertos de los mensajes de comunicación introducirían normalmente la entidad de protección de red en qué interfaz física y troncal específico. Los detalles de estos mensajes de comunicación se almacenan en la tabla apropiada dentro del almacenamiento de la entidad de protección de red para detectar los mensajes fraudulentos y evitar que estos mensajes fraudulentos entren en la red de comunicaciones simplemente descartando los mensajes de comunicación cuya dirección de origen de mensaje con el puerto difieren de la dirección(es) de origen permitida con el puerto apropiado para la interfaz física con un troncal de la entidad de protección de red almacenada en la tabla apropiada.

En una forma de implementación de acuerdo con el primer aspecto, el procesador está configurado para crear el contenido de la tabla apropiada basándose en los mensajes IP que se han enviado para llenar la tabla mencionada anteriormente a través de la interfaz física y el troncal, en el que los mensajes IP enviados para llenarla tienen un campo de tiempo de vida que se establece en uno.

Esto proporciona la ventaja de que una relación de confianza puede iniciarse almacenando solo aquellos mensajes de comunicación específicos en la tabla apropiada enviando los mensajes mencionados anteriormente con un campo de tiempo de vida (TTL) establecido en uno. En el otro extremo, la recepción, al final de la transmisión un campo de TTL = 1 indica al nodo receptor que el mensaje llegó desde el último salto al nodo y con eso el TTL = 1 se convierte en el TTL = 0 y se descartará.

En una forma de implementación de acuerdo con el primer aspecto, la interfaz física comprende un troncal de conexión configurado para recibir el mensaje de comunicación; y la tabla apropiada indica la al menos una dirección IP de origen permitida con un puerto específico para una combinación de la interfaz física y el troncal de conexión en la que un datagrama de ese tipo debería entrar en la entidad de protección de red.

Cuando la tabla apropiada almacena direcciones IP de origen permitidas con los puertos específicos para una combinación de una interfaz física y el troncal de conexión asociado en esa interfaz física, la detección y la defensa contra los mensajes fraudulentos puede mejorarse adicionalmente debido a que se requiere un mayor grado de información de configuración. En casos extremos, el atacante para provocar daño(s) requiere más información y visión de la configuración específica de la pasarela/encaminador para generar mensajes fraudulentos para un solo ataque específico en cualquier forma a través de un datagrama que pueda pasar a la entidad de protección de red.

En una forma de implementación de acuerdo con el primer aspecto, la dirección de origen de mensaje del mensaje de comunicación comprende una dirección IP de origen y un número de puerto; y la tabla apropiada indica una combinación permitida de una dirección IP de origen y un número de puerto para la combinación de la interfaz física y el troncal de conexión.

Cuando la tabla apropiada almacena combinaciones de direcciones de origen/puertos permitidas para las combinaciones existentes de combinaciones de interfaz física/troncal de conexión, puede realizarse una protección aún mejor contra los mensajes fraudulentos debido a que se requiere un grado aún mayor de información de configuración, como por preferencia solo la red de destino y sus administradores tienen en este caso los conocimientos necesarios sobre una configuración de cada entidad de protección de red. El atacante debería saber qué direcciones de origen y números de puerto se transmiten en qué interfaces físicas y troncales de conexión de una entidad de protección de red específica, de acuerdo con cada ruta diferente a través de Internet, ya que pueden existir varias rutas desde un origen a un destino. Por lo tanto, sería extremadamente difícil y también consumiría mucho más tiempo generar mensajes fraudulentos que puedan pasar la solución de entidad de protección de red descrita en este caso para evitar el fraude IP en la propia red.

En una forma de implementación de acuerdo con el primer aspecto, la dirección de origen de mensaje con el puerto del mensaje de comunicación comprende además una máscara de red, un número de bytes para la unidad de transmisión máxima y la información de velocidad; y la tabla apropiada indica una combinación permitida de una dirección IP de origen y un número de puerto para la combinación de la interfaz física y el troncal de conexión. Por ejemplo, una máscara de red, un número de bytes para la unidad de transmisión máxima y la información de velocidad, que también están en la cabecera IP de un datagrama no se comprueban para el método de prevención de fraude IP descrito en el presente documento.

Cuando la tabla apropiada permite solo los parámetros específicos almacenados en las combinaciones de dirección de origen, número de puerto, máscara de red, número de bytes para la unidad de transmisión máxima e información de velocidad, etc., en una cabecera IP para las combinaciones específicas de la interfaz física y el troncal de conexión puede realizarse un alto grado de protección contra los mensajes fraudulentos debido a que se requiere una gran cantidad de información de configuración en función de las posibles variantes de conectividad de las posibles entidades de protección multirred. El atacante tiene que saber por qué enrutamiento qué dirección IP de origen y número de puerto, con además, por ejemplo, una máscara de red, un número de bytes para la unidad de transmisión máxima y la velocidad se usan para la transmisión en qué combinación de interfaz física y troncal de conexión en una entidad de protección de red específica. Por lo tanto, es muy difícil generar mensajes fraudulentos con el uso de parámetros de origen no correctos que pueden pasar a las posibles entidades de protección multirred.

En una forma de implementación de acuerdo con el primer aspecto, el procesador está configurado para renovar la tabla apropiada sobre una base de intervalo de tiempo con el fin de permitir que los mensajes de comunicación válidos, cuyas direcciones de origen de mensaje se cambian dinámicamente, entren en la red de comunicación.

Las tablas pueden renovarse en intervalos de tiempo para permitir la configuración de direcciones IP dinámica, por ejemplo, para permitir la configuración DHCP de las direcciones IP o para permitir el HTTP-anónimo en IPv4, respectivamente en la RFC 4941 para las extensiones de privacidad de las direcciones IPv6 sin estado.

En una forma de implementación de acuerdo con el primer aspecto, el procesador está configurado para recuperar la dirección de origen de mensaje y el número de puerto del mensaje de comunicación basándose en la inspección OSI capa 2.

Esto proporciona la ventaja de que OSI capa 2 (o capa de enlace de datos) es una capa baja en el modelo de referencia ISO-OSI; por lo tanto, la complejidad computacional para la inspección de los paquetes de datos en esa segunda capa es baja. Por lo tanto, la complejidad computacional para el procesador que implementa la inspección OSI capa 2 es baja, lo que da como resultado una ejecución rápida de cada inspección en la que se realiza la comprobación de la dirección de origen con el puerto.

En una forma de implementación de acuerdo con el primer aspecto, el procesador está configurado además para establecer una alarma antes de descartar el mensaje de comunicación cuando la dirección IP de origen de mensaje y/o el número de puerto del mensaje de comunicación difieren (s) de la interfaz y el ID de troncal en su tabla apropiada a la forma en que entró en la entidad de protección de red desde Internet para una transmisión posterior a su destino.

Esto proporciona la ventaja de que la detección de un mensaje fraudulento y su dirección de origen con el puerto puede protocolizarse y el agresor tiene que dar marcha atrás.

En una forma de implementación de acuerdo con el primer aspecto, la entidad de protección de red comprende una interfaz de configuración para llenar la tabla apropiada con valores configurables.

Esto proporciona la ventaja de que la tabla apropiada puede llenarse manualmente por un operador o automáticamente tras una solicitud.

En una forma de implementación de acuerdo con el primer aspecto, la entidad de protección de red es uno de entre una pasarela, un responsable de un encaminador periférico de proveedor.

Esto proporciona la ventaja de que una pasarela, un responsable de un encaminador periférico de proveedor que se usa para gestionar una red de comunicación pueden usarse para implementar la entidad de protección de red. Por lo tanto, no se deben instalar nuevos elementos de red, sino que solo debería implementarse una mejora para la característica descrita en este caso.

De acuerdo con un segundo aspecto, la invención se refiere a un método para proteger una red de comunicación contra los mensajes fraudulentos que vienen a la red, comprendiendo el método: recibir un mensaje de comunicación a través de una interfaz física y un troncal, comprendiendo el mensaje de comunicación una dirección de origen de mensaje con un número de puerto; proporcionar una tabla apropiada, indicando la tabla apropiada al menos una dirección IP de origen permitida con un número de puerto específico para la interfaz física y el troncal; recuperar la al menos una dirección de origen permitida de la tabla apropiada y comparar la dirección de origen de mensaje con la al menos una dirección de origen permitida; y descartar el mensaje si la dirección de origen de mensaje difiere de la única dirección de origen dedicada con un puerto para la interfaz física con un troncal de la entidad de protección de red.

Un método de protección de red de este tipo proporciona una mejor protección de las redes de comunicación contra los mensajes fraudulentos de los usuarios criminales. Esto se consigue proporcionando una tabla apropiada para recopilar su propia inteligencia, en qué direcciones de origen de mensaje de los mensajes de comunicación se recibirían normalmente en qué interfaz física y troncal. Los detalles de estos mensajes de comunicación se almacenan en la tabla apropiada para detectar los mensajes fraudulentos y evitar que estos mensajes fraudulentos entren en la red de comunicaciones simplemente descartando los mensajes de comunicación cuya dirección de origen de mensaje y número de puerto difieran de su entrada en la entidad de protección de red, la interfaz y el troncal adecuados almacenados para la dirección IP y el número de puerto usados del mensaje en la tabla apropiada.

En una implementación de acuerdo con el segundo aspecto, el método comprende: proporcionar la tabla apropiada basándose en el encaminamiento IP de los mensajes enviados a través de la interfaz física y el troncal apropiados, en la que los mensajes IP tienen un campo de tiempo de vida que está establecido en uno.

Esto proporciona la ventaja de que puede iniciarse una relación de confianza almacenando solo aquellos mensajes de comunicaciones específicos para el encaminamiento IP en la tabla apropiada que se han reunido enviando mensajes idénticos en los que el campo de tiempo de vida (TTL) se establece en uno. Un campo de TTL = 1 de este tipo indica al nodo receptor que el mensaje llegó desde el último salto al nodo y con eso el TTL = 1 se convierte en el TTL = 0 y se descartará.

En una forma de implementación de acuerdo con el segundo aspecto, el método comprende: recibir el mensaje de comunicación a través de un troncal de conexión de la interfaz física; y proporcionar la tabla apropiada que indique la al menos una dirección IP de origen permitida con un puerto específico para una combinación de la interfaz física y el troncal de conexión en la que un datagrama de ese tipo debe entrar en la entidad de protección de red.

Cuando la tabla apropiada almacena las direcciones IP de origen permitidas con los puertos específicos para una combinación de una interfaz física y el troncal de conexión asociado en esa interfaz física, la detección y la defensa

contra los mensajes fraudulentos puede mejorarse adicionalmente debido a que se requiere un mayor grado de información de configuración. En casos extremos, el atacante para provocar daño(s) requiere más información y visión de la configuración específica de pasarela/encaminador para generar mensajes fraudulentos para un solo ataque específico en cualquier forma a través de un datagrama que puede pasar el método de protección.

En una forma de implementación de acuerdo con el segundo aspecto, el método comprende: recibir el mensaje de comunicación, la dirección de origen de mensaje del mensaje de comunicación que comprende una dirección IP de origen y un número de puerto; y descartar el mensaje de comunicación si la dirección IP de origen y el número de puerto difieren de una combinación permitida de una dirección IP de origen y un número de puerto para una combinación de la interfaz física y el troncal de conexión.

Cuando la tabla apropiada almacena las combinaciones permitidas de direcciones de origen/puertos para las combinaciones existentes de combinaciones interfaz física/troncal de conexión, puede realizarse una aún mejor protección contra los mensajes fraudulentos debido a que se requiere un grado aún mayor de información de configuración, como por preferencia solo la red de destino y sus administradores tienen en este caso los conocimientos necesarios sobre una configuración de cada entidad de protección de red. El atacante debería saber qué direcciones de origen y números de puerto se transmiten en qué interfaces físicas y troncales de conexión de una entidad de protección de red específica, de acuerdo con cada ruta diferente a través de Internet, ya que pueden existir varias rutas desde un origen a un destino. Por lo tanto, sería extremadamente difícil y también consumiría mucho más tiempo generar mensajes fraudulentos que puedan pasar la solución de entidad de protección de red descrita en este caso para evitar el fraude IP en la propia red.

Un código de programa de este tipo puede implementarse fácilmente en una pasarela existente responsable de un encaminador periférico de proveedor y actualizar estos dispositivos a entidades de protección de red de acuerdo con la divulgación.

Breve descripción de los dibujos

Se describirán unas realizaciones adicionales de la invención con respecto a las siguientes figuras, en las que:

La figura 1 muestra un diagrama de bloques que ilustra una entidad de protección de red 100 para proteger una red de comunicación contra los mensajes fraudulentos en un modo operativo de acuerdo con una forma de implementación;

La figura 2 muestra un diagrama de bloques que ilustra la entidad de protección de red 100 mostrada en la figura 1 en un modo de configuración para reunir el parámetro de interfaz y troncal con las direcciones IP y los puertos de acuerdo con una forma de implementación.

La figura 3 muestra una vista tridimensional de una pasarela 300 como una implementación de una entidad de protección de red de acuerdo con una forma de implementación.

La figura 4 muestra un diagrama de bloques que ilustra un sistema de comunicación 400 que comprende una red de comunicación doméstica protegida por una entidad de protección de red 100 contra los mensajes fraudulentos de acuerdo con una forma de implementación; y

La figura 5 muestra un diagrama esquemático que ilustra un método 500 para proteger una red de comunicación contra los mensajes fraudulentos de acuerdo con una forma de implementación.

Descripción detallada de las realizaciones

En la siguiente descripción detallada, se hace referencia a los dibujos adjuntos, que forman una parte de la misma, y en los que se muestra a modo de ilustración unos aspectos específicos en los que la divulgación puede practicarse. Se entiende que pueden usarse otros aspectos y pueden realizarse cambios estructurales o lógicos sin alejarse del alcance de la presente divulgación. La siguiente descripción detallada, por lo tanto, no debe tomarse en un sentido limitativo, y el alcance de la presente divulgación está definido por las reivindicaciones adjuntas.

Se entiende que los comentarios hechos en relación con un método descrito también pueden ser ciertos para un dispositivo o sistema correspondiente configurado para realizar el método, y viceversa. Por ejemplo, si se describe una etapa de método específica, un dispositivo correspondiente puede incluir una unidad para realizar la etapa de método descrita, incluso si dicha unidad no se describe o se ilustra explícitamente en las figuras. Además, se entiende que las características de los diversos aspectos a modo de ejemplo descritos en el presente documento pueden combinarse entre sí, a menos que se indique específicamente lo contrario.

En la siguiente descripción, se describen los métodos y los dispositivos para proteger las redes de comunicación contra los mensajes fraudulentos. Los dispositivos y los sistemas descritos apuntan a funcionalidades, pero pueden denominarse de manera diferente en función de, por ejemplo, el fabricante y el estado de desarrollo de tales nodos,

pueden incluir circuitos integrados y/o pasivos y pueden fabricarse de acuerdo con diversas tecnologías. Por ejemplo, los circuitos pueden incluir circuitos integrados lógicos, circuitos integrados analógicos, circuitos integrados de señales mixtas, circuitos ópticos, circuitos de memoria y/o pasivos integrados.

En la siguiente descripción, se describen los métodos y dispositivos para explotar el campo de mensaje de tiempo de vida de los mensajes de comunicación, en particular los mensajes IP. El tiempo de vida (TTL) o el límite de salto es un mecanismo que limita la vida útil o el tiempo de vida de los datos en un ordenador o red. El TTL puede implementarse como un contador o una marca de tiempo adjunta a o incrustada en los datos. Una vez que ha transcurrido el recuento de eventos prescritos o el intervalo de tiempo, los datos se descartan. El TTL evita que un paquete de datos circule indefinidamente. El TTL describe además una relación de proximidad entre dos entidades de red. Una reducción del TTL archivado caracteriza una distancia (en tiempo o espacio) entre dos entidades de red.

En el marco del protocolo de Internet (IP), el TTL es un campo de 8 bits. En la cabecera IPv4, el TTL es el noveno octeto de 20. En la cabecera IPv6, el TTL es el octavo octeto de 40. El valor máximo de TTL es 255, el valor máximo de un solo octeto. El valor de tiempo de vida puede representar un límite superior en el tiempo que un datagrama IP puede existir en un sistema de Internet. El remitente del datagrama establece el campo de TTL y cada encaminador de la ruta lo reduce hasta su destino. El objetivo del campo de TTL es evitar una situación en la que un datagrama que no puede entregarse circule en un sistema de Internet con el fin de proporcionar un rendimiento estable. En el marco de IPv4, el tiempo de vida se mide en segundos; cada host que pasa el datagrama debe reducir el TTL en al menos una unidad. En la práctica, sin embargo, el campo de TTL se reduce en uno en cada salto. Para reflejar esta práctica, el campo se renombra como límite de salto en IPv6.

En la siguiente descripción, se describen los métodos y dispositivos que se basan en troncales o troncales de conexión. La troncalización se conoce como un método para proporcionar acceso de red a muchos clientes compartiendo un conjunto de líneas o accesos en lugar de proporcionarlos individualmente. Un troncal puede definirse como una línea de comunicación punto a punto permanente entre dos puertos de una entidad de comunicación, por ejemplo, una pasarela. En el contexto de Ethernet, la expresión troncalización de Ethernet especifica el transporte de múltiples VLAN (redes de área local virtuales) a través de un único enlace de red a través de un protocolo de troncalización. Para permitir múltiples VLAN en un enlace, se identifican las tramas de las VLAN individuales.

La figura 1 muestra un diagrama de bloques que ilustra una entidad de protección de red 100 para proteger una red de comunicación contra los mensajes fraudulentos en un modo de funcionamiento de acuerdo con una forma de implementación.

La entidad de protección de red 100 incluye una interfaz física 101, FE0, un almacenamiento 103 y un procesador 107. La interfaz física 101, FE0 está configurada para recibir un mensaje de comunicación 102. El mensaje de comunicación 102 incluye una dirección de origen de mensaje X. El almacenamiento 103 se usa para almacenar una tabla apropiada 105. La tabla apropiada 105 indica al menos una dirección de origen permitida A para la interfaz física 101, FE0. El procesador 107 está configurado para recuperar las una o más direcciones de origen permitidas A del almacenamiento 103 y para comparar la dirección de origen de mensaje X con las una o más direcciones de origen permitidas A. El procesador 107 está configurado además para descartar el mensaje de comunicación 102 si la dirección de origen de mensaje X difiere de la al menos una dirección de origen permitida A. El procesador 107 puede crear la tabla apropiada 105 basándose en los mensajes IP recibidos a través de la interfaz física 101, FE0, mensajes IP en los que un campo de tiempo de vida se estable en uno, por ejemplo, como se describe a continuación con respecto a la figura 2. La interfaz física 101, FE0 puede incluir un troncal de conexión configurado para recibir el mensaje de comunicación 102. La tabla apropiada 105 puede indicar la al menos una dirección de origen permitida A para una combinación de la interfaz física 101, FE0 y el troncal de conexión.

La dirección de origen de mensaje X del mensaje de comunicación 102 puede incluir una dirección IP de origen y un número de puerto. La tabla apropiada 105 puede indicar una combinación permitida de una dirección IP de origen y un número de puerto para la combinación de la interfaz física 101, FE0 y el troncal de conexión. La dirección de origen de mensaje X del mensaje de comunicación 102 puede incluir además una máscara de red, un número de bytes para la unidad de transmisión máxima y la información de velocidad. La tabla apropiada 105 puede indicar una combinación permitida de una dirección IP de origen, un número de puerto, una máscara de red, un número de bytes para la unidad máxima de transmisión y una información de velocidad para la combinación de la interfaz física 101, FE0 y el troncal de conexión.

El procesador 107 puede renovar la tabla apropiada 105 sobre una base de intervalo de tiempo con el fin de permitir que los mensajes de comunicación válidos 102, cuyas direcciones de origen de mensaje X se cambian dinámicamente, entren en la red de comunicación. El procesador 107 puede configurarse para recuperar la dirección de origen de mensaje X del mensaje de comunicación 102 basándose en la inspección OSI de capa 2.

El procesador 107 puede establecer una alarma antes de descartar el mensaje de comunicación 102 cuando la dirección de origen de mensaje X del mensaje de comunicación 102 difiere de la al menos una dirección de origen

permitida A. La entidad protección de red 100 puede incluir una interfaz de configuración para llenar la tabla apropiada 105 con valores configurables.

La entidad de protección de red 100 puede ser, por ejemplo una pasarela, un encaminador o un encaminador periférico de proveedor.

La entidad de protección de red 100 mostrada en la figura 1 se ilustra en un modo de funcionamiento, es decir, uno o más mensajes de comunicación 102 llegan a la interfaz física 101, FE0 con una dirección de origen X y un puerto P y el procesador 107 comprueba si la dirección de origen X y el número de puerto P del mensaje de comunicación 102 se almacenan junto con un identificador FE0, 101 de la interfaz física FE0 y el troncal de conexión T1 en la tabla apropiada 105 del almacenamiento 103. Si la dirección de origen X y el puerto P se almacenan en la tabla como una entrada permitida para la interfaz FE0 y el troncal de conexión T1, entonces el mensaje de comunicación 102 puede entrar en la red de comunicación (no mostrada en la figura 1, véase la figura 4 por ejemplo), de lo contrario el mensaje de comunicación 102 no puede pasar y puede descartarse. La tabla 105 apropiada puede incluir múltiples direcciones de origen y números de puerto permitidos para las respectivas interfaces físicas y troncales de conexión, por ejemplo, la dirección B con el puerto P2 para la interfaz física FE0 y el troncal de conexión T2 o la dirección C con el puerto P1 para la interfaz física FE1 y el troncal de conexión T1. La tabla apropiada 105 puede incluir múltiples interfaces físicas y múltiples troncales de conexión por interfaz física, por ejemplo, una dirección de origen A y un puerto P1 permitidos para la interfaz física FE0 y el troncal T1, la dirección de origen B y el puerto P2 permitidos para la interfaz física FE1 y el troncal T2, la dirección de origen C y el puerto P1 permitidos para la interfaz física FE1 y el troncal T1, la dirección de origen D y el puerto P3 permitido para la interfaz física GE0 y el troncal T1 como un ejemplo representado en la figura 1.

Mientras que la figura 1 ilustra un modo de funcionamiento de la entidad de protección de red 100 donde la tabla apropiada 105 existe y se llena con información de dirección permitida, la figura 2 ilustra el modo de configuración en el que la entidad de protección de red 100 gana información para llenar la tabla apropiada 105.

La figura 2 muestra un diagrama de bloques que ilustra la entidad de protección de red 100 mostrada en la figura 1 en un modo de configuración de acuerdo con una forma de implementación. La entidad de protección de red 100 mostrada en la figura 2 corresponde a la entidad de protección de red 100 mostrada en la figura 1. La figura 2 ilustra la configuración a modo de ejemplo de la tabla apropiada 105 de acuerdo con un ejemplo. Cuando un mensaje de confianza 202 llega a la interfaz física 101, por ejemplo un mensaje IP que incluye un campo de mensaje, por ejemplo en una cabecera del mensaje IP, que indica un tiempo de vida igual a uno, la entidad de protección de red 100 asume que este mensaje se origina en el siguiente elemento de red, por ejemplo, el próximo encaminador de salto o pasarela, es decir, un elemento de red seguro que no está dañado por un atacante malintencionado. Por lo tanto, la dirección de origen de mensaje de este mensaje de confianza 202 se trata como una dirección de origen válida que puede usarse para llenar la tabla apropiada 105.

El procesador 107 comprueba si un campo de mensaje de TTL se incluye en el mensaje de confianza 202 y si existe una relación de confianza de este tipo, la dirección de origen A y el número de puerto P1 del mensaje de confianza 202 se almacenan junto con el identificador FE0 de la física interfaz 101 y el troncal de conexión T1 en la tabla apropiada 105. Si el mensaje entrante lleva un TTL = 1, se descartará en la medida en que el nodo receptor abstrae el 1 del valor de TTL y no puede reenviar más y se descartará.

Como alternativa, pueden aplicarse otras relaciones de confianza para comprobar si un mensaje 202 se origina a partir de un elemento de red seguro. Por ejemplo, puede usarse incluso un TTL que sea igual a 2 o valores superiores si se conoce la configuración de red. Por ejemplo, si el mensaje pasa una gran cantidad de encaminadores en una red no anónima, tal como por ejemplo, internet, el valor de TTL puede aumentarse mediante el número de elementos de red conocidos que un mensaje tiene que pasar antes de llegar a la interfaz física 101. En lugar del campo de TTL, pueden usarse otros campos de mensaje del mensaje de comunicación que proporcionan una relación de confianza que no puede manipularse, por ejemplo, basándose en una marca de tiempo o en un número de secuencia, etc.

La figura 3 muestra una vista en 3 dimensiones de una pasarela 300 como una implementación de una entidad de protección de red de acuerdo con una forma de implementación. La pasarela 300 es un ejemplo de implementación a modo de ejemplo de una entidad de protección de red 100 como se ha descrito anteriormente con respecto a las figuras 1 y 2. Otros ejemplos son los encaminadores periféricos de proveedor y otras entidades de red con una funcionalidad de encaminamiento en la periferia de una red. La pasarela a modo de ejemplo 300 mostrada en la figura 3 incluye dos interfaces de Ethernet rápida FE0 310, FE1 311, cuatro interfaces serie 0/0 320, 0/1 321, 0/2 322, 0/3 323 de un primer tipo, cuatro interfaces serie 1/0 330, 1/1 331, 1/2 332, 1/3 333 de un segundo tipo y dos interfaces de gestión 341, 342. Por supuesto que cualquier otra configuración de la interfaz puede implementarse.

La pasarela 300 de una red de comunicación comienza con la recolección de su propia inteligencia en qué direcciones IP con qué puertos llegan los mensajes en qué interfaces y troncales. Los detalles de estos, por ejemplo, mensajes desvelados a través de TTL = 1 se almacenan en tablas y se renuevan en las tablas en intervalos de

tiempo para futuras comparaciones. Cada paquete se comprueba en su manera de entrar en la pasarela con una dirección IP y un puerto específicos. Esto se traduce en la interfaz y el troncal en OSI capa 2.
Por ejemplo, el campo de dirección de origen de mensaje “142.213.32.1 1000 1500 80” puede indicar una dirección IPv4 142.213.32.1 255.255.255.252 respectivamente 142.213.32.1/30 con velocidad de 1000 MB/s, unidad de transmisión máxima (MTU) de 1500 bytes y el puerto 80.

La expresión a modo de ejemplo “FE0 9 acceso/arriba” puede indicar la interfaz Ethernet rápida 0/9 en la dirección corriente arriba. La entrada “troncal FE0/22” o “modo de grupo de canal 22” pueden indicar el troncal veintidosavo también denominado como grupo de canal 22.

Si estos parámetros, junto con las direcciones IP y los puertos específicos se establecen en la base de datos, respectivamente, las tablas de la pasarela (o encaminador periférico de proveedor), no se concederá acceso a cualesquiera presuntas direcciones IP y números de puerto, ya que podrían venir en las interfaces y/o troncales equivocadas.

La figura 4 muestra un diagrama de bloques que ilustra un sistema de comunicación 400 que comprende una red de comunicación doméstica protegida por una entidad de protección de red 100 contra los mensajes fraudulentos de acuerdo con una forma de implementación.

El sistema de comunicación 400 incluye una red de comunicación doméstica 420, por ejemplo, una HPLMN (red móvil terrestre pública doméstica) y un ISP (proveedor de servicios de Internet) doméstico, acoplados por una entidad de protección de red, por ejemplo, un dispositivo 100 como se ha descrito anteriormente con respecto a las figuras 1 a 3, por ejemplo, una pasarela o un encaminador, a la Red informática mundial 410 o a otra red de comunicación de transporte. Una pluralidad de redes de proveedor de servicios de Internet (ISP) exteriores 402a, 402b, 402c, 402x están acopladas por sus correspondientes pasarelas 404a, 404b, 404c, 404x de la Red informática mundial 410 para permitir la comunicación con la red de comunicación 420. Cada una de las redes de proveedor de servicios de Internet (ISP) exteriores 402a, 402b, 402c, 402x incluye una pluralidad de terminales de cliente. En la figura 4, la red de proveedor de servicios de Internet (ISP) exterior 402a incluye los terminales de cliente 403a, 405a, 407a; la segunda red de proveedor de servicios de Internet (ISP) exterior 402b incluye los terminales de cliente 403b, 405b, 407b; la tercera red de proveedor de servicios de Internet (ISP) exterior 402c incluye los terminales de cliente 403c, 405c, 407c; y la cuarta red de proveedor de servicios de Internet (ISP) exterior 402x incluye los terminales de cliente 403x, 405x, 407x. Sin embargo, pueden aplicarse cualquier otro número de redes de proveedores de servicios de Internet (ISP) exteriores y cualquier otro número de terminales de cliente correspondiente.

En el sistema de comunicación 400 un terminal, por ejemplo el terminal 407x, representa el atacante malintencionado que está enviando un mensaje fraudulento 430 con contenido perjudicial en la cadena de paquetes de IP bajo la dirección IP falsificada 173.1.121.98 (a modo de ejemplo) y el número de puerto 253 (a modo de ejemplo) a un cliente de la red de comunicación doméstica 420, es decir, a una dirección de destino de uno de los terminales de cliente 423, 425, 427, 429. El mensaje fraudulento 430 pasa a la Red informática mundial 410 y se transporta a la entidad de protección de red 100 que recibe el mensaje fraudulento 430.

Debido a la configuración de la entidad de protección de red 100, como se ha descrito anteriormente con respecto a las figuras 1 a 3, los paquetes de IP bajo la IP falsificada 173.1.121.98 y el número de puerto 253 llegan a la entidad de protección de red 100 en una interfaz y un troncal incorrectos, es decir, una combinación de interfaz y troncal para la que la dirección IP y el número de puerto (173.1.121.98/31 253) no se almacenan en la tabla apropiada. Como consecuencia, el mensaje fraudulento 430 se descarta y no entra en la red de comunicación doméstica 420.

En una implementación a modo de ejemplo, la tabla apropiada de la entidad de protección de red 100 puede incluir una cadena IPv4 bajo “142.213.32.1 1000 1500 80” llegando en la interfaz FE0/9 con un troncal de grupo de canal 22. La misma interfaz con el troncal idéntico también puede presentarse para las otras numerosas direcciones IP y puertos. Sin embargo, no todas las direcciones IP con puertos tienen un mapeo idéntico con el fin de llegar a una carga equilibrada en todas las interfaces y los troncales.

La presunta o falsificada dirección IP IPv4 173.1.121.98 y número de puerto 253 usado por la parte que envía el contenido malicioso hacia un terminal de cliente de la red de comunicación doméstica 420 llegará desde la Internet 410 hacia la entidad de protección de red 100, por ejemplo, desde la pasarela a través de la interfaz FE0/9 y el 22º troncal, que no son los valores almacenados en su base de datos, es decir, la tabla apropiada para la IP 173.1.121.98 con el puerto 253. A medida que el paquete llega en interfaces y/o troncales equivocados, la entidad de protección de red 100 o pasarela descarta el paquete 430. Como se ha descrito anteriormente, la dirección IP y el puerto correctos pueden ser 142.213.32.1 con número de puerto 80, pero no la falsificada 173.1.121.98 con número de puerto 253 bajo los que se envió.

La figura 5 muestra un diagrama esquemático que ilustra un método 500 para proteger una red de comunicación contra los mensajes fraudulentos de acuerdo con una forma de implementación.

El método 500 incluye recibir 501 un mensaje de comunicación a través de una interfaz física, por ejemplo, una interfaz física 101 como se ha descrito anteriormente con respecto a las figuras 1 y 2 o una interfaz física 310, 311, 320, 321, 322, 323, 330, 331, 332, 333 como se ha descrito anteriormente con respecto a la figura 3. El mensaje de comunicación incluye una dirección de origen de mensaje, por ejemplo, una dirección de origen de mensaje X como se ha descrito anteriormente con respecto a la figura 1 y un número de puerto, por ejemplo, un número de puerto P como se ha descrito anteriormente con respecto a la figura 1. El método 500 incluye además: proporcionar 502 una tabla apropiada, por ejemplo una tabla apropiada 105 tal como se ha descrito anteriormente con respecto a las figuras 1 y 2, indicando la tabla apropiada una dirección de origen dedicada y un troncal de conexión dedicado para la interfaz física y el troncal; recuperar 503 la dirección de origen dedicada incluyendo su puerto específico (es decir, dedicado) de la tabla apropiada y comparar la dirección de origen de mensaje y el puerto con la dirección de origen dedicada y el troncal de conexión dedicado, como se describe en el presente documento; y descartar el mensaje 504 si la dirección de origen de mensaje difiere de la dirección de origen dedicada o si el número de puerto difiere del número de puerto dedicado.

El método 500 puede incluir proporcionar 502 la tabla apropiada basándose en los mensajes IP que se envían a través de una interfaz física y el troncal, mensajes IP en los que se establece un campo de tiempo de vida en uno, por ejemplo, como se ha descrito anteriormente con respecto a la figura 2. El método 500 puede incluir recibir 501 el mensaje de comunicación a través de un troncal de conexión de la interfaz física; y proporcionar 502 la tabla apropiada indicando la dirección de origen dedicada para una combinación de la interfaz física y el troncal de conexión, por ejemplo, como se ha descrito anteriormente con respecto a la figura 1. El método 500 puede incluir recibir 502 el mensaje de comunicación, la dirección de origen de mensaje del mensaje de comunicación que comprende una dirección IP de origen y un número de puerto; y descartar 504 el mensaje de comunicación si la dirección IP de origen y el número de puerto difieren de una combinación permitida de una dirección IP de origen y un número de puerto para una combinación de la interfaz física y el troncal de conexión, por ejemplo, como se ha descrito anteriormente con respecto a las figuras 1, 2 y 4.

Los métodos, sistemas y dispositivos descritos en el presente documento pueden implementarse como un circuito eléctrico y/u óptico dentro de un chip o un circuito integrado o un circuito integrado de aplicación específica (ASIC). La invención puede implementarse en una circuitería electrónica u óptica digital y/o analógica.

Los métodos, sistemas y dispositivos descritos en el presente documento pueden implementarse como software en un procesador de señal digital (DSP), en un microcontrolador o en cualquier otro procesador lateral o como un circuito de hardware dentro de un circuito integrado de aplicación específica (ASIC) de un procesador de señal digital (DSP).

La invención puede implementarse en circuitería electrónica digital, o en hardware informático, firmware, software, o en combinaciones de los mismos, por ejemplo, en hardware disponible de dispositivos transceptores ópticos convencionales o en un nuevo hardware dedicado para procesar los métodos descritos en el presente documento.

La presente divulgación también soporta un producto de programa informático que incluye un código ejecutable por ordenador o instrucciones ejecutables por ordenador que, cuando se ejecutan, hacen que al menos un ordenador ejecute las etapas de ejecución y cálculo que se describen en el presente documento, en particular, el método 500 como se ha descrito anteriormente con respecto a la figura 5 y las técnicas descritas anteriormente con respecto a las figuras 1 a 4. Un producto de programa informático de este tipo puede incluir un código de programa de almacenamiento de medio de almacenamiento legible del mismo para su uso por un ordenador. El código de programa puede realizar el método 500 como se ha descrito anteriormente con respecto a la figura 5.

Los siguientes pertenecen a ejemplos específicos de acuerdo con la invención.

El Ejemplo 1 es una entidad de protección de red para proteger una red de comunicación contra los mensajes fraudulentos, comprendiendo el elemento de protección de red: una interfaz física que comprende un troncal de conexión asociado a la interfaz física para recibir un mensaje de comunicación, en la que el mensaje de comunicación comprende una dirección de origen de mensaje y un número de puerto y en la que el mensaje de comunicación se dirige a un destino dentro de la red de comunicación; un almacenamiento para almacenar una tabla apropiada, tabla apropiada que es apropiada para indicar una dirección de origen dedicada y un número de puerto dedicado a la interfaz física y al troncal de conexión asociado; y un procesador configurado para recuperar la dirección de origen dedicada y el número de puerto dedicado del almacenamiento y para comparar la dirección de origen de mensaje con la dirección de origen dedicada y el número de puerto con el número de puerto dedicado, en la que el procesador está configurado además para descartar el mensaje de comunicación si o bien la dirección de origen de mensaje difiere de la dirección de origen dedicada o el número de puerto difiere del número de puerto dedicado.

En el Ejemplo 2, la materia objeto del Ejemplo 1 puede incluir opcionalmente que el procesador esté configurado para crear un contenido de la tabla apropiada basándose en los mensajes IP enviados a través de la interfaz física, mensajes IP en los que el campo de tiempo de vida se establece en uno.

En el Ejemplo 3 la materia objeto de uno cualquiera de los Ejemplos 1-2 puede incluir opcionalmente que la tabla apropiada indique la dirección de origen dedicada y el número de puerto dedicado para una combinación de la interfaz física y el troncal de conexión asociado.

En el Ejemplo 4, la materia objeto del Ejemplo 3 puede incluir opcionalmente que la tabla apropiada indique una combinación permitida de una dirección IP de origen y un número de puerto para la combinación de la interfaz física y el troncal de conexión asociado.

En el Ejemplo 5, la materia objeto del Ejemplo 4 puede incluir opcionalmente que la dirección de origen de mensaje y el número de puerto asociado del mensaje de comunicación comprendan además una máscara de red, un número de bytes para la unidad de transmisión máxima y la información de velocidad; y que la tabla apropiada indique una combinación permitida de una dirección IP de origen y un número de puerto para la combinación de la interfaz física y el troncal de conexión asociado.

En el Ejemplo 6 la materia objeto de uno cualquiera de los Ejemplos 1-5 puede incluir opcionalmente que el procesador esté configurado para renovar la tabla apropiada sobre una base de intervalo de tiempo con el fin de permitir que los mensajes de comunicación válidos, en los que las direcciones de origen mensaje se cambian dinámicamente, entren en la red de comunicación.

En el Ejemplo 7 la materia objeto de uno cualquiera de los Ejemplos 1-6 puede incluir opcionalmente que el procesador esté configurado para recuperar la dirección de origen de mensaje y el número de puerto del mensaje de comunicación basándose en una inspección OSI capa 2.

En el Ejemplo 8 la materia objeto de uno cualquiera de los Ejemplos 1-7 puede incluir opcionalmente que el procesador esté configurado además para establecer una alarma antes de descartar el mensaje de comunicación cuando la dirección de origen de mensaje del mensaje de comunicación difiere de la dirección de origen dedicada o cuando el número de puerto del mensaje de comunicación difiere del número de puerto dedicado.

En el Ejemplo 9 la materia objeto de uno cualquiera de los Ejemplos 1-8 puede incluir opcionalmente una interfaz de configuración para llenar la tabla apropiada con valores configurables.

En el Ejemplo 10 la materia objeto de uno cualquiera de los Ejemplos 1-9 puede incluir opcionalmente que la entidad de protección de red sea uno de entre una pasarela o un encaminador, en particular, un encaminador periférico de proveedor.

Ejemplo 11 es un método para proteger una red de comunicación contra los mensajes fraudulentos, comprendiendo el procedimiento: recibir un mensaje de comunicación a través de un troncal de conexión de una interfaz física, en el que el mensaje de comunicación comprende una dirección de origen de mensaje y un número de puerto y en el que el mensaje de comunicación se dirige a un destino dentro de la red de comunicación; proporcionar una tabla apropiada, tabla apropiada que es apropiada para indicar una dirección de origen dedicada y un número de puerto dedicado a la interfaz física y al troncal de conexión; recuperar la dirección de origen dedicada y el número de puerto dedicado del almacenamiento y comparar la dirección de origen de mensaje con la dirección de origen dedicada y el número de puerto con el número de puerto dedicado; y descartar el mensaje de comunicación si o bien la dirección de origen de mensaje difiere de la dirección de origen dedicada o el número de puerto difiere del número de puerto dedicado.

En el Ejemplo 12 la materia objeto del Ejemplo 11 puede incluir opcionalmente: proporcionar la tabla apropiada basándose en los mensajes IP enviados a través de la interfaz física, mensajes IP en los que un campo de tiempo de vida se establece en uno.

En el Ejemplo 13 la materia objeto de uno cualquiera de los Ejemplos 11-12 puede incluir opcionalmente: proporcionar la tabla apropiada que indica la dirección de origen dedicada y el número de puerto dedicado para una combinación de la interfaz física y el troncal de conexión.

En el Ejemplo 14 la materia objeto del Ejemplo 13 puede incluir opcionalmente: recibir el mensaje de comunicación, la dirección de origen de mensaje del mensaje de comunicación que comprende una dirección IP de origen y un número de puerto; y descartar el mensaje de comunicación si la dirección IP de origen y el número de puerto difieren de una combinación permitida de una dirección IP de origen y un número de puerto para una combinación de la interfaz física y el troncal de conexión.

El Ejemplo 15 es un programa de ordenador que comprende un código de programa para ejecutar el método de acuerdo con uno cualquiera de los Ejemplos 11 a 14 cuando se ejecuta en un ordenador.

Mientras que una característica o aspecto específico de la divulgación puede haberse divulgado con respecto a solo una de varias implementaciones, tal característica o aspecto puede combinarse con una o más de otras características o aspectos de las otras implementaciones como puede ser deseable y ventajoso para cualquier

aplicación dada o específica. Además, en la medida en que los términos “incluir”, “tener”, “con”, u otras variantes de los mismos se usan o en la descripción detallada o en las reivindicaciones, tales términos pretenden ser inclusivos de una manera similar al término “comprender”. Además, los términos “a modo de ejemplo” y “por ejemplo” se entienden simplemente como un ejemplo, en lugar de lo mejor u óptimo. Los términos “acoplado” y “conectado”, junto con sus derivados pueden haberse usado. Debería entenderse que estos términos pueden haberse usado para indicar que dos elementos cooperan o interactúan entre sí sin tener en cuenta si están en contacto físico o eléctrico directo, o no están en contacto directo entre sí.

Aunque se han ilustrado y descrito en el presente documento los aspectos específicos, se apreciará por los expertos en la materia que puede sustituirse una variedad de implementaciones alternativas por los aspectos específicos mostrados y descritos sin apartarse del alcance de la presente divulgación. Esta aplicación se destina a cubrir cualesquiera adaptaciones o variaciones de los aspectos específicos tratados en el presente documento.

Aunque los elementos en las siguientes reivindicaciones se exponen en una secuencia específica con un etiquetado correspondiente, a menos que las recitaciones de reivindicación impliquen de otro modo una secuencia específica para implementar algunos o todos de estos elementos, no se pretende que estos elementos se limiten necesariamente a implementarse en esa secuencia específica.

Muchas alternativas, modificaciones y variaciones serán evidentes para los expertos en la materia a la luz de las enseñanzas anteriores. Por supuesto, los expertos en la materia reconocerán fácilmente que hay numerosas aplicaciones de la invención más allá de las descritas en el presente documento. Aunque la presente invención se ha descrito haciendo referencia a una o más realizaciones específicas, los expertos en la materia reconocen que pueden hacerse muchos cambios en la misma sin alejarse del alcance de la presente invención. Por lo tanto, debe entenderse que dentro del alcance de las reivindicaciones adjuntas, la invención puede ponerse en práctica de otro modo que como se describe específicamente en el presente documento.

REIVINDICACIONES

1. Una entidad de protección de red (100) para proteger una red de comunicación contra los mensajes fraudulentos, comprendiendo el elemento de protección de red (100):

una interfaz física (101, FE0) que comprende un troncal de conexión (T1) asociado a la interfaz física (FE0) para recibir un mensaje de comunicación (102), en la que el mensaje de comunicación (102) comprende una dirección de origen de mensaje (X) y un número de puerto (P) y en la que el mensaje de comunicación se dirige a un destino dentro de la red de comunicación;
un almacenamiento (103) para almacenar una tabla apropiada (105), tabla apropiada (105) que es apropiada para indicar una dirección de origen dedicada (A) y un número de puerto dedicado (P1) para la interfaz física (101, FE0) y el troncal de conexión asociado (T1); y
un procesador (107) configurado para recuperar la dirección de origen dedicada (A) y el número de puerto dedicado (P) del almacenamiento (103) y para comparar la dirección de origen de mensaje (X) con la dirección de origen dedicada (A) y el número de puerto (P) con el número de puerto dedicado (P1), en la que el procesador (107) está configurado además para descartar el mensaje de comunicación (102) si o bien la dirección de origen de mensaje (X) difiere de la dirección de origen dedicada (a) o el número de puerto (P) difiere del número de puerto dedicado (P1),
caracterizado por que el procesador (107) está configurado para crear un contenido de la tabla apropiada (105) basándose en los mensajes IP enviados a través de la interfaz física (101, FE0), mensajes IP en los que un campo de tiempo de vida se ha establecido en uno.

2. La entidad de protección de red (100) de la reivindicación 1,
en la que la tabla apropiada (105) indica la dirección de origen dedicada (A) y el número de puerto dedicado (P) para una combinación de la interfaz física (101, FE0) y el troncal de conexión asociado (T1).

3. La entidad de protección de red (100) de la reivindicación 2,
en la que la tabla apropiada (105) indica una combinación permitida de una dirección IP de origen (X) y un número de puerto (P) para la combinación de la interfaz física (101, FE0) y el troncal de conexión asociado (T1).

4. La entidad de protección de red (100) de la reivindicación 3,
en la que la dirección de origen de mensaje (X) y el número de puerto asociado (P) del mensaje de comunicación (102) comprende además una máscara de red, un número de bytes para la unidad de transmisión máxima y la información de velocidad; y
en la que la tabla apropiada (105) indica una combinación permitida de una dirección IP de origen (X) y un número de puerto (P) para la combinación de la interfaz física (101, FE0) y el troncal de conexión asociado (T1).

5. La entidad de protección de red (100) de una de las reivindicaciones anteriores,
en la que el procesador (107) está configurado para renovar la tabla apropiada (105) sobre una base de intervalos de tiempo con el fin de permitir los mensajes de comunicación válidos (102) cuyas direcciones de origen de mensaje (X) se cambian dinámicamente para entrar en la red de comunicación.

6. La entidad de protección de red (100) de una de las reivindicaciones anteriores,
en la que el procesador (107) está configurado para recuperar la dirección de origen de mensaje (X) y el número de puerto (P) del mensaje de comunicación (102) basándose en una inspección OSI capa 2.

7. La entidad de protección de red (100) de una de las reivindicaciones anteriores,
en la que el procesador (107) está configurado además para establecer una alarma antes de descartar el mensaje de comunicación (102) cuando la dirección de origen de mensaje (X) del mensaje de comunicación (102) difiere de la dirección de origen dedicada (A) o cuando el número de puerto del mensaje de comunicación (102) difiere del número de puerto dedicado (P1).

8. La entidad de protección de red (100) de una de las reivindicaciones anteriores, que comprende:

una interfaz de configuración para llenar la tabla apropiada (105) con valores configurables.

9. La entidad de protección de red (100) de una de las reivindicaciones anteriores,
en la que la entidad de protección de red (100) es uno de entre una pasarela o un encaminador, en particular, un encaminador periférico de proveedor.

10. Un método (500) para proteger una red de comunicación contra los mensajes fraudulentos, comprendiendo el método (500):

recibir (501) un mensaje de comunicación a través de un troncal de conexión (T1) de una interfaz física (101, FE0), en la que el mensaje de comunicación comprende una dirección de origen de mensaje (X) y un número de puerto (P) y en la que el mensaje de comunicación está dirigido a un destino dentro de la red de comunicación;

proporcionar (502) una tabla apropiada (105), tabla apropiada (105) que es apropiada para indicar una dirección de origen dedicada (A) y un número de puerto dedicado (P) para la interfaz física (101, FE0) y el troncal de conexión (T1);
recuperar (503) la dirección de origen dedicada (A) y el número de puerto dedicado (P) del almacenamiento (103) y comparar la dirección de origen de mensaje (X) con la dirección de origen dedicada (A) y el número de puerto (P) con el número de puerto dedicado (P1); y
descartar (504) el mensaje de comunicación (102) si o bien la dirección de origen de mensaje (X) difiere de la dirección de origen dedicada (A) o el número de puerto (P) difiere del número de puerto dedicado (P1),
caracterizado por:

proporcionar (502) la tabla apropiada basándose en los mensajes IP enviados a través de la interfaz física (101, FE0), mensajes IP en los que un campo de tiempo de vida se ha establecido en uno.

11. El método (500) de la reivindicación 10, que comprende:

proporcionar (502) la tabla apropiada que indica la dirección de origen dedicada (A) y el número de puerto dedicado (P) para una combinación de la interfaz física (FE0) y el troncal de conexión (T1).

12. El método (500) de la reivindicación 11, que comprende:

recibir (502) el mensaje de comunicación, la dirección de origen de mensaje del mensaje de comunicación que comprende una dirección IP de origen y un número de puerto; y
descartar (504) el mensaje de comunicación si la dirección IP de origen y el número de puerto difieren de una combinación permitida de una dirección IP de origen y un número de puerto para una combinación de la interfaz física y el troncal conexión.

13. Programa informático que comprende un código de programa para ejecutar el procedimiento de una cualquiera de las reivindicaciones 10 a 12 cuando se ejecuta en un ordenador.

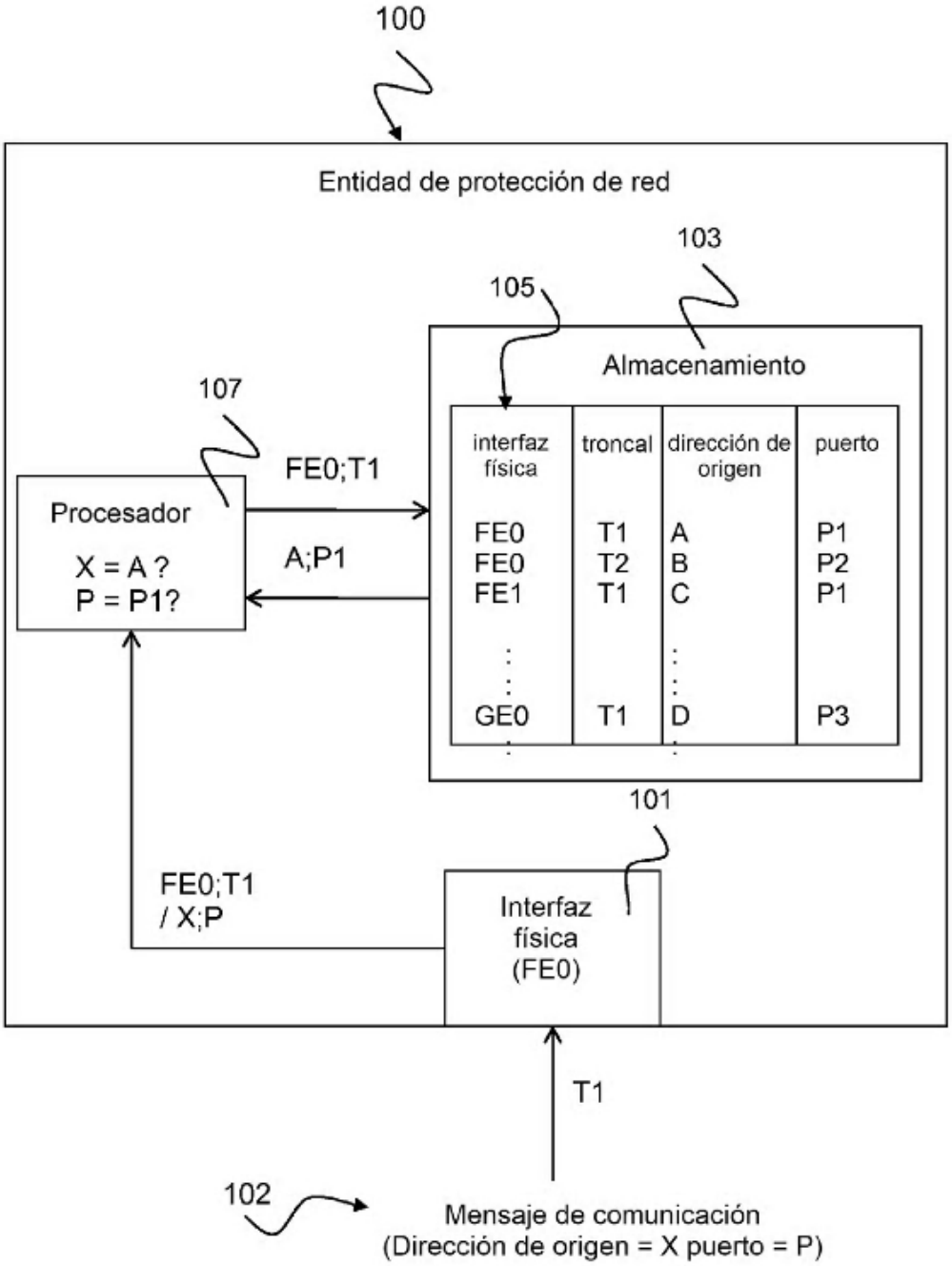
100
Entidad de protección de red
103
105
Almacenamiento
107
interfaz física
troncal
dirección de origen
puerto
FE0;T1
Procesador
X = A ?
P = P1?
A;P1
FE0 T1 A P1
FE0 T2 B P2
FE1 T1 C P1
GE0 T1 D P3
101
FE0;T1
/ X;P
Interfaz física (FE0)
T1
102
Mensaje de comunicación
(Dirección de origen = X puerto = P)

Fig. 1

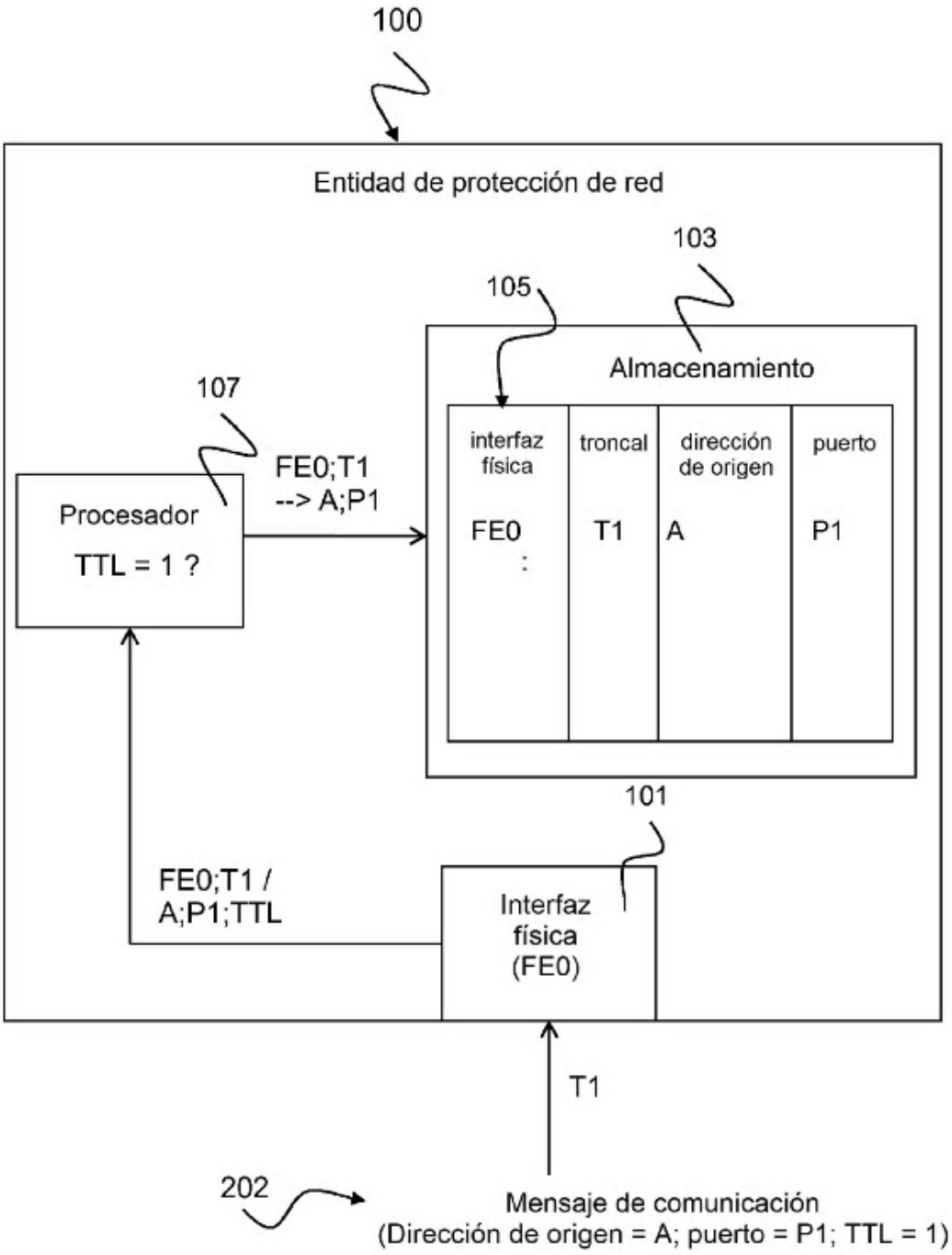
100
Entidad de protección de red
103
105
Almacenamiento
107
interfaz física
troncal
dirección de origen
puerto
FE0;T1
--> A;P1
Procesador
TTL = 1 ?
FE0
T1
A
P1
:
101
FE0;T1 /
A;P1;TTL
Interfaz física (FE0)
T1
202
Mensaje de comunicación
(Dirección de origen = A; puerto = P1; TTL = 1)

Fig. 2

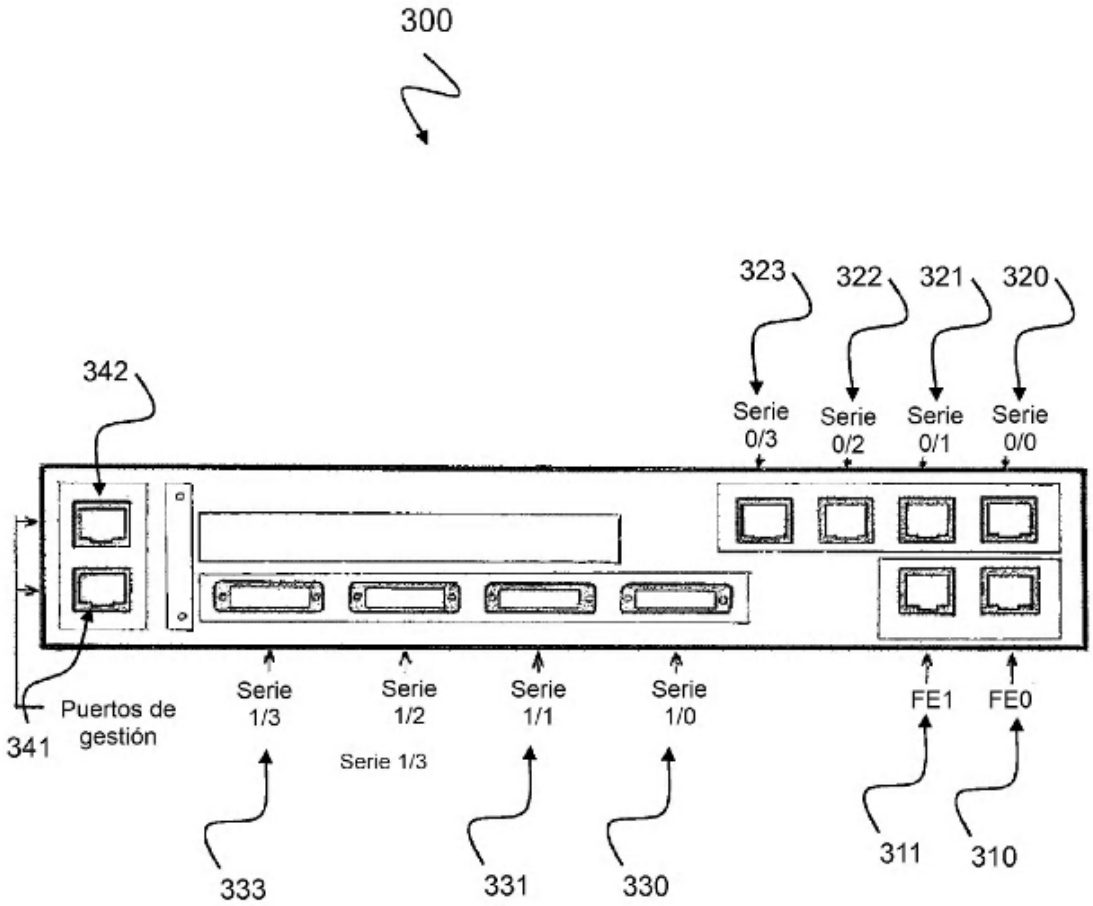
300
323
322
321
320
342
Serie 0/3
Serie 0/2
Serie 0/1
Serie 0/0
Puertos de gestión
341
Serie 1/3
Serie 1/2
Serie 1/1
Serie 1/0
FE1
FE0
Serie 1/3
333
331
330
311
310

Fig. 3

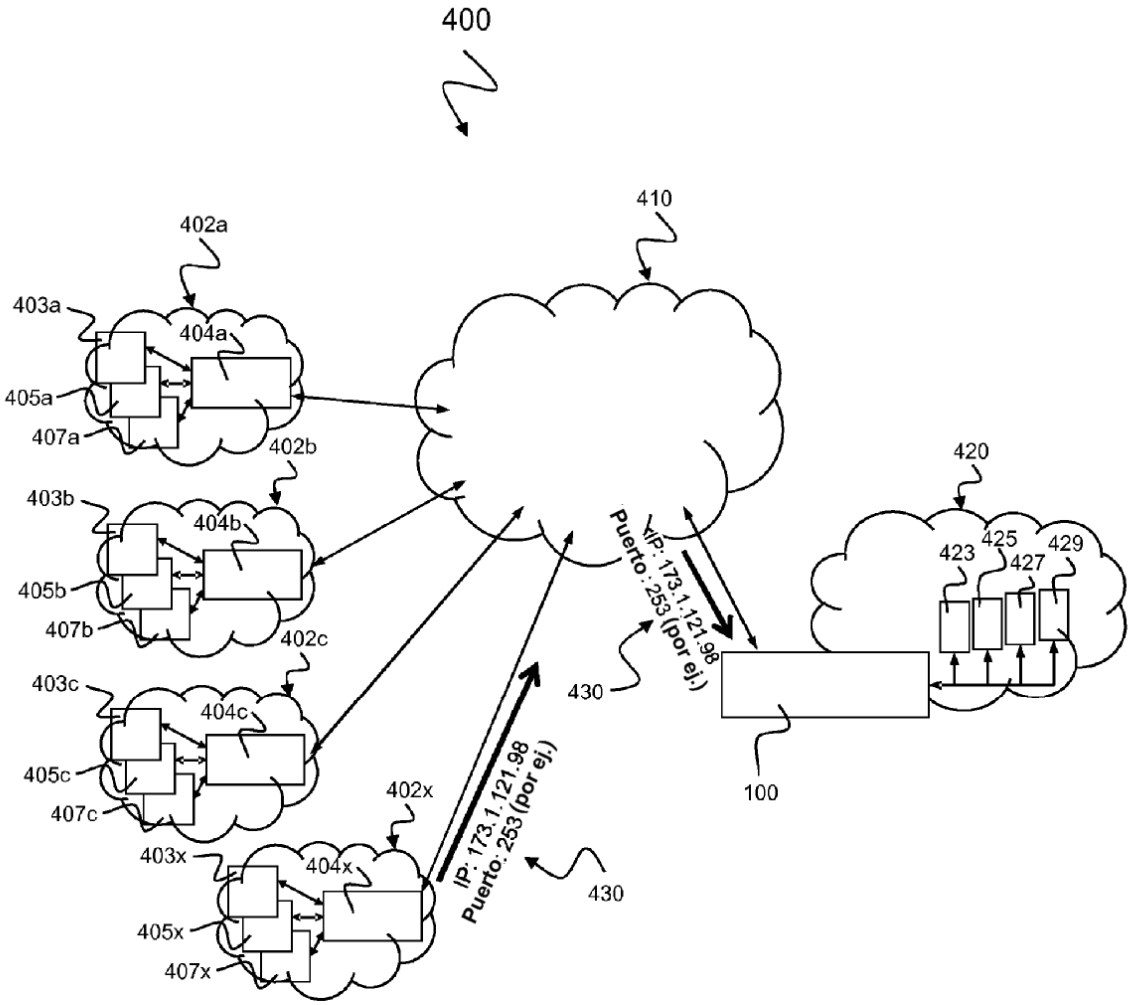
400
410
402a
403a
404a
405a
407a
402b
403b
404b
405b
407b
402c
403c
404c
405c
407c
402x
403x
404x
405x
407x
420
423
425
427
429
100
430
IP: 173.1.121.98
Puerto: 253 (por ej.)
IP: 173.1.121.98
Puerto: 253 (por ej.)
430

Fig. 4

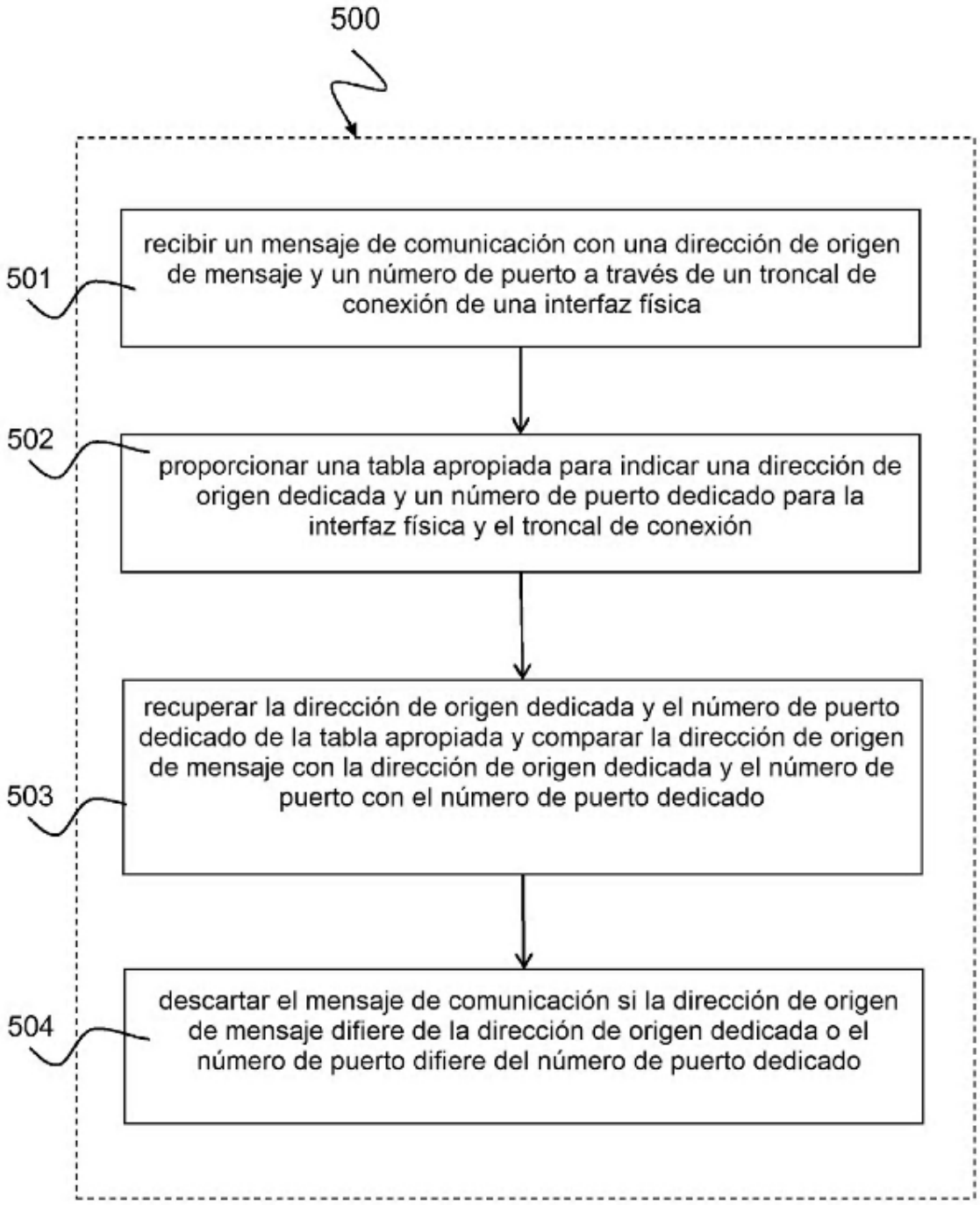
500
recibir un mensaje de comunicación con una dirección de origen de mensaje y un número de puerto a través de un troncal de conexión de una interfaz física
501
proporcionar una tabla apropiada para indicar una dirección de origen dedicada y un número de puerto dedicado para la interfaz física y el troncal de conexión
502
recuperar la dirección de origen dedicada y el número de puerto dedicado de la tabla apropiada y comparar la dirección de origen de mensaje con la dirección de origen dedicada y el número de puerto con el número de puerto dedicado
503
descartar el mensaje de comunicación si la dirección de origen de mensaje difiere de la dirección de origen dedicada o el número de puerto difiere del número de puerto dedicado
504

Fig. 5