(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 652 292**

(51) Int. CI.:

H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.12.2013 PCT/US2013/073679**

(87) Fecha y número de publicación internacional: **12.06.2014 WO14089489**

(96) Fecha de presentación y número de la solicitud europea: **06.12.2013 E 13860780 (9)**

(97) Fecha y número de publicación de la concesión europea: **06.09.2017 EP 2929472**

(54) Título: **Aparato, sistema y procedimiento para la monitorización de red mejorada, comunicación de datos, y proceso de datos**

(30) Prioridad:

07.12.2012 US 201261734909 P
07.12.2012 US 201261734910 P
07.12.2012 US 201261734912 P
07.12.2012 US 201261734915 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.02.2018

(73) Titular/es:

CPACKET NETWORKS, INC. (100.0%)
765 Ravendale Drive
Mountain View, CA 94043, US

(72) Inventor/es:

KAY, RONY

(74) Agente/Representante:

TORNER LASALLE, Elisabet

DESCRIPCIÓN

Aparato, sistema y procedimiento para la monitorización de red mejorada, comunicación de datos, y proceso de datos

Campo de la invención

La presente invención versa, en general, acerca de una monitorización de red y un análisis de datos. Más en particular, la presente invención versa acerca de una monitorización y una búsqueda mejoradas de dispositivos distribuidos por una red, una comunicación y un procesamiento mejorados de datos en red, reduciendo datos para facilitar la identificación y la presentación de variaciones de datos, y una comunicación y una medición mejoradas de datos de rendimiento.

Antecedentes de la invención

El uso generalizado de redes de ordenadores para aumentar la productividad y para facilitar las comunicaciones hace de la monitorización del tráfico de redes, del análisis de redes y de la seguridad de redes inquietudes importantes. La carga de tráfico y el número de flujos de datos que recorren las redes y los centros de datos están aumentando rápidamente, lo que tiene como resultado un número rápidamente creciente de flujos de datos, de servicios, y de contadores de rendimiento que han de ser monitorizados por arquitecturas de gestión de redes. Para algunos flujos de paquetes de datos, puede ser suficiente monitorizar la métrica de rendimiento por flujo, tal como los bytes transmitidos o recibidos, en una granularidad de tiempo de un segundo. Esta es una configuración común para arquitecturas típicas de gestión de redes tales como arquitecturas de protocolo simple de gestión de redes (SNMP). Sin embargo, para otros flujos de paquetes de datos, puede ser importante monitorizar la métrica de funcionamiento por flujo en una granularidad de tiempo más fina, tal como de 1 milisegundo o 10 milisegundos, dado que existen fenómenos que pueden tener un impacto de manera significativa la calidad del servicio de un flujo que puede ser visible a estas granularidades de tiempo más finas, pero que no son visibles con una granularidad de tiempo de un segundo. Las pilas típicas de SNMP pueden no estar diseñadas para este nivel, y pueden no cambiar bien de escala al mismo, de monitorización de grano fino en un gran número de dispositivos de red que pueden estar desplegados en el mundo entero. Además, los sistemas típicos de gestión de redes pueden proporcionar una interfaz de usuario que permita un análisis eficaz flexible de grandes cantidades de datos de monitorización de red.

Es contra estos antecedentes que surgió la necesidad de desarrollar el aparato, el sistema y el procedimiento para una monitorización de redes, una comunicación de datos y un procesamiento de datos mejorados descritos en la presente memoria.

El documento US 2005/0120054 A1 da a conocer un procedimiento de aprendizaje dinámico y una arquitectura adaptable de perfil de comportamiento normal (NBP) para proporcionar una protección rápida de aplicaciones empresariales. La arquitectura adaptable de NBP incluye una pluralidad de elementos de perfil. Cada elemento de perfil incluye una pluralidad de propiedades del perfil que contienen los valores descriptivos del elemento respectivo. Un sistema de seguridad de nivel de aplicación puede identificar y evitar ataques dirigidos a aplicaciones empresariales haciendo corresponder eventos de aplicación contra al menos un único elemento de perfil en el NBP adaptable.

Sumario de la invención

La presente invención está definida por la reivindicación independiente 1. Las reivindicaciones dependientes versan acerca de características opcionales de algunas realizaciones de la invención. Con el fin de determinar el grado de protección, se tendrá en cuenta debidamente cualquier elemento que sea equivalente a un elemento especificado en las reivindicaciones.

Un aspecto de la divulgación versa acerca de un sistema que incluye un primer dispositivo y un segundo dispositivo configurados para monitorizar una pluralidad de flujos de datos que recorren el segundo dispositivo. El segundo dispositivo está configurado para recoger estadística asociada con la pluralidad de flujos de datos, e incluye lógica de análisis de tráfico que está configurada para aumentar la pluralidad de flujos de datos con datos que incluyen información estadística basada en la estadística y en información de direcciones asociadas con el primer dispositivo. El primer dispositivo está configurado para recibir los datos. La lógica de análisis de tráfico es operable para enviar la información estadística al primer dispositivo con independencia de una solicitud en tiempo real de al menos una porción de la información estadística del primer dispositivo. La lógica de análisis de tráfico es configurable en función de al menos la información de direcciones.

Otro aspecto de la divulgación versa acerca de un sistema que incluye un primer dispositivo y un segundo dispositivo. El primer dispositivo incluye lógica de análisis de tráfico configurada para procesar primeros datos medidos en cada uno de una pluralidad de intervalos de tiempo de una primera granularidad de tiempo para obtener segundos datos asociados con cada uno de una pluralidad de intervalos de tiempo de una segunda granularidad de tiempo. La primera granularidad de tiempo es más fina que la segunda granularidad de tiempo. El segundo dispositivo está configurado para recibir y representar visualmente los segundos datos. La lógica de análisis de

tráfico es configurable de forma sensible al segundo dispositivo para reducir un volumen de los primeros datos para obtener los segundos datos, de forma que se mantenga en los segundos datos una indicación de una característica en los primeros datos, quedando la característica enmascarada si los segundos datos estuviesen basados en una agregación de los primeros datos en cada uno de la pluralidad de intervalos de tiempo de la segunda granularidad de tiempo.

Un aspecto de la invención versa acerca de un aparato. En una realización, el aparato incluye una pluralidad de máquinas de estado controladas por microcódigo, de lógica de reducción de datos y de lógica de transmisión, sin que medie solicitud. Al menos una de las máquinas de estado controladas por microcódigo está configurada para generar primeros datos estadísticos medidos en cada uno de una pluralidad de intervalos de tiempo de una primera granularidad de tiempo en función de datos de red incluidos en cada uno de una pluralidad de flujos de datos que recorren la al menos una de la pluralidad de máquinas de estado controladas por microcódigo. La lógica de reducción de datos está configurada para recibir los primeros datos estadísticos, y para obtener segundos datos estadísticos que tienen un volumen reducido con respecto a un volumen de los primeros datos estadísticos en función del desempeño de una operación matemática sobre los primeros datos estadísticos. Los segundos datos estadísticos están asociados con cada uno de la pluralidad de intervalos de tiempo de una segunda granularidad de tiempo. La primera granularidad de tiempo es más fina que la segunda granularidad de tiempo. La lógica de transmisión, sin que medie solicitud, está configurada para enviar los segundos datos estadísticos a través de una red con independencia de una solicitud en tiempo real procedente de la red.

Según otro aspecto de la divulgación, el aparato incluye una pluralidad de máquinas de estado controladas por microcódigo, lógica de generación de alertas y lógica de transmisión, sin que medie solicitud. Al menos una de la pluralidad de máquinas de estado controladas por microcódigo está configurada para generar datos estadísticos medidos en cada uno de una pluralidad de intervalos de tiempo en función de los datos de red incluidos en cada uno de una pluralidad de flujos de datos que recorren la al menos una de la pluralidad de máquinas de estado controladas por microcódigo. La lógica de generación de alerta está configurada para generar una indicación de alerta asociada con el al menos uno de la pluralidad de flujos de datos procesando los datos estadísticos para determinar si los datos estadísticos implican una característica asociada con la alerta. La lógica de transmisión, sin que medie solicitud, está configurada para enviar la indicación de alerta a través de una red con independencia de una solicitud procedente de la red.

Un aspecto adicional de la divulgación versa acerca de un sistema para la monitorización de la red y el análisis de tráfico de la red que incluye una pluralidad de dispositivos de red y una estación de gestión. Cada uno de la pluralidad de dispositivos de red está asociado con puertos correspondientes de una pluralidad de puertos. Cada uno de la pluralidad de dispositivos de red está configurado para determinar los datos de análisis de tráfico de la red asociados con una característica de los datos de red que recorren cada uno de la pluralidad de puertos. La estación de gestión está configurada para determinar una clasificación de la pluralidad de puertos en función de los datos de análisis de tráfico de la red en respuesta a una solicitud de búsqueda que implica la característica, y está configurada para representar visualmente la pluralidad de puertos en función de la clasificación.

Un aspecto adicional de la divulgación versa acerca de un sistema que incluye una pluralidad de primeros dispositivos, estando configurado cada uno de la pluralidad de primeros dispositivos con un conjunto correspondiente de puertos incluido en una pluralidad de puertos. Cada uno de la pluralidad de primeros dispositivos está configurado para determinar segundos datos en función de los primeros datos asociados con cada uno del conjunto correspondiente de puertos. El sistema también incluye un segundo dispositivo acoplado con la pluralidad de primeros dispositivos en una red. El segundo dispositivo está configurado para buscar la pluralidad de puertos en función de un criterio de búsqueda de entrada, para clasificar al menos dos de la pluralidad de puertos en función de los segundos datos y del criterio de búsqueda de entrada, y para representar visualmente los al menos dos de la pluralidad de puertos en un orden clasificado.

También se contemplan otros aspectos y realizaciones de la invención. No se pretende que el anterior sumario y la siguiente descripción detallada restrinjan la invención a ninguna realización particular sino que simplemente se pretende que describan algunas realizaciones de la invención.

Breve descripción de los dibujos

Para una mejor comprensión de la naturaleza y de los objetos de la invención, se debería hacer referencia a la siguiente descripción detallada tomada junto con los dibujos adjuntos, en los que:

La FIG. 1 ilustra un ejemplo de una red con ubicaciones representativas en las que se puede conectar un dispositivo de red, según una realización de la invención;

la FIG. 2 ilustra un sistema para la monitorización de la red y el análisis de tráfico de la red, según una realización de la invención;

las FIGURAS 3A a 3C ilustran ejemplos de representaciones visuales que muestran una solicitud de búsqueda que implica una característica de datos de análisis de tráfico de la red, y una clasificación de puertos en respuesta a la solicitud de búsqueda, según una realización de la invención;

la FIG. 4A ilustra un ejemplo de datos de funcionamiento de la red con una granularidad de un segundo en la que queda enmascarada una característica de los datos que recorren el dispositivo de red, según la técnica anterior;

la FIG. 4B ilustra un ejemplo de datos de funcionamiento de la red con una granularidad de un milisegundo en la que se mantiene una característica de los datos que recorren un dispositivo de red, según una realización de la invención;

la FIG. 4C ilustra un ejemplo de datos de análisis de tráfico de la red que tiene un volumen reducido en comparación con los datos de funcionamiento de la red de la FIG. 4B mientras que mantiene una indicación de la característica de los datos que recorren el dispositivo de red, según una realización de la invención;

la FIG. 5 ilustra un ejemplo de una red con ubicaciones representativas en las que se pueden observar valores de sello de tiempo asociados con flujos de datos, según una realización de la invención;

la FIG. 6 ilustra un diagrama de bloques lógicos de un sistema para la gestión de un dispositivo de red, según una realización de la invención;

la FIG. 7 ilustra un diagrama de bloques lógicos de la lógica de análisis de tráfico incluida en el dispositivo de red, según una realización de la invención;

la FIG. 8 ilustra un diagrama de bloques lógicos de una arquitectura de una realización de la invención;

la FIG. 9 ilustra el uso de la arquitectura de la FIG. 8 para aplicaciones bidireccionales, según una realización de la invención;

la FIG. 10 ilustra la arquitectura interna del circuito de distribución mostrado en la FIG. 8, según una realización de la invención;

la FIG. 11 ilustra la arquitectura interna del motor de reglas mostrado en la FIG. 8, basado en una máquina de estado controlada por microcódigo, según una realización de la invención;

la FIG. 12 ilustra un ejemplo de una secuencia de ejecución de instrucciones de microcódigo para implementar una regla de comparación, según una realización de la invención;

la FIG. 13 ilustra un ejemplo de la arquitectura interna de la lógica de condición mostrada en la FIG. 11, según una realización de la invención; y

la FIG. 14 ilustra un diagrama de bloques lógicos de una interfaz entre motores de reglas y sus módulos asociados de direccionamiento, según una realización de la invención.

Descripción detallada de la invención

La FIG. 1 ilustra un ejemplo de una red 100 con ubicaciones representativas 120 en las que se puede conectar un dispositivo de red, según una realización de la invención. La red 100 es un ejemplo de una red que puede ser desplegada en un centro de datos para conectar clientes con Internet. Las conexiones mostradas en la FIG. 1 son bidireccionales a no ser que se indique lo contrario. En una realización, la red 100 incluye conmutadores centrales 102, dispositivos periféricos 104 de encaminamiento y conmutadores 106 de acceso. Los conmutadores centrales 102 proporcionan conectividad a Internet a través de múltiples enlaces 110 de alta capacidad, tales como Ethernet de 10 Gigabits, 10GEC 802.1Q y/o paquete OC-192 por enlaces SONET. Los conmutadores centrales 102 pueden estar conectados entre sí por medio de múltiples enlaces 111 de alta capacidad, tales como para soportar una disponibilidad elevada. Los conmutadores centrales 102 también pueden estar conectados con dispositivos periféricos 104 de encaminamiento a través de múltiples enlaces 112. Los dispositivos periféricos 104 de encaminamiento pueden estar conectados con los conmutadores 106 de acceso a través de múltiples enlaces 114. Los enlaces 112 y los enlaces 114 pueden ser enlaces de alta capacidad o pueden ser enlaces de menor capacidad, tales como Ethernet de 1 Gigabit y/o paquete OC-48 por enlaces SONET. Los clientes pueden conectarse a los conmutadores 106 de acceso a través de puertos físicos y/o lógicos 116.

La FIG. 2 ilustra un sistema 600 para una monitorización de la red y un análisis de la red, según una realización de la invención. El sistema 600 incluye dispositivos 602A - 602N de red que monitorizan y llevan a cabo un análisis, tal como del tráfico de la red. El tráfico de la red que se monitoriza y analiza por medio de los dispositivos 602 de red puede entrar en los dispositivos 602 de red a través de interfaces 612A - 612Z. Después de la monitorización y del análisis por medio de los dispositivos 602 de red, el tráfico de la red puede salir de los dispositivos de red a través de

las interfaces 612 si las interfaces 612 son bidireccionales, o a través de otras interfaces (no mostradas) si las interfaces 612 son unidireccionales. Cada uno de los dispositivos 602 de red puede tener un gran número de interfaces 612 de alta capacidad, tales como 32 interfaces de red de 10 Gigabits.

En una realización, cada uno de los dispositivos 602 de red puede monitorizar y analizar el tráfico en una red correspondiente 100, tal como una red de centro de datos. Con referencia a la FIG. 1, en un ejemplo las interfaces 612 pueden estar conectadas con la red 100 en ubicaciones correspondientes de las ubicaciones 120. Cada una de las interfaces 612 puede monitorizar el tráfico procedente de un enlace de la red 100. Por ejemplo, en la FIG. 1, uno o más dispositivos 602 de red pueden monitorizar el tráfico en los enlaces 112 y 114.

Los dispositivos 602 de red están conectados con una estación 604 de gestión en una red 606. La red 606 puede ser una red de área amplia, una red de área local o una combinación de redes de área amplia y/o de área local. Por ejemplo, la red 606 puede representar una red que abarca un área geográfica grande. La estación 604 de gestión puede monitorizar, recoger y representar visualmente datos de análisis del tráfico procedentes de los dispositivos 602 de red, y puede proporcionar órdenes de control a los dispositivos 602 de red. De esta forma, la estación de gestión puede permitir que una empresa explotadora, de una única ubicación, monitorice y controle los dispositivos 602 de red desplegados en el mundo entero.

En una realización, la estación 604 de gestión puede recibir una solicitud de búsqueda (criterio de búsqueda) como entrada. La solicitud de búsqueda puede implicar una característica de los datos de red que recorren uno o más puertos asociados con los dispositivos 602 de red. El o los puertos pueden ser puertos físicos de los dispositivos 602 de red, y pueden corresponderse con una o más de las interfaces 612. De forma alternativa, los uno o más puertos pueden ser puertos lógicos en una única corriente de tráfico. La característica de los datos de la red puede adoptar diversas formas conocidas por una persona con un nivel normal de dominio de la técnica relacionadas con los datos de red. Por ejemplo, se puede indicar la característica en función de la aparición de un patrón de bits en los datos de red y/o en función de la aparición de un patrón de variación en una velocidad de transferencia de datos asociada con los datos de red. De forma alternativa o adicional, la solicitud de búsqueda puede implicar una característica operativa de los uno o más puertos, o una característica operativa de uno o más de los dispositivos 602 de red. La característica operativa puede adoptar diversas formas conocidas por una persona con un nivel normal de dominio de la técnica relacionadas con la operabilidad de los dispositivos de red. Por ejemplo, la característica operativa puede estar basada en la existencia de una condición de alarma de un grado particular de gravedad, o puede estar basada en información de la configuración, tal como la configuración del soporte físico, del soporte lógico y/o de servicios al cliente.

En respuesta a la solicitud de búsqueda, la estación 604 de gestión puede procesar datos de análisis de la red recibidos de los dispositivos 602 de red por medio de la red 606. La estación 604 de gestión puede determinar qué puertos, interfaces 612 y/o dispositivos 602 de red están implicados por la solicitud de búsqueda, y puede representar visualmente estos puertos, interfaces 612 y/o dispositivos 602 de red, tal como en una lista o tabla. En una realización, la estación 604 de gestión puede clasificar los puertos, las interfaces 612 y/o los dispositivos 602 de red que están implicados por la solicitud de búsqueda, y puede representar visualmente los puertos, las interfaces 612 y/o los dispositivos 602 de red en el orden clasificado (véase la siguiente exposición con referencia a las FIGURAS 3A a 3C). La búsqueda y la clasificación pueden llevarse a cabo en función de cualquier algoritmo y/o criterio conocidos por una persona con un nivel normal de dominio de la técnica. Por ejemplo, en respuesta a una solicitud de búsqueda de puertos con datos de red que recorren los puertos que tienen una característica particular, la estación 604 de gestión puede seleccionar un subconjunto de puertos entre los dispositivos 602 de red para los cuales los datos de red que recorren los puertos tienen la característica, y puede representar ese subconjunto de puertos. Se puede representar visualmente el subconjunto de puertos en orden clasificado en función de un número de veces que se ha detectado la característica en los datos de red que recorren el subconjunto de los puertos.

Además, en una realización, la estación 604 de gestión puede remozar la representación visual de los puertos, las interfaces 612 y/o los dispositivos 602 de red tras un cambio en la clasificación debido a variaciones dinámicas en los datos de análisis de la red. Por ejemplo, la estación 604 de gestión puede remozar dinámicamente la representación visual de los puertos en función de variaciones en tiempo real en el número de veces que se ha detectado una característica en los datos de red que recorren los puertos.

Según se utiliza en la presente memoria, datos de análisis de la red hace referencia en términos generales tanto a datos de análisis de tráfico de la red asociados con los datos que recorren uno o más dispositivos de red (tales como los dispositivos 602 de red), y otros datos relacionados con la red asociados con las características operativas de uno o más puertos, interfaces y/o dispositivos de red. Los datos de tráfico de red pueden incluir, por ejemplo, datos asociados con la evaluación de reglas basadas en firma y/o de comportamiento aplicadas a los datos de red que recorren uno o más de los dispositivos 602 de red. Los datos de análisis de tráfico de la red pueden incluir estadística (tales como datos de rendimiento) asociada con los datos de red. Ejemplos de esta estadística incluyen datos relacionados con la cantidad de los datos de red y/o con la calidad de los datos de red, pudiendo incluir los ejemplos de estadística de calidad de los datos números de errores detectados en datos que recorren un puerto, y el tiempo de espera de la red de ida o de ida y vuelta asociado con los datos recibidos en un puerto. De forma alternativa o adicional, los datos de análisis de tráfico de la red pueden incluir datos derivados de un procesamiento

adicional de los datos asociados con la evaluación de las reglas aplicadas a los datos de la red, o de la estadística asociada con los datos de la red. Este procesamiento adicional puede llevarse a cabo por medio de los dispositivos 602 de red para mejorar el cambio de escala de la arquitectura de gestión de la red, según se describe a continuación.

Los dispositivos 602 de red pueden llevar a cabo de forma eficaz la monitorización, el filtrado, la agregación, la reiteración, el equilibrado, la colocación de un sello de tiempo y/o la modificación de tráfico de la red en una arquitectura unificada, en función de reglas que pueden ser muy granulares (tales como granulares hasta el bit) en cualquier lugar en el tráfico de la red, mientras que al mismo tiempo actúan como un “tope en el hilo” minimizando la perturbación del tráfico de la red introducido por los dispositivos 602 de red. Al llevar a cabo al menos esta amplia variedad de funciones, los dispositivos 602 de red pueden obtener datos de análisis de la red que pueden proporcionar los dispositivos 602 de red a la estación 604 de gestión para soportar una amplia variedad de solicitudes de búsqueda recibidas por la estación 604 de gestión. Estas solicitudes de búsqueda pueden estar relacionadas con una amplia gama de características del tráfico de la red y/o dispositivos de la red. La capacidad de búsqueda y de clasificación de la estación 604 de gestión tiene una combinación convincente de ventajas, debido a que esta capacidad puede ser entre dispositivos 602 de red desplegados en el mundo entero, puede ser en esta amplia gama de características, y puede tener en cuenta cambios dinámicos en los resultados de búsqueda y/o en la clasificación de los resultados de búsqueda debidos a variaciones dinámicas en los datos de análisis de la red. La capacidad de búsqueda y de clasificación de la estación 604 de gestión también puede permitir un análisis flexible, eficaz y basado en el contexto y el filtrado de la gran cantidad de datos de análisis de la red disponibles en la estación 604 de gestión.

Los dispositivos 602 de red pueden recoger datos de análisis del tráfico de la red de diversas formas. Por ejemplo, un dispositivo 602 de red puede aplicar una o más reglas para seleccionar un flujo de datos (puerto lógico), tal como en función de un campo de cabecera del paquete tal como una dirección IP o un identificador de capa superior, tal como un puerto de protocolo de control de la transmisión (TCP). De forma alternativa o adicional, el dispositivo 602 de red puede recoger estadística asociada con el tráfico de la red, tal como para flujos de datos (puertos lógicos) y/o puertos físicos de datos. De forma alternativa o adicional, el dispositivo 602 de red puede insertar y/o retirar un sello de tiempo de uno o más paquetes incluidos en el flujo de datos como parte de la medición del tiempo de espera del flujo de datos por parte de la red (véase la siguiente exposición con referencia a la FIG. 5). La inserción y la retirada del sello de tiempo pueden llevarse a cabo sobre la marcha, sin capturar los paquetes de datos, y sin copiar los paquetes de datos. La solicitud de búsqueda puede asociarse con cualquiera de estos tipos, o con todos ellos, de datos de análisis de tráfico de la red.

Una regla es un criterio específico utilizado por el aparato para determinar si debe reaccionar a una unidad de datos, tal como un paquete incluido en un flujo de datos. Un tipo de regla está basado en la firma. Las firmas son secuencias de bits en cualquier lugar en el contenido digital de tráfico que indican una característica del tráfico de interés al aparato. Las secuencias de bits pueden ser completamente invariantes, o pueden contener porciones que son comodines no esenciales a la evaluación de la regla. Una firma podría aparecer en la cabecera o en la carga útil de paquetes individuales de la red, o en una secuencia de paquetes. Una firma puede abarcar una o más cabeceras de paquetes y cargas útiles correspondientes, y se utiliza una inspección profunda de paquetes para descubrir tales firmas. Se utiliza una inspección de corriente para descubrir firmas en una secuencia de paquetes. Se utilizan ambos tipos de inspección para una visibilidad completa de diversos tipos de tráfico de red.

Un segundo tipo de regla es de comportamiento. Dos tipos de reglas de comportamiento son las reglas de comportamiento locales y las basadas en red. Se contempla que se puedan utilizar reglas de comportamiento locales para detectar cambios que pueden ser medidos localmente en el aparato. Estos cambios incluyen, sin limitación, cambios en el volumen de tráfico o en el equilibrio de tráfico de entrada y de salida, tales como solicitudes y respuestas, que pasa por el aparato. Se pueden utilizar las reglas de comportamiento basadas en red para detectar cambios en la red que pueden ser medidos junto con otros dispositivos de red, incluyendo, sin limitación, el aparato. Un ejemplo de tal regla es el volumen total de tráfico promediado en múltiples puntos en la red durante un periodo específico de tiempo en comparación con un umbral máximo. Otro ejemplo es el número total de eventos de un tipo específico, tales como indicaciones de error de la red, que se han producido a través de la red durante un periodo específico de tiempo, de nuevo en comparación con un umbral máximo. La monitorización de la estadística recogida para una evaluación de la regla puede ser importante, por ejemplo, debido a que se puede detectar un funcionamiento defectuoso en la red en función de su impacto sobre el comportamiento o rendimiento de la red. De forma alternativa o adicional, se puede detectar un nuevo tipo de ataque en función de su impacto sobre el comportamiento o rendimiento de la red, incluso cuando se desconoce su firma.

Un tercer tipo de regla es tanto de comportamiento como basada en la firma. Un ejemplo de tal regla es el número total de paquetes que contienen una firma específica que han pasado por un dispositivo 602 de red durante un periodo específico de tiempo durante el día en comparación con un umbral máximo y/o mínimo. El puerto lógico al que pertenece un paquete (o paquetes, tales como paquetes incluidos en un flujo de datos) puede determinarse aplicando al paquete (o paquetes, tales como paquetes incluidos en un flujo de datos) una regla tal como una regla basada en la firma, una regla de comportamiento o una combinación de reglas de comportamiento y basadas en firma.

Además de la aplicación de reglas y de recogida de estadística, los dispositivos 602 de red pueden llevar a cabo funciones adicionales para mejorar la comunicación escalable de datos de análisis del tráfico de la red en la red 606. En particular, las funciones de procesamiento y de análisis de datos pueden dividirse entre los dispositivos 602 de red y la estación 604 de gestión, de forma que los dispositivos 602 de red lleven a cabo porciones significativas de estas funciones localmente, tal como en soporte físico, en lógica reconfigurable y/o en soporte lógico inalterable. Por ejemplo, los dispositivos 602 de red pueden mejorar la estadística recogida por los dispositivos 602 de red, tal como la estadística asociada con flujos de datos, para reducir el volumen de los datos de análisis del tráfico de la red que han de ser comunicados a la estación 604 de gestión mientras que mantiene una indicación de una característica (función) de los flujos de datos mostrada en la estadística recogida (véase la exposición con referencia a las siguientes FIGURAS 4A a 4C). En una realización, la búsqueda y la clasificación de los puertos, de las interfaces 612 y/o de los dispositivos 602 de red pueden estar basadas en los datos de análisis del tráfico de la red que han sido reducidos según se ha descrito anteriormente.

De forma alternativa o adicional, los dispositivos 602 de red pueden procesar la estadística y/o información basada en reglas recogidas por los dispositivos 602 de red, y en función de este procesamiento pueden generar una indicación de alerta para la estación 604 de gestión. La indicación de alerta puede estar asociada con indicaciones correspondientes de los puertos, de las interfaces 612 y/o de los dispositivos 602 de red en función de la detección de una característica en los datos de red que recorren los correspondientes de los puertos, de las interfaces 612 y/o de los dispositivos 602 de red. En una realización, la búsqueda y la clasificación de los puertos, de las interfaces 612 y/o de los dispositivos 602 de red pueden estar basados en si la indicación de alerta está presente para cada uno de los puertos, de las interfaces 612 y/o de los dispositivos 602 de red.

De forma alternativa o adicional, los dispositivos 602 de red pueden llevar a cabo operaciones matemáticas sobre la estadística y/o en la información basada en reglas recogidas por los dispositivos 602 de red. En una realización, estas operaciones matemáticas pueden incluir al menos uno de un mínimo, un máximo, una media, una convolución, una media móvil, una suma de cuadrados, una operación de filtrado lineal, y una operación de filtrado no lineal. En una realización, la búsqueda y la clasificación de los puertos, de las interfaces 612 y/o de los dispositivos 602 de red pueden estar basados en un resultado de al menos una de estas operaciones matemáticas sobre la estadística y/o información basada en reglas asociada con los datos de la red.

El desempeño descrito anteriormente de porciones significativas de análisis de datos y de procesamiento de funciones en los dispositivos 602 de red en vez de en la estación 604 de gestión tiene diversas ventajas. La reducción del volumen de los datos de análisis del tráfico de la red que han de ser comunicados a la estación 604 de gestión puede reducir de forma significativa la sobrecarga del ancho de banda de la red por flujo asociado con la gestión de la red. Esto puede ser importante, dado que la carga de tráfico y el número de flujos de datos que recorren las redes y los centros de datos aumentan rápidamente, lo que tiene como resultado un número rápidamente creciente de contadores de rendimiento que han de ser monitorizados por las arquitecturas de gestión de redes. Además, el procesamiento de estadística y/o de información basada en reglas recogidas por los dispositivos 602 de red en los dispositivos 602 de red puede reducir significativamente la carga de procesamiento en la estación 604 de gestión. Esto puede reducir los requisitos de procesamiento y de memoria en la estación 604 de gestión, puede simplificar el soporte lógico que se ejecuta en la estación 604 de gestión, y puede acelerar la operación de la estación 604 de gestión.

En una realización, se pueden comunicar los datos de análisis de la red a la estación 604 de gestión mediante una gestión basada en la transmisión, sin que medie solicitud (véase la siguiente exposición con referencia a la FIG. 6). La gestión basada en la transmisión, sin que medie solicitud, también puede reducir de forma significativa la sobrecarga del ancho de banda de la red eliminando la sobrecarga debida a sondeos en protocolos de gestión basados en la recepción, sin que medie solicitud, tales como el protocolo simple de gestión de redes (SNMP).

Además, en las redes actuales, los flujos de datos representan una amplia variedad de servicios con una variedad de requisitos de rendimiento. Por ejemplo, para algunos flujos de paquetes de datos, puede ser suficiente monitorizar la métrica de rendimiento por flujo, tal como bytes transmitidos o recibidos, con una granularidad de tiempo de un segundo. Esta es una configuración común para arquitecturas típicas de gestión de redes, tales como arquitecturas de SNMP. Sin embargo, para otros flujos de paquetes de datos, puede ser importante monitorizar la métrica de rendimiento por flujo con una granularidad de tiempo más fina, tal como 1 milisegundos o 10 milisegundos, dado que existen fenómenos que pueden tener un impacto de forma significativa sobre la calidad del servicio de un flujo que pueden ser visibles a estas granularidades de tiempo más finas, pero que no son visibles con una granularidad de tiempo de un segundo. Las pilas típicas de SNMP pueden no estar diseñadas para este nivel, y pueden no cambiar bien de escala al mismo, de monitorización de grano fino. Además, las arquitecturas de gestión basadas en la transmisión, sin que medie solicitud, al eliminar la sobrecarga por sondeo asociada con el SNMP, pueden proporcionar esta monitorización basada en flujo de grano más fino con una mayor eficacia.

Las FIGURAS 3A a 3C ilustran ejemplos de representaciones visuales que muestran una solicitud de búsqueda que implica una característica de los datos de análisis del tráfico de la red, y una clasificación de puertos en respuesta a la solicitud de búsqueda, según una realización de la invención. La FIG. 3A ilustra una representación visual que muestra un término de búsqueda, dispositivos de red y puertos en los que se produce una cadena particular en los

datos que recorren los puertos, y una clasificación de los puertos en función del número de apariciones de la cadena, según una realización de la invención. En el ejemplo de la FIG. 3A, la cadena es “AQUA”. El identificador del dispositivo de la red y/o el identificador del puerto pueden ser, por ejemplo, una dirección IP, una dirección MAC, un identificador del fabricante o un identificador definido por un usuario, pero no está limitado a estos tipos de identificadores.

La FIG. 3B ilustra una representación visual que muestra un término de búsqueda, dispositivos de red y puertos en los que se produce una condición particular (tal como una microrráfaga) en los datos que recorren los puertos, y una clasificación de los puertos en función del número de apariciones de la condición, según una realización de la invención. En el ejemplo de la FIG. 3B, la condición es una microrráfaga. El identificador del dispositivo de red y/o el identificador del puerto pueden ser, por ejemplo, una dirección IP, una dirección MAC, un identificador del fabricante o un identificador definido por un usuario, pero no está limitado a estos tipos de identificadores.

La FIG. 3C ilustra una representación visual que muestra un término de búsqueda, dispositivos de red y puertos para los cuales una velocidad medida de transferencia de datos que recorren los puertos supera un umbral particular, y una clasificación de los puertos por velocidad de transferencia de datos, según una realización de la invención. En el ejemplo de la FIG. 3C, el umbral es de 1 Gbps. El identificador del dispositivo de red y/o el identificador del puerto pueden ser, por ejemplo, una dirección IP, una dirección MAC, un identificador del fabricante o un identificador definido por un usuario, pero no está limitado a estos tipos de identificadores.

En una realización, con referencia a la FIG. 2, uno o más de los dispositivos 602 de red pueden incluir lógica de análisis del tráfico configurada para procesar primeros datos (tales como primeros datos estadísticos no reducidos que pueden incluir primeros datos no reducidos de rendimiento de la red) medidos en intervalos de tiempo de una primera granularidad de tiempo para obtener segundos datos (tales como segundos datos estadísticos reducidos que pueden incluir segundos datos reducidos de rendimiento de la red) asociados con los intervalos de tiempo de una segunda granularidad de tiempo. Estos segundos datos pueden incluirse en los datos de análisis del tráfico de la red proporcionados a la estación 604 de gestión por medio de los uno o más dispositivos 602 de red. La primera granularidad de tiempo puede ser más fina que la segunda granularidad de tiempo. La estación 604 de gestión puede estar configurada para recibir los segundos datos procedentes de los uno o más dispositivos 602 de red, y para representar visualmente los segundos datos. La lógica de análisis del tráfico es configurable de forma sensible a la estación 604 de gestión para reducir un volumen de los primeros datos para obtener los segundos datos, de forma que se mantenga en los segundos datos una indicación de una función (característica) de los primeros datos, quedando la función enmascarada si los segundos datos estuviesen basados en una agregación de los primeros datos en cada uno de los intervalos de tiempo de la segunda granularidad de tiempo. En las FIGURAS 4A a 4C, que se exponen a continuación, se proporciona un ejemplo de esta reducción de los datos.

La FIG. 4A ilustra un ejemplo de datos no reducidos 640 de rendimiento de la red con una segunda granularidad en la que queda enmascarada una función de los datos que recorren el dispositivo 602 de red (véase la FIG. 2), según la técnica anterior. Se muestran los datos no reducidos 640 de rendimiento de la red como un ancho de banda (número de bits que puede fluir en un tiempo dado) de un flujo de datos producido por un codificador de televisión por protocolo de Internet (IPTV) medido como una función del tiempo. Para una segunda granularidad, quedan enmascaradas funciones notables en los datos (que son visibles en la FIG. 4B) debido a que cada muestra de datos en los datos no reducidos 640 de rendimiento de la red puede estar basada en una cantidad agregada de datos transmitidos en un intervalo de tiempo significativamente mayor que la duración de cada uno de las funciones notables en los datos que quedan enmascaradas.

La FIG. 4B ilustra un ejemplo de datos no reducidos 650 de rendimiento de la red con una granularidad de un milisegundo en la que se mantiene una función 658 de datos que recorren el dispositivo 602 de red (véase la FIG. 2), según una realización de la invención. Se muestran los datos no reducidos 650 de rendimiento de la red como ancho de banda (número de bits de datos que pueden fluir en un tiempo dado) de una salida de flujo de datos por un codificador de televisión por protocolo de Internet (IPTV) medido como una función del tiempo. Los datos no reducidos 650 de rendimiento de la red incluyen la función 658, que puede indicarse como un subconjunto de los datos no reducidos 650 de rendimiento de la red. La función 658 puede incluir un pico 652, durante el cual el ancho de banda por milisegundo de los datos no reducidos 650 de rendimiento de la red es sustancialmente mayor que un ancho de banda medio de los datos no reducidos 650 de rendimiento de la red. El pico 652 está precedido por un valle 654, durante el cual el ancho de banda por milisegundo de los datos no reducidos 650 de rendimiento de la red es sustancialmente menor que un ancho de banda medio de los datos no reducidos 650 de rendimiento de la red. La función 658 también puede incluir el valle 654. De forma alternativa, la función 658 puede incluir únicamente el pico 652. Puede haber otras caídas 656 en los datos no reducidos 650 de rendimiento de la red, pero la extensión de tiempo del valle 654 puede ser significativamente mayor que la extensión de tiempo de las otras caídas 656. La función 658 puede producirse en los datos no reducidos 650 de rendimiento de la red debido, por ejemplo, a un “hipo” no deseable en la salida del flujo de datos por el codificador de IPTV, durante el cual el codificador de IPTV, primero no llega a transmitir datos (durante el valle 654), luego emite ráfagas (durante el pico 652) para mantener el ancho de banda medio de los datos no reducidos 650 de rendimiento de la red. Este fenómeno es un ejemplo de una microrráfaga, que es un breve periodo durante el que la carga instantánea de tráfico en un canal de comunicaciones es significativamente mayor y/o menor que una carga típica de tráfico en el canal de

comunicaciones. El canal de comunicaciones puede ser un canal físico (asociado con un puerto físico) o un canal lógico (asociado con un flujo o puerto lógico) que puede tener una porción de capacidad de transporte de datos del canal físico. Las microrráfagas en una red, tal como la red 100 (véase la FIG. 1), pueden ser problemáticas debido, por ejemplo, a que el pico 652 puede violar limitaciones de capacidad en la red 100, dando lugar a una pérdida de paquetes.

La FIG. 4C ilustra un ejemplo de datos reducidos 660 de rendimiento de la red que tienen un volumen reducido en comparación con los datos no reducidos 650 de rendimiento de la red de la FIG. 4B mientras que mantienen una indicación de la función 658 de los datos que recorren el dispositivo 602 de red (véase la FIG. 2), según una realización de la invención. Se muestran los datos reducidos 660 de rendimiento de la red como ancho de banda (número de bits de datos que pueden fluir en un tiempo dado) de un flujo de datos producido por un codificador de televisión por protocolo de Internet (IPTV) medido como una función del tiempo. Los datos reducidos 660 de rendimiento de la red tiene una granularidad de un segundo. Los datos reducidos 660 de rendimiento de la red pueden obtenerse aplicando operaciones matemáticas a los datos no reducidos 650 de rendimiento de la red. En el ejemplo de la FIG. 4C, los datos reducidos 660A de rendimiento de la red son el máximo, en intervalos de tiempo de 1 segundo, de las muestras de granularidad de 1 milisegundo de los datos no reducidos 650 de rendimiento de la red en cada uno de los intervalos de tiempo de 1 segundo. En una realización, una indicación de variaciones incluidas en los datos no reducidos 650 de rendimiento de la red en un intervalo de tiempo de 1 segundo que son sustancialmente mayores que un valor medio de los datos no reducidos 650 de rendimiento de la red en el intervalo de tiempo de 1 segundo son visibles tras la representación visual de los datos reducidos 660A de rendimiento de la red. Los datos reducidos 660B de rendimiento de la red son la media, en intervalos de tiempo de 1 segundo, de las muestras de granularidad de 1 milisegundo de los datos no reducidos 650 de rendimiento de la red en cada uno de los intervalos de tiempo de 1 segundo. Los datos reducidos 660C de rendimiento de la red son el mínimo, en intervalos de tiempo de 1 segundo, de las muestras de granularidad de 1 milisegundo de los datos no reducidos 650 de rendimiento de la red en cada uno de los intervalos de tiempo de 1 segundo. En una realización, una indicación de variaciones incluida en los datos no reducidos 650 de rendimiento de la red en un intervalo de tiempo de 1 segundo que son sustancialmente menores que un valor medio de los datos no reducidos 650 de rendimiento de la red en el intervalo de tiempo de 1 segundo son visibles tras la representación visual de los datos reducidos 660C de rendimiento de la red. Como puede verse a partir de los datos reducidos 660A de rendimiento de la red, se mantiene una indicación del pico 652 (véase la FIG. 4B) en los datos no reducidos 650 de rendimiento de la red en los datos reducidos 660A de rendimiento de la red como el pico 662, aunque un volumen de los datos reducidos 660A de rendimiento de la red puede ser al menos 10 veces menor (en este caso, 1000 veces menor) que un volumen de los datos no reducidos 650 de rendimiento de la red. Por ejemplo, la indicación 662 puede incluir un máximo de los datos no reducidos 650 de rendimiento de la red en al menos uno de los intervalos de tiempo de 1 segundo. De esta forma, se puede reducir de forma significativa un volumen de los datos reducidos de rendimiento de la red con una granularidad de 1 segundo con respecto a un volumen de datos no reducidos de rendimiento de la red con una granularidad de 1 milisegundo, mientras se mantiene una indicación 662 del pico 652 en los datos reducidos de rendimiento de la red.

En una realización, los datos reducidos 660 de rendimiento de la red pueden incluir un máximo y un mínimo de los datos no reducidos 650 de rendimiento de la red, de forma que las indicaciones tanto de un pico como de un valle en los datos no reducidos 650 de rendimiento de la red sean visibles tras la representación visual de los datos reducidos de rendimiento de la red. El valor medio del pico puede ser al menos cinco veces mayor que una media de los datos no reducidos 650 de rendimiento de la red en un intervalo de tiempo de 1 segundo (granularidad de tiempo de los datos reducidos 660 de rendimiento de la red) incluyendo el pico, y un valor medio del valle puede ser al menos cinco veces menos que una media de los datos no reducidos 650 de rendimiento de la red en un intervalo de tiempo de 1 segundo (granularidad de tiempo de los datos reducidos 660 de rendimiento de la red) incluyendo el valle.

Con referencia a la FIG. 2, en una realización, la lógica de análisis del tráfico puede ser configurable de forma sensible a la estación 604 de gestión para variar una granularidad de tiempo de los datos reducidos de rendimiento de la red producidos por la lógica de análisis del tráfico. La lógica de análisis del tráfico puede ser configurable de forma sensible a la estación 604 de gestión para incluir en los datos reducidos de rendimiento de la red al menos uno de un mínimo, un máximo y una media de los datos no reducidos de rendimiento de la red en intervalos de tiempo de la granularidad de tiempo de los datos reducidos de rendimiento de la red.

La FIG. 5 ilustra un ejemplo de una red 670 con ubicaciones representativas 672A - 672D en las que se pueden medir valores de sello de tiempo asociados con los flujos de datos, según una realización de la invención. Con referencia a la FIG. 2, el dispositivo 602 de red puede insertar un sello de tiempo en uno o más paquetes, y/o quitarlo de los mismos, incluidos en un flujo de datos como parte de la medición del tiempo de espera de la red para paquetes incluidos en el flujo de datos. El tiempo de espera de la red de paquetes es un retraso de paquetes introducido por una red. Por ejemplo, el tiempo de espera de la red excluye retrasos debidos a un procesamiento del soporte lógico en una fuente (tal como el anfitrión 674) y en un destino (tal como el anfitrión 676). El tiempo de espera de la red puede ser medido bien en la ida (el tiempo desde el envío de un paquete por la fuente hasta la recepción del mismo en el destino, tal como desde la ubicación 672A hasta la ubicación 672D), o en la ida y la vuelta (la suma del tiempo de espera de ida desde la fuente hasta el destino, además del tiempo de espera de vuelta desde

el destino de nuevo a la fuente, tal como la suma del tiempo de espera de ida desde la ubicación 672A hasta la ubicación 672D además del tiempo de espera de vuelta desde la ubicación 672D hasta la ubicación 672A). El tiempo de espera de la red puede ser el retraso desde el tiempo del inicio de la transmisión de paquetes en un remitente hasta el tiempo del final de la recepción de paquetes en un receptor. De forma alternativa, el tiempo de espera de la red puede ser el retraso desde el momento del inicio de la transmisión de paquetes en un remitente hasta el momento del inicio de la recepción de paquetes en un receptor.

Un tiempo reducido de espera de la red para flujos de datos es importante para diversas aplicaciones, tales como plataformas algorítmicas de compraventa. En una compraventa algorítmica, retrasos excesivos y/o impredecibles en la ejecución de compraventas reduce la predictibilidad de los algoritmos y el potencial de beneficio y, por lo tanto, son una desventaja frente a los competidores. Puede ser útil medir el tiempo de espera de la red de ida y/o el tiempo de espera de la red de ida y vuelta. En redes asimétricas con distintos tiempos de espera de la red en cada dirección, las mediciones del tiempo de espera de la red de ida pueden facilitar la determinación de los tiempos de espera de la red en cada dirección. Además, las mediciones del tiempo de espera de la red de ida pueden ser útiles en redes en las que las transacciones del anfitrión 674 al anfitrión 676 recorren un recorrido distinto que las transacciones del anfitrión 676 al anfitrión 674. Por ejemplo, en una compraventa algorítmica, se pueden recibir datos del mercado por medio de un sistema de agente de bolsa por un recorrido de comunicaciones desde la bolsa, y se pueden enviar instrucciones a la bolsa desde el sistema del agente de bolsa por un recorrido distinto de comunicaciones.

El dispositivo 602 de red puede insertar y retirar sellos de tiempo sobre la marcha en soporte lógico y/o en lógica reconfigurable, sin capturar los paquetes de datos, y sin copiar los paquetes de datos. De esta forma, la inserción y la retirada del sello de tiempo pueden llevarse a cabo con un grado elevado de precisión dado que se evitan los retrasos potencialmente impredecibles asociados con un procesamiento de soporte lógico y con la captura y/o la copia de los paquetes de datos. El dispositivo 602 de red también puede medir el tiempo de espera de la red para cada paquete en el flujo de datos, puede determinar el tiempo de espera de la red por flujo (tal como una media de los tiempos de espera de la red por paquete para paquetes incluidos en un flujo de datos) y la fluctuación (variación en el tiempo de espera de la red), y puede comunicar a la estación 604 de gestión el tiempo de espera de la red por flujo y la fluctuación.

La FIG. 6 ilustra un diagrama de bloques lógicos de un sistema para la gestión del dispositivo 602 de red, según una realización de la invención. El dispositivo 602 de red incluye lógica 682 de procesamiento del recorrido de los datos para monitorizar los flujos 695 de datos, una interfaz 696 de salida y lógica 694 de análisis del tráfico. La lógica 682 de procesamiento del recorrido de los datos está configurada para proporcionar información 686 relacionada con los datos de la red a la lógica 694 de análisis del tráfico y datos de la red directamente a la interfaz 696 de salida a lo largo del recorrido 692 de los datos. La información 686 relacionada con los datos de la red puede incluir, sin limitación, datos obtenidos de una aplicación de una o más reglas a los datos de la red, incluyendo los flujos 695 de datos, estadística asociada con los datos de la red, granularidades de tiempo en las cuales se recogen los datos y/o la estadística basada en reglas e información de medición del tiempo de espera de la red asociada con los datos de la red, según se ha descrito anteriormente con referencia a la FIG. 2. El dispositivo 602 de red puede estar configurado para identificar un subconjunto de los flujos 695 de datos, y para recoger la información 686 relacionada con los datos de la red del subconjunto identificado de los flujos 695 de datos. La lógica 694 de análisis del tráfico procesa la información 686 relacionada con los datos de la red para obtener datos de análisis del tráfico de la red, según se describe con referencia a las FIGURAS 2, 4-5 y 7-8. La lógica 694 de análisis del tráfico puede estar configurada por otro dispositivo en función de información de direcciones asociada con el otro dispositivo. El otro dispositivo puede ser la estación 604 de gestión. De forma alternativa, el otro dispositivo puede ser otro dispositivo de red que se interconecte con una estación de gestión. La lógica 694 de análisis del tráfico puede generar uno o más paquetes que incluyen los datos de análisis del tráfico de la red y la información de direcciones.

En una realización, la lógica 694 de análisis del tráfico puede generar datos 690 de análisis del tráfico de la red en forma de paquetes, y puede proporcionar los datos 690 de análisis del tráfico de la red a la interfaz 696 de salida. La lógica 694 de análisis del tráfico es operable para enviar los datos 690 de análisis del tráfico de la red al otro dispositivo (tal como la estación 604 de gestión) con independencia de una solicitud en tiempo real, procedente del otro dispositivo, de al menos una porción de los datos 690 de análisis del tráfico de la red. La solicitud en tiempo real puede ser un sondeo procedente del otro dispositivo. Según se ha descrito anteriormente con referencia a la FIG. 2, una gestión basada en la transmisión, sin que medie solicitud, puede reducir de forma significativa la sobrecarga del ancho de banda de la red reducida con una gestión de la red eliminando la sobrecarga debida a sondeos en protocolos de gestión basada en la recepción, sin que medie solicitud, tales como el protocolo simple para gestión de redes (SNMP).

En esta realización, la gestión basada en la transmisión, sin que medie solicitud, puede llevarse a cabo con independencia de los protocolos tradicionales de gestión de la red, dado que la lógica 694 de análisis del tráfico puede aumentar los flujos 695 de datos que recorren el recorrido 692 de los datos con los datos 690 de análisis del tráfico de la red. Según se ha descrito anteriormente con referencia a la FIG. 2, las pilas típicas de SNMP pueden no estar diseñadas para una monitorización de grano crecientemente fino, y pueden no cambiar bien de escala a la misma, que puede ser necesaria para la monitorización de flujos de paquetes. Además, la estación 604 de gestión

puede proporcionar información 688 de control a la lógica 694 de análisis del tráfico por medio de la lógica 682 de procesamiento del recorrido de los datos sin recorrer un puerto local 684 de gestión. En la presente realización, el puerto local 684 de gestión, si se incluye en el dispositivo 602 de red, puede soportar una configuración de porciones del dispositivo 602 de red distinta de la lógica 694 de análisis del tráfico.

La lógica 694 de análisis del tráfico puede estar configurada para enviar, sin que haya solicitud, los datos 690 de análisis del tráfico de la red al otro dispositivo en función de un periodo de transmisión de datos. La lógica 694 de análisis del tráfico puede estar configurada para recoger la información 686 relacionada con los datos de la red en función de un periodo de recogida de datos. La lógica 694 de análisis del tráfico puede ser configurable de forma sensible a un abono por parte del otro dispositivo a los datos 690 de análisis del tráfico de la red. El abono puede identificar los flujos 695 de datos en función de identificadores, estando asociado cada uno de los identificadores con uno correspondiente de los flujos 695 de datos. La lógica 694 de análisis del tráfico puede ser configurable de forma sensible al otro dispositivo para anunciar los flujos 695 de datos al otro dispositivo.

En otra realización, la lógica 694 de análisis del tráfico puede proporcionar datos 691 de análisis del tráfico de la red a un puerto local 684 de gestión. El puerto local 684 de gestión puede proporcionar datos 691 de análisis del tráfico de la red a la estación 604 de gestión. La estación 604 de gestión puede proporcionar información 689 de control a la lógica 694 de análisis del tráfico a través del puerto local 684 de gestión, que puede estar configurado para soportar una configuración de la lógica 694 de análisis del tráfico.

La FIG. 7 ilustra un diagrama de bloques lógicos de la lógica 694 de análisis del tráfico incluida en el dispositivo 602 de red (véase la FIG. 6), según una realización de la invención. La lógica 694 de análisis del tráfico puede incluir una o más de lógica 700 de reducción de datos, lógica 702 de transmisión, sin que medie solicitud, lógica 704 de generación de alertas, lógica 706 de análisis del tiempo de espera de la red y de la fluctuación, lógica 708 de cálculo y lógica 710 de control.

La lógica 700 de reducción de datos puede estar configurada para llevar a cabo funciones de la lógica 694 de análisis del tráfico asociadas con la reducción de datos. Por ejemplo, la lógica de reducción de datos puede estar configurada para procesar primeros datos (tales como primeros datos estadísticos no reducidos que pueden incluir primeros datos no reducidos de rendimiento de la red) medidos en intervalos de tiempo de una primera granularidad de tiempo para obtener segundos datos (tales como segundos datos estadísticos reducidos que pueden incluir segundos datos reducidos de rendimiento de la red) asociados con intervalos de tiempo de una segunda granularidad de tiempo. La primera granularidad de tiempo puede ser más fina que la segunda granularidad de tiempo. Los datos estadísticos no reducidos pueden ser medidos por al menos una de una pluralidad de máquinas de estado controladas por microcódigo (véase más abajo con referencia a la FIG. 8), y pueden ser medidos en función de los datos de red incluidos en cada uno de una pluralidad de flujos 695 de datos que recorren las al menos una de la pluralidad de máquinas de estado controladas por microcódigo. Se puede reducir el volumen de los datos estadísticos reducidos con respecto al volumen de los datos estadísticos no reducidos, tal como en al menos diez veces. La reducción de volumen puede basarse en el desempeño de una operación matemática sobre los datos estadísticos no reducidos, tales como al menos un mínimo, un máximo, una media, una convolución, una media móvil, una suma de los cuadrados, una operación de filtrado lineal y una operación de filtrado no lineal. La lógica 700 de reducción de datos puede ser configurable para reducir un volumen de los datos estadísticos no reducidos para obtener los datos estadísticos reducidos, de forma que se mantenga una indicación de una función (característica) de los datos estadísticos no reducidos en los datos estadísticos reducidos, quedando la función enmascarada si los datos estadísticos reducidos estuviesen basados en una agregación de los datos estadísticos no reducidos en cada uno de los intervalos de tiempo de la segunda granularidad de tiempo. Los datos estadísticos reducidos pueden tener otros atributos de los datos reducidos 660 de rendimiento de la red descritos con referencia a las FIGURAS 4A a 4C.

La lógica 702 de transmisión, sin que medie solicitud, puede estar configurada para llevar a cabo funciones de la lógica 694 de análisis del tráfico asociadas con la gestión basada en la transmisión, sin que medie solicitud, según se describe con referencia a la FIG. 6. Por ejemplo, la lógica 702 de transmisión, sin que medie solicitud, puede estar configurada para enviar los datos estadísticos reducidos en una red con independencia de una solicitud en tiempo real procedente de la red. La lógica 702 de transmisión, sin que medie solicitud, puede ser configurable para generar uno o más paquetes que incluyen datos estadísticos reducidos e información de direcciones asociada con un dispositivo ubicado en otro lugar en la red. La lógica 702 de transmisión, sin que medie solicitud, puede ser configurable para anunciar la pluralidad de flujos de datos a un dispositivo ubicado en otro lugar en la red. Con referencia a la FIG. 6, la lógica 702 de transmisión, sin que medie solicitud, puede ser operable para enviar, sin que haya solicitud, los datos estadísticos reducidos mediante comunicaciones que recorren al menos una porción del recorrido 692 de datos.

La lógica 704 de generación de alertas puede estar configurada para llevar a cabo funciones del dispositivo 602 de red (véase la FIG. 2) asociadas con la generación de indicaciones de alerta, según se describe con referencia a la FIG. 2. La lógica 704 de generación de alertas puede estar configurada para generar una indicación de alerta asociada con al menos uno de la pluralidad de flujos 695 de datos (véase la FIG. 8) procesando datos estadísticos para determinar si los datos estadísticos implican una característica asociada con la alerta. La característica puede

adoptar diversas formas conocidas por una persona con un nivel normal de dominio de la técnica relacionadas con los datos de red. Por ejemplo, se puede indicar la característica en función de la aparición de un patrón de bits en los datos de red y/o en función de la aparición de un patrón de variación en una velocidad de transferencia de datos asociada con los datos de la red. De forma alternativa o adicional, la característica puede adoptar diversas formas conocidas por una persona con un nivel normal de dominio de la técnica relacionadas con la operabilidad de los dispositivos de red. Por ejemplo, la característica operativa puede indicarse en función de la existencia de una condición de alarma de un grado particular de gravedad, o puede estar basada en información de configuración, tal como la configuración del soporte físico, del soporte lógico y/o del servicio al cliente. Los datos estadísticos pueden ser medidos mediante al menos una de una pluralidad de máquinas de estado controladas por microcódigo (véase más abajo con referencia a la FIG. 8), y pueden ser medidos en función de los datos de red incluidos en cada uno de una pluralidad de flujos 695 de datos que recorren la al menos una de la pluralidad de máquinas de estado controladas por microcódigo.

En una realización, la lógica 704 de generación de alertas puede estar configurada para determinar si los datos estadísticos implican la característica asociada con la alerta en función del desempeño de una operación matemática sobre los datos estadísticos. La operación matemática puede incluir al menos uno de un mínimo, un máximo, una media, una convolución, una media móvil, una suma de los cuadrados, una operación de filtrado lineal y una operación de filtrado no lineal. La lógica 704 de generación de alertas puede estar configurada para aplicar la operación matemática a los datos estadísticos en múltiples intervalos de tiempo, de forma que se implique la característica asociada con la alerta si el máximo de los datos estadísticos en al menos uno de la pluralidad de intervalos de tiempo es sustancialmente mayor que un valor medio de los datos estadísticos en el al menos uno de los múltiples intervalos de tiempo.

La lógica 706 de análisis del tiempo de espera de la red y de la fluctuación puede estar configurada para llevar a cabo un análisis sobre los datos medidos de tiempo de espera de la red por paquete para obtener información de tiempo de espera de la red por flujo y de fluctuación. Por ejemplo, la lógica 706 de análisis del tiempo de espera de la red y de la fluctuación puede llevar a cabo una operación matemática sobre los datos de tiempo de espera de la red por paquete para obtener información de tiempo de espera de la red por flujo y de fluctuación. La operación matemática puede incluir al menos uno de un mínimo, un máximo, una media, una convolución, una media móvil, una suma de los cuadrados, una operación de filtrado lineal y una operación de filtrado no lineal.

La lógica 708 de cálculo puede estar configurada para llevar a cabo operaciones matemáticas para soportar la lógica 700 de reducción de datos, la lógica 704 de generación de alertas y la lógica 706 de análisis del tiempo de espera de la red y de la fluctuación. La operación matemática puede incluir al menos uno de un mínimo, un máximo, una media, una convolución, una media móvil, una suma de los cuadrados, una operación de filtrado lineal y una operación de filtrado no lineal.

La lógica 710 de control puede estar configurada para procesar información de control recibida procedente de la red (tal como una estación 604 de gestión; véase la FIG. 6) y para convertir la información de control en señales para configurar una o más de la lógica 700 de reducción de datos, de la lógica 702 de transmisión, sin que medie solicitud, de la lógica 704 de generación de alertas, de la lógica 706 de análisis del tiempo de espera de la red y de la fluctuación y de la lógica 708 de cálculo.

La FIG.8 ilustra un diagrama de bloques lógicos de la arquitectura de una realización de la invención. Esta arquitectura puede ser utilizada en el dispositivo 602 de red (véanse las FIGURAS 2 y 6). El dispositivo 602 de red puede ser desplegado como un “tope en el hilo” con tres (o más) interfaces. En una realización, hay una interfaz para el tráfico 695 de entrada de la red, una segunda interfaz para el tráfico 697 de salida de la red y una tercera interfaz 1212 para el tráfico de salida de la red que ha sido duplicado o redirigido, o para comunicaciones de gestión. Los paquetes 695 introducidos desde la red 110 entran en primer lugar un circuito 1202 de distribución. En la realización ilustrada, el circuito 1202 de distribución divide los paquetes 695 introducidos en segmentos de tráfico. En otra realización, los paquetes 695 introducidos son divididos en segmentos por un preprocesador que puede preceder al circuito de distribución. Este preprocesador, que puede ser un núcleo de protocolos personalizado o estándar, también puede proporcionar la funcionalidad de fragmentación/reensamblado y/o de reordenación de los paquetes. Normalmente, un segmento de tráfico es una secuencia de bytes de longitud fija derivada de un único paquete introducido, en el mismo orden que los bytes que entraron en el circuito 1202 de distribución. No se debe confundir un segmento de tráfico con un segmento de protocolo de control de transmisión (TCP), que podría incluir múltiples paquetes. Si un paquete no tiene suficientes bytes restantes para llenar un segmento de tráfico, se dejan sin uso los bytes restantes del segmento de tráfico. Se puede asociar cada byte de un segmento de tráfico con un bit de control que sirve de indicador de validez, marcándose como inválidos los bytes no utilizados.

En la realización ilustrada en la FIG. 8, cada segmento de tráfico es encaminado en paralelo para un procesamiento por parte de cada motor de reglas de un conjunto de motores 1204A - 1204N de reglas, a los que se hace referencia de aquí en adelante como 1204. El circuito 1202 de distribución también mantiene cada uno de los paquetes 695 introducidos hasta que una interfaz 696 de salida indica al circuito 1202 de distribución si el paquete debería ser remitido o borrado, por ejemplo saltándolo. Estos segmentos tienen una anchura en bytes idéntica a la anchura del

bus para segmentos entre el circuito 1202 de distribución y cada motor 1204 de reglas, y entre el circuito 1202 de distribución y la interfaz 696 de salida.

Cada motor 1204 de reglas afirma una indicación de avance al circuito 1202 de distribución cuando está listo para segmentos adicionales de tráfico procedentes del circuito 1202 de distribución. Cuando todos los motores 1204 de reglas han afirmado sus líneas de avance, el circuito 1202 de distribución envía el siguiente segmento de tráfico a todos los motores 1204 de reglas. Cada uno de los motores individuales 1204 de reglas ejecuta una regla configurada. En una realización, cada motor 1204 de reglas evalúa en un valor de verdadero o falso y afirma una línea ejecutada al final de cada paquete.

Después de que un motor 1204 de reglas ha completado la evaluación de una regla, notifica al circuito 1206 de agregación del resultado. Si la regla se evalúa en verdadero, se afirma la línea adaptada al circuito 1206 de agregación. Cuando se completa la evaluación de una regla para una porción de datos, que puede ser el conjunto de segmentos de tráfico obtenidos de la división de uno o más paquetes 695 introducidos, se afirma la línea ejecutada. Las líneas de acción indican al circuito 1206 de agregación si redirigir o duplicar el segmento de datos, y permitir un cambio de escala futuro a interfaces adicionales para su duplicación o redirección. Cuando la salida de un motor 1204A de reglas es invalidar las salidas de un subconjunto de motores 1204B - 1204N de reglas, el motor 1204A de reglas puede afirmar líneas de invalidación correspondientes a ese subconjunto de motores 1204B - 1204N de reglas. En otra realización, el motor 1204A de reglas puede afirmar una línea de invalidación que invalida los motores 1204B - 1204N de reglas.

El circuito 1206 de agregación incluye lógica de salida que impone normativas, que son conjuntos de reglas y la relación lógica, causal y/o temporal entre los mismos. El circuito 1206 de agregación espera hasta que los motores 1204 de reglas afirmen sus bits ejecutados correspondientes antes de tomar una decisión en función de las salidas de todos los motores 1204 de reglas. La decisión, normalmente soltar, remitir o duplicar el paquete, es pasada a la interfaz 696 de salida, junto con el identificador de interfaz de duplicación. El identificador de interfaz de duplicación indica a la interfaz 696 de salida si el paquete está siendo duplicado. El circuito 1206 de agregación afirma un reinicio al circuito 1202 de distribución cuando el circuito 1206 de agregación determina que el circuito 1202 de distribución puede saltarse todos los segmentos restantes del paquete actual e ir directamente al procesamiento del siguiente paquete. Puede ser deseable que el circuito 1206 de agregación también soporte la duplicación o redirección del tráfico a la interfaz 1212 de gestión.

Cuando se debe remitir un paquete, la interfaz 696 de salida solicita mediante la siguiente línea de paquetes que se le envíe el siguiente paquete desde el circuito 1202 de distribución. Durante la transferencia del siguiente paquete, la interfaz 696 de salida afirma una indicación de siguiente segmento al circuito 1202 de distribución cuando está lista para uno o más segmentos adicionales de tráfico desde el circuito 1202 de distribución. En una realización, cuando la interfaz 696 de salida recibe segmentos de tráfico procedentes del circuito 1202 de distribución, la interfaz 696 de salida puede introducir en memoria intermedia parte del paquete, o todo él, la interfaz 696 de salida puede introducir en memoria intermedia parte del paquete, o todo él, según sea necesario, antes de transmitirlo como un paquete 697 de salida. Esto depende de las funciones de postprocesamiento que puede ser necesario llevar a cabo, que pueden incluir, sin restricción, una codificación. En otra realización, se pueden enviar segmentos del paquete según son recibidos por la interfaz 696 de salida. En ese modo de operación, si la decisión del circuito 1206 de agregación es soltar el paquete, entonces se trunca el paquete y se vuelve prácticamente inutilizable para el equipo conectado que recibe el paquete.

Para un procesamiento de paquetes y de corrientes, no es preciso que haya implicación de ninguna unidad central de procesamiento (CPU) de uso general. Hay una interfaz de gestión general/de instrucciones/de control disponible para un equipo externo, que normalmente contiene una CPU, para controlar el circuito 1202 de distribución, el circuito 1206 de agregación y todos los motores 1204 de reglas mediante el control del circuito 1206 de agregación.

Una realización de un motor 1204 de reglas es una máquina de estado controlada por microcódigo que ejecuta una regla configurada basada en comportamiento o firma. Se compila una regla a un conjunto de bits, o microcódigo, que se utiliza para programar la máquina de estado controlada por microcódigo y los registros asociados de configuración. Cada máquina de estado controlada por microcódigo incluye una rutina de cálculo que opera según el microcódigo almacenado en un almacenamiento asociado de control. Las máquinas de estado controladas por microcódigo configuran un recorrido optimizado de datos para llevar a cabo tales operaciones como operaciones de paridad, de paridad enmascarada, y de inclusión/exclusión de alcance sobre cada segmento de tráfico. El recorrido de los datos comprende etapas delgadas cuya implementación requiere únicamente algunos niveles lógicos, permitiendo, de esta manera, un diseño de frecuencia muy elevada.

Se puede implementar el conjunto de motores 1204 de reglas como un tejido de procesamiento en cadena de máquinas de estado controladas por microcódigo que operan de forma simultánea y colaborativa sobre cada segmento de tráfico. Esta estructura regular se presta a la creación de diseños paralelos de alta capacidad mediante la reiteración de un número pequeño de bloques fundamentales de construcción. También proporciona una capacidad para preservar la información del estado, tal como información de conexión de TCP, localmente en la máquina relevante de estado controlada por microcódigo como parte de su estado. A diferencia del enfoque típico en

cortafuegos de información de estado, que preserva todas las conexiones en una memoria compartida, este tejido también permite que se almacene información de estado como un estado local de una única máquina de estado controlada por microcódigo. Sin embargo, la arquitectura también soporta una tabla global de estado (que puede contener información de conexión) que está disponible globalmente para todos los motores 1204 de reglas. La tabla de estado global puede mantenerse en una CAM o una memoria externa, y puede implementarse como memoria en chip. Si se encuentra en una CAM o una memoria externa, se puede acceder a la tabla de estado global por medio de los motores 1204 de reglas mediante la interfaz 1212 de gestión, que es responsable de un controlador que mantiene la información de estado y presenta información relevante de estado pertinente al paquete actual a todos los motores de reglas. Los motores 1204 de reglas pueden acceder simultáneamente a la información en la tabla de estado global, tal como mediante líneas de señal de soporte físico a cada motor 1204 de reglas. En la presente realización, no se malgasta ningún ciclo de reloj gestionando colas de solicitudes de consultas a una CAM o a una memoria externa. La tabla de estado global puede ser actualizada paquete por paquete por medio de un soporte físico dedicado. Esta arquitectura, junto con su conjunto asociado de instrucciones, también puede ser personalizada y optimizada. Esto permite un procesamiento eficaz, fácilmente configurable y unificado de la cabecera y una inspección profunda de las cargas útiles de paquete.

El circuito 1206 de agregación incluye lógica de salida que impone normativas. Una normativa puede ser una colección sencilla de reglas relacionadas con el uso de lógica booleana. En una realización, el circuito 1206 de agregación agrega las salidas de bloques individuales, por ejemplo expresadas como una O booleana de varias reglas. Si cualquiera de estas múltiples reglas es un árbol, en el que se puede configurar cada nodo del árbol para que funcione como una O o Y lógica. Se puede configurar una normativa para que sea una relación compuesta complicada entre reglas, tal como una suma de productos y/o una relación causal o temporal. La lógica de agregación puede implementar cualquier lógica combinatoria o secuencial.

En una realización, el circuito 1206 de agregación genera señales de control para activar y desactivar un subconjunto de uno o más del conjunto de motores 1204 de reglas. La lógica de agregación también puede reiniciar o proporcionar una información de retorno de reglas al subconjunto de motores 1204 de reglas, y puede establecer parámetros utilizados por el circuito 1202 de distribución. Un motor 1204 de reglas puede incluir lógica y puede generar señales de control para activar y desactivar directamente uno o más motores adicionales de reglas.

Con referencia a las FIGURAS 6 y 8, la lógica 682 de procesamiento del recorrido de los datos puede incluir el circuito 1202 de distribución, las una o más máquinas 1204 de estado controladas por microcódigo y el circuito 1206 de agregación. El recorrido 692 de los datos puede incluir al menos un circuito 1202 de distribución, la interfaz 696 de salida y conexiones con el circuito 1202 de distribución y la interfaz 696 de salida recorridas por los paquetes de datos incluidos en uno o más de los flujos 695 de datos que recorren el dispositivo 602 de red.

La FIG. 8 ilustra un ejemplo de una arquitectura paramétrica, que permite el cambio de escala de métrica de rendimiento clave, tal como el caudal de proceso, con parámetros de diseño, tales como la anchura del segmento de tráfico, sin cambiar la estructura fundamental de la arquitectura. Se pueden utilizar segmentos más anchos de tráfico, que se corresponden con un recorrido más ancho de los datos, para aumentar el caudal de proceso total del sistema transmitiendo, sin que medie solicitud, más bits por ciclo de reloj del soporte físico a través del aparato. Es posible afinar la anchura del recorrido de los datos y alcanzar una solución de compromiso entre el uso de recursos (puertas) de silicio y la frecuencia operativa del aparato. Se puede calcular con precisión el caudal de proceso más desfavorable a través del aparato multiplicando la anchura del segmento de tráfico por el número de ciclos de reloj por segundo dividido por el número más desfavorable de ciclos de reloj por segmento de tráfico. Para aplicaciones típicas, el número más desfavorable de ciclos de reloj por segmento de tráfico es inferior a cinco, preferentemente dos. Se puede calcular con precisión el tiempo de espera más desfavorable dependiendo de si la normativa de desvío es almacenar y remitir o conmutar. Para almacenar y remitir, el tiempo de espera más desfavorable es directamente proporcional al cociente del número de segmentos en dos paquetes de tamaño máximo dividido por la frecuencia del reloj. El tiempo de procesamiento es lineal en el número de segmentos de tráfico en un paquete.

La arquitectura ilustrada en la FIG. 8 está diseñada para ser óptima, específicamente, para aplicaciones de monitorización de la red, de análisis del tráfico y de seguridad. Sin embargo, esta arquitectura también es suficientemente general para implementar una correspondencia de patrones de uso general, incluyendo aplicaciones de clasificación de paquetes, de inspección profunda y de base de datos sobre la marcha. El denominador común es el concepto de procesamiento de datos un segmento cada vez, siendo el tamaño de un segmento un parámetro de diseño de una arquitectura paramétrica.

Las reglas utilizadas por los motores 1204 de reglas pueden especificarse de varias formas, incluyendo sin limitación la configuración de bits del soporte físico, el uso de un ensamblador de bajo nivel, la traducción de lenguajes existentes utilizados por los sistemas de detección de intrusos (IDS) y los cortafuegos comunes, o el uso de un lenguaje de alto nivel. En una realización, se utiliza un ensamblador de bajo nivel, basado en una arquitectura de conjunto de instrucciones (ISA) única y patentada correspondiente a una arquitectura subyacente de soporte físico optimizada para aplicaciones de seguridad de la red. En otra realización, se utiliza un lenguaje de alto nivel, con definición de reglas a medida, basado en un lenguaje patentado de alto nivel para la sección de entrada de

inspección de corrientes y paquetes (SPIFE). Algunos ejemplos de reglas en un lenguaje de alto nivel de definición de reglas incluyen:

drop inbound eth:ip:tcp ip.src = 1.2.3.4, tcp.dport = 80;
Significado: soltar paquetes de TCP que están entrando (de la red externa hacia el segmento protegido), que tienen una dirección IP fuente de 1.2.3.4 y un puerto 80 de destino (http).
drop inbound eth:ip:udp payload: “malicious”;
Significado: soltar paquetes de protocolo de datagrama de usuario (UDP) que están entrando (de la red externa hacia el segmento protegido) si su carga útil contiene la palabra clave “malicious”.
drop inbound eth:ip:udp payload: “malic*ious” [ignorecase];
Significado: soltar paquetes de protocolo de datagrama de usuario (UDP) que están entrando (de la red externa hacia el segmento protegido) si su carga útil incluye la palabra clave “malicious” en la que un número cualquiera de caracteres separa la “c” de la “i”. La carga útil no distingue entre mayúsculas y minúsculas, de forma que, por ejemplo, se sueltan “Malicious”, “mAliCious” y “MALICIOUS”.
count all inbound eth:ip:icmp icmp.type = PING_REPLY;
Significado: contar los paquetes de rastreo-respuesta de protocolo de mensajes de control de Internet (ICMP) enviados por las capas de protocolo IP y de Ethernet.
duplicate all inbound eth:ip:icmp icmp.type = PING_REPLY;
Significado: duplicar los paquetes entrantes de rastreo-respuesta de ICMP enviados por las capas de protocolo IP y de Ethernet a la tercera interfaz sin interferir con el flujo normal de paquetes de la primera interfaz a la segunda interfaz, o desde la segunda interfaz a la primera interfaz.
redirect all inbound eth:ip:icmp icmp.type = PING_REPLY;
Significado: redirigir los paquetes entrantes de rastreo-respuesta de ICMP enviados por las capas de protocolo IP y de Ethernet a la tercera interfaz.

La FIG. 9 ilustra el uso de la arquitectura de la FIG. 8 para aplicaciones bidireccionales, según una realización de la invención. Un ejemplo son las aplicaciones cliente-servidor, para las que es deseable monitorizar los comportamientos de protocolo bidireccional o el desencadenamiento de eventos. Si el servidor se encuentra fuera de la porción de la red protegida por el aparato y el cliente se encuentra dentro de esa porción de la red, el tráfico procedente del servidor es entrante y las solicitudes y respuestas de ese cliente son salientes. Los paquetes entrantes 695 de entrada son procesados por el circuito 1202 de distribución, el conjunto de motores 1204 de reglas y el circuito 1206 de agregación para obtener paquetes entrantes 697 de salida. La interfaz 696 de salida no se muestra en la FIG. 9 en aras de la sencillez. Los paquetes salientes 1300 de entrada son procesados por el circuito 1302 de distribución, un conjunto de motores 1304 de reglas y el circuito 1306 de agregación para obtener paquetes salientes 1310 de salida. El circuito 1202 de distribución, el conjunto de motores 1204 de reglas y el circuito 1206 de agregación forman un primer recorrido en la primera dirección, o de entrada, y puede alinearse con el circuito diferenciado 1302 de distribución, el conjunto de motores 1304 de reglas y el circuito 1306 de agregación que forman un segundo recorrido en una segunda dirección, o de salida, distinta, tal como opuesta, de la primera dirección. El alineamiento en este contexto es conceptual, y no implica ninguna restricción sobre el posicionamiento físico mutuo de estos bloques en una implementación. Para gestionar las aplicaciones bidireccionales, puede ser deseable que el conjunto de motores 1204 de reglas intercambie información de control con el conjunto de motores 1304 de reglas. En otra realización, cada motor 1204 de reglas podría alternar dinámicamente entre el procesamiento de tráfico del primer recorrido y del segundo recorrido. Esta alteración dinámica puede ser controlada por microcódigo, y también puede ser controlada por los bits de configuración del motor 1204 de reglas. Los motores 1204 de reglas pueden alternar entre el procesamiento de tráfico del primer recorrido y del segundo recorrido de forma independiente y/o como un grupo.

La FIG. 10 ilustra una realización de la arquitectura interna del circuito 1202 de distribución mostrado en la FIG. 8, según una realización de la invención. Los paquetes 695 de entrada introducen una memoria intermedia 1320 de tramas. En la presente realización, la memoria intermedia 1320 es una memoria intermedia FIFO, y está organizada de forma lógica en tamaños de segmento iguales a la anchura del recorrido de los datos a través del aparato. Los paquetes 695 de entrada pueden haber sido divididos ya en segmentos de tráfico por medio de un preprocesador, en cuyo caso puede no requerirse la memoria intermedia 1320 de tramas. De lo contrario, se colocan los paquetes 695 de entrada en la memoria intermedia 1320 de tramas con un separador entre los paquetes 695 de entrada. La memoria intermedia 1320 de tramas lógicamente tiene un puerto de escritura, para los paquetes de entrada, y dos puertos de lectura, uno para un bloque lógico 1324 de distribución y el otro para la interfaz 696 de salida. Una

implementación estándar de tal memoria intermedia utiliza dos bloques separados de memoria, de tal forma que uno se encuentre cerca de la interfaz de entrada y uno se encuentre cerca de la interfaz de salida. En una implementación de almacenar y remitir, un paquete permanece almacenado en la memoria intermedia 1320 de tramas hasta que se ha comunicado por medio del circuito 1206 de agregación una decisión de los motores 1204 de reglas a la interfaz 696 de salida, provocando que la interfaz 696 de salida afirme la siguiente línea de paquetes. En una implementación de conmutación, cada segmento de tráfico de un paquete es remitido sin retraso a la interfaz 696 de salida. Se puede enviar una señal de aborto a la interfaz 696 de salida para provocar que la interfaz 696 de salida corrompa una porción del paquete para provocar que el paquete sea desechado por los dispositivos en el extremo de recepción en la red. Tanto la memoria intermedia 1320 de tramas como la lógica 1324 de distribución pueden tener interfaces de gestión/de instrucción/de control.

La lógica 1324 de distribución saca un segmento de datos de la memoria intermedia 1320 de tramas cuando todos los motores conectados 1204 de reglas están listos para el siguiente segmento de datos, según se indica por su negación de sus líneas de control de avance a la lógica 1324 de distribución. Si uno o más de los motores 1204 de reglas no está listo, la lógica 1324 de distribución niega la línea de control de avance a la memoria intermedia 1320 de tramas y espera hasta que todos los motores 1204 de reglas están listos. La lógica 1324 de distribución recibe el reinicio del circuito 1206 de agregación, descrito con referencia a la FIG. 8, que provoca que la lógica 1324 de distribución se salte todos los segmentos restantes del paquete actual y vaya directamente al procesamiento del siguiente paquete.

La FIG. 11 ilustra el diseño interno de un motor 1204 de reglas basado en una máquina de estado controlada por microcódigo configurada según una realización de la invención. El diseño está basado en una máquina programable personalizada de estado con una memoria local independiente. Normalmente, la memoria es memoria estática de acceso aleatorio (SRAM), pero puede ser de un tipo distinto. La programación de la máquina de estado se lleva a cabo escribiendo contenido en una memoria 1406 de almacenamiento de control. Las implementaciones de *bus* para permitir la lectura de la memoria local distribuida, y la escritura en la misma, son bien conocidas en la técnica. También se contempla que el motor 1204 de reglas pueda ser implementado de diversas formas, tales como utilizando circuitos integrados para aplicaciones específicas (ASIC) o dispositivos de lógica programable (PLD).

Cada motor 1204 de reglas puede contener una pequeña memoria intermedia local 1400 de primero en entrar y en salir (FIFO) para contener segmentos de tráfico recibidos procedentes del circuito 1202 de distribución mientras cada motor 1204 de reglas se encuentra procesando un segmento precedente. Si está presente, esta memoria intermedia indica a la lógica de distribución mediante la línea de avance cuándo puede aceptar segmentos adicionales.

El fin de la memoria intermedia local es evitar periodos de tiempo durante los que no hay datos disponibles para ser procesados por un motor 1204 de reglas (retrasos). Se puede visualizar la memoria intermedia local como una ventana de longitud fija que se desliza sobre los datos de entrada. Se proporciona un segmento de tráfico a cada motor 1204 de reglas por medio del circuito 1202 de distribución cuando se ha afirmado a todos los motores 1204 de reglas sus líneas de avance, lo que indica que las memorias intermedias locales de todos los motores 1204 de reglas tienen espacio para el segmento de tráfico. Los segmentos de tráfico que ya están en las memorias intermedias locales de los motores 1204 de reglas están disponibles para un procesamiento en paralelo por todos los motores 1204 de reglas. Como resultado, un motor 1204 de reglas que ha completado el procesamiento de un primer segmento de tráfico puede recibir inmediatamente, sin que medie solicitud, el siguiente segmento de tráfico de la memoria intermedia local, sin ser retrasado por otro motor 1204 de reglas que aún no ha completado el procesamiento del primer segmento. Dado que hay un máximo número de comparaciones y, por lo tanto, de ciclos de procesamiento, requeridos para aplicar una regla a un segmento de tráfico, se puede acotar el tamaño de esta memoria intermedia local. Normalmente, el procesamiento de un segmento de tráfico por medio de un motor 1204 de reglas no requiere más de dos ciclos. Si se establece entonces dos ciclos como el número de ciclos de procesamiento para cualquier segmento de tráfico, deslizar la ventana cada dos ciclos el número de bytes requerido para incluir el siguiente segmento de tráfico garantiza que ninguna de las memorias intermedias locales se llena.

Un bloque 1402 de lógica de condición indica mediante una línea de avance cuándo está listo para recibir el siguiente segmento de datos procedente de la memoria intermedia 1400 de entrada o directamente procedente del circuito 1202 de distribución. La lógica de condición está configurada por cada línea de microcódigo para llevar a cabo una o más comparaciones en el segmento actual y, en función de las comparaciones, seleccionar el siguiente estado utilizando un selector 1404. La lógica 1402 de condición y el selector 1404 están incluidos en una rutina 1403 de cálculo. La lógica 1402 de condición implementa operaciones combinatorias al igual que lógica secuencial, que depende de su estado interno. En la presente realización, el siguiente estado es la dirección de la siguiente instrucción de microcódigo que ha de ser ejecutada. Además, la lógica 1402 de condición establece las indicaciones de ejecutado, correspondencia, acción e invalidación proporcionadas al circuito 1206 de agregación. La lógica de agregación puede generar señales de control para activar y desactivar la lógica 1402 de condición, o para proporcionar una información de retorno de reglas a la lógica 1402 de condición.

Cada línea de microcódigo en el almacenamiento 1406 de control determina qué tipo de comparación llevar a cabo en el segmento actual de tráfico. En función de los resultados de la comparación, la línea de microcódigo también

proporciona la dirección de la siguiente línea de microcódigo que ha de ser ejecutada. En una realización, cada línea en el almacenamiento 1406 de control incluye cuatro tipos de información:

1. Bits de control (tales como códigos de operación o bits de configuración) que determinan qué tipo de comparaciones lleva a cabo la lógica 1402 de condición, y qué estado interno debería almacenarse en variables internas de estado (flops y registros).

2. Valores utilizados por las comparaciones. Los tipos de comparación incluyen paridad, pertenencia a un conjunto, comparación de alcance y operaciones más complejas, tales como comparaciones de contador que indican si se ha producido una secuencia de bits más de 3 veces en los anteriores 10 segmentos.

3. Direcciones de direcciones subsiguientes que han de ser ejecutadas en función de la salida de la lógica 1402 de condición. Dependiendo del resultado de la lógica 1402 de condición, se puede seleccionar una de múltiples siguientes direcciones. Permitir más de una siguiente dirección permite una mayor flexibilidad para implementar condiciones complejas, mientras haya ciclos de reloj.

4. Control del estado interno y salidas primarias del motor 1204 de reglas. Por ejemplo, esto puede incluir si se afirma o no la línea ejecutada, ya sea para hacer avanzar el siguiente segmento en el paquete o para mantenerse para otra comparación que implique el segmento actual, o si moverse inmediatamente al extremo del paquete actual.

Estos distintos tipos de comparaciones, junto con la arquitectura, permiten el procesamiento tanto de paquetes individuales como de corrientes de paquetes por medio del conjunto de motores 1204 de reglas. Un motor 1204 de reglas puede procesar una corriente sin reconstruirla completamente en realidad en la memoria externa del sistema. En función de las instrucciones de microcódigo, el motor 1204 de reglas puede tomar decisiones que están basadas en una secuencia de eventos que se producen con el paso del tiempo y que están encapsulados en distintos paquetes.

La FIG. 12 muestra un ejemplo de una secuencia de ejecución de instrucciones de microcódigo para implementar una regla de comparación, según una realización de la invención. La secuencia de búsquedas para una secuencia de cuatro bytes “abcd” en dos segmentos sucesivos (se supone que cada uno es de 2 bytes), seguida por una secuencia de dos bytes con un valor entre “10” y “14”, ambos inclusive. Para un paquete de veinte bytes que se representa simbólicamente como “1234yzwxabcd12345678”, el estado real hace una transición desde el inicio del paquete hasta que una decisión sea 0 -> 1 -> 1 -> 1 -> 1 -> 1 -> 2 -> 3 -> 4. Cuando el motor 1204 de reglas alcanza el estado 4, afirma las salidas tanto de ejecutado como de correspondencia al circuito 1206 de agregación en la FIG. 8. Si los paquetes de datos no incluyen el contenido deseado, entonces en cuanto el SEGMENTO es igual al separador de paquetes de dos bytes “- -”, hay una transición automática al estado 5. En el estado 5, el motor 1204 de reglas afirma la línea ejecutada y niega la línea adaptada.

El número de operaciones que pueden ser ejecutadas en paralelo en el SEGMENTO y su tipo depende de la implementación específica de soporte físico, incluyendo la anchura de la línea de memoria del almacenamiento de control. Este ejemplo supone que la comparación del SEGMENTO con un valor dado y la comprobación de si el SEGMENTO se encuentran dentro de un alcance dado pueden realizarse en paralelo. De lo contrario, las operaciones pueden realizarse en dos ciclos de reloj consecutivos separados. Por ejemplo, el estado 3 realiza dos comprobaciones en paralelo y supone que los siguientes tres valores de dirección pueden ser especificados en una línea de memoria del almacenamiento de control.

La FIG. 13 ilustra un ejemplo de la implementación de la lógica de condición de la FIG. 11, según una realización de la invención. En función del segmento introducido procedente de la memoria intermedia local 1400 y del código de operación y de los bits de configuración procedentes del almacenamiento 1406 de control, se puede realizar un conjunto de comparaciones en paralelo entre el segmento, los operandos y las variables internas de estado. Un operando es un valor configurado utilizado para una comparación. Una variable interna de estado incluye valores almacenados en flops, registros, o contadores, tal como estadística. Estos valores incluyen el resultado de comparaciones entre valores almacenados, tales como el número de veces que el valor en un primer contador ha superado el valor en un segundo contador. En la presente realización, cada bloque 1402 de lógica de condición tiene dos contadores que se dedican a contar el número de paquetes y el número total de segmentos (o bytes) que han sido procesados por el microcódigo en el almacenamiento 1406 de control. También hay contadores y registros de estado asociados con interfaces de entrada, de salida y de gestión. Las comparaciones pueden realizarse entre registros y contadores locales y/o contadores globales.

Cada subbloque en la FIG. 13 implementa una comparación específica. Se implementan comparaciones de operandos con datos tales como una comprobación de paridad 1502 y de alcance 1504 por medio de circuitos 1500 de comprobación de condición, que son utilizados para evaluar reglas basadas en firma. La modificación del estado interno almacenado en flops, registros o contadores 1510 y comparaciones entre un estado interno variable y un operando 1512 (u otro registro/variable interno de estado o un contador/variable global de estado) se implementan mediante circuitos 508 de análisis de la condición, que pueden ser utilizados para evaluar reglas de comportamiento o para recoger estadística. Existe una actualización automática de los estados internos, tales como el número de

bytes del paquete actual que han sido procesados hasta entonces, según se especifica mediante el código de operación y las entradas de configuración. Los resultados de las comparaciones paralelas entre subbloques son aumentados por un bloque en un bloque configurable 1514 de lógica de salida (booleana o secuencial o ambas). La selección de la siguiente dirección utilizada por el selector 1404 y las salidas de las máquinas de estado controladas por microcódigo visibles al circuito 1206 de agregación están configuradas por la lógica configurable 1514 de salida.

Las realizaciones de la presente invención permiten la modificación del tráfico de la red que puede tener una granularidad bit a bit (ser granular hasta el bit) en cualquier lugar en el tráfico de la red. Se puede modificar el tráfico de la red en forma de paquetes en cualquier lugar en la carga útil o en la cabecera del paquete. Estas modificaciones a la carga útil o la cabecera del paquete pueden incluir cambios de uno o más bits existentes, la inserción de uno o más bits, y la eliminación de uno o más bits. También se contempla que las realizaciones de la presente invención permitan una reflexión selectiva del tráfico de entrada con una granularidad bit a bit, de forma que solo se dirija el tráfico que necesita ser mirado en detalle a una entidad con una menor velocidad de transferencia de procesamiento de paquetes, tal como una CPU o un analizador de protocolo.

Con referencia a la FIG. 8, la arquitectura de una realización de la invención también soporta modificaciones y una reflexión granulares del tráfico. Después de completar la evaluación de una regla para un segmento de datos correspondiente a uno o más paquetes 695 de entrada, cada motor 1204 de reglas notifica al circuito 1206 de agregación mediante líneas de instrucción de modificaciones que han de ser realizadas a cada paquete en el segmento de datos. Las instrucciones de modificación indicadas por un motor 1204A de reglas pueden ser idénticas a las instrucciones de modificación, o solaparse a las mismas, indicadas por uno o más de los otros motores 1204B - 1204N de reglas. La lógica en el circuito 1206 de agregación que puede incluir lógica tanto secuencial como combinatoria combina las instrucciones de modificación indicadas por los motores 1204 de reglas en una orden de modificación que incluye indicaciones de todas las modificaciones que han de ser realizadas a cada paquete en el segmento de datos. Cuando se combinan las instrucciones de modificación indicadas por los motores 1204 de reglas en la orden de modificación, el circuito 1206 de agregación puede eliminar o modificar instrucciones de modificación para eliminar la redundancia.

Para cada paquete en el segmento de datos, la interfaz 696 de salida normalmente responde a una orden de modificación procedente del circuito 1206 de agregación si la interfaz 696 de salida ha recibido indicaciones del circuito 1206 de agregación en la línea de decisión de que el paquete sea remitido, redirigido o duplicado. Dado que el circuito 696 de salida recibe segmentos de tráfico procedentes del circuito 1202 de distribución en respuesta a las indicaciones del siguiente paquete y del siguiente segmento, el circuito 696 de salida puede introducir en memoria intermedia parte de un paquete, o todo él, para facilitar la modificación del paquete por medio del circuito 696 de salida. El circuito 696 de salida puede contener memoria que almacena la orden de modificación o una versión procesada de la orden de modificación. Como parte de la modificación del paquete, el circuito 696 de salida puede modificar campos en el paquete utilizados para la detección de errores o la corrección de errores, tal como el campo de secuencia de comprobación de tramas (FCS) o de comprobación cíclica de la redundancia (CRC) para la cabecera, la carga útil o todo el paquete. Si el circuito 696 de salida inserta campos en un paquete o encapsula un paquete con una nueva cabecera, se pueden añadir al paquete uno o más campos nuevos para la detección de errores o la corrección de errores.

En función de las salidas de los motores 1204 de reglas, el circuito 1206 de agregación utiliza las líneas identificadoras de la interfaz de duplicación para indicar a la interfaz 696 de salida que se está redirigiendo o duplicando un paquete, y la o las interfaces a las que se está enviando el paquete. El paquete redirigido o duplicado puede ser modificado por la interfaz 696 de salida. Los datos reflejados pueden corresponderse con uno o más puertos 800 que pueden ser cualquier combinación de puertos físicos y lógicos. Los datos reflejados pueden ser datos redirigidos a la interfaz 1212 de gestión desde la interfaz 696 de salida o datos duplicados dirigidos a la interfaz 1212 de gestión y también remitidos desde la interfaz 696 de salida. Alguna combinación de la interfaz 696 de salida y la interfaz 1212 de gestión puede tener una cantidad limitada de memoria para la correspondencia de velocidades de transferencia de datos de los segmentos de tráfico que entran en la interfaz 1212 de gestión desde el circuito 1202 de distribución hasta la salida de la interfaz 1212 de gestión. También se puede llevar a cabo cualquier correspondencia de velocidades de transferencia de datos mediante dispositivos externos conectados con la interfaz 1212 de gestión. La salida de la interfaz 1212 de gestión puede combinar datos reflejados y comunicaciones de gestión o de control.

Las modificaciones de paquetes pueden facilitar la seguridad y la monitorización de la red, tal como permitiendo una monitorización selectiva de tráfico sospechoso, evitando ataques, o mitigar ataques en curso. Por ejemplo, se pueden modificar los paquetes 695 de entrada en la FIG. 8 con un número no estándar o no asignado de puertos TCP, utilizando la arquitectura mostrada en la FIG. 8, formando paquetes 697 de salida con un número de puertos TCP correlacionados con una aplicación segura corriente abajo para una monitorización. Los paquetes 695 de entrada de fuentes desconocidas con opciones no autorizadas de protocolo de Internet (IP) pueden ser modificados creando paquetes 697 de salida, por ejemplo, con las opciones de IP borradas o modificadas para ser no operativas para evitar o mitigar ataques. Los paquetes 695 de entrada con direcciones IP falsificadas pueden ser modificados formando paquetes 697 de salida con la dirección IP de un dispositivo corriente abajo de monitorización.

Esta modificación también puede facilitar la gestión de tráfico además, o con independencia, de facilitar la seguridad de la red. Por ejemplo, los paquetes 695 de entrada pueden ser modificados creando paquetes 697 de salida con una etiqueta insertada de red de área local virtual (VLAN) o con una etiqueta de conmutación multiprotocolo basada en etiquetas (MPLS) que pueden corresponderse con el envío, por parte del cliente, de los paquetes 695 de entrada a un segmento específico de LAN en el caso de la etiqueta de VLAN, o con un túnel específico de MPLS en el caso de la etiqueta de MPLS. Esto es un ejemplo de etiquetado de paquetes. Los paquetes 695 de entrada también pueden ser modificados formando paquetes 697 de salida con una etiqueta de conmutación multiprotocolo basada en etiquetas (MPLS) que contiene una marca de calidad de servicio que indica el tipo de procesamiento que debe recibir este paquete de los dispositivos corriente abajo. Esta operación es un ejemplo de coloración de paquetes.

Esta modificación también puede facilitar la integración de dispositivos en un sistema. Por ejemplo, los paquetes 695 de entrada pueden ser modificados formando paquetes 697 de salida que tienen una cabecera encapsulada. Esta cabecera encapsulada puede transmitir información de control de significado para un dispositivo corriente abajo particular. Un fin común de la encapsulación de cabeceras es indicar los resultados de preprocesamiento de paquetes 695 de entrada por un dispositivo con la arquitectura mostrada en la FIG. 8, de forma que los dispositivos corriente abajo, tales como NP, que reciben paquetes 697 de salida no necesiten repetir el mismo procesamiento, ahorrando recursos de cálculo y mejorando el rendimiento de la red.

Se utiliza la reflexión para dirigir tráfico de entrada a una entidad tal como una CPU o un analizador de protocolo para una monitorización y un análisis detallados del tráfico. Es deseable una reflexión selectiva entre los puertos 800 de entrada debido a que una CPU o un analizador de protocolo normalmente no puede procesar paquetes a la misma velocidad de transferencia de datos que la arquitectura de la FIG. 8, que está diseñada para altas velocidades de transferencia de datos de múltiples gigabits por segundo.

La reflexión con granularidad bit a bit permite una reflexión selectiva, precisa, quirúrgica. El uso de la arquitectura mostrada en la FIG. 8 para filtrar flexiblemente el tráfico de alta velocidad permite el uso de una CPU o un analizador de protocolo para tráfico dirigido de manera precisa enviado por la interfaz 1212 de gestión. Tampoco hay restricción sobre los tipos de puertos 800, tales como un puerto físico o un puerto lógico definido por una LAN virtual, que puede ser reflejado a la interfaz 1212 de gestión. Por ejemplo, puede ser deseable inspeccionar únicamente paquetes que comuniquen cotizaciones de bolsa o de una página Web particular. La inspección profunda de paquetes soportada por la arquitectura de la FIG. 8 permite la aplicación de reglas, incluyendo reglas basadas en firma, en las que la firma puede aparecer en la cabecera o carga útil de paquetes individuales, o en una secuencia de paquetes. Las reglas de comportamiento también pueden integrarse con reglas basadas en firma para definir los criterios para una reflexión selectiva. El filtrado del tráfico de alta velocidad que utiliza una combinación de reglas de comportamiento y basadas en firma puede adaptarse para generar una solución a nivel del sistema que aprovecha mejor las capacidades de procesamiento de la CPU o del analizador de protocolo, sin requerir NP ni CAM costosos. Por ejemplo, la arquitectura de la FIG. 8 puede aplicar una regla incluyente basada en firma para el tráfico reflejado si la carga de tráfico reflejado es sustancialmente menor que la máxima capacidad de procesamiento del analizador de protocolo, y puede aplicar reglas basadas en firma progresivamente más estrictas según se aproxima la carga de tráfico reflejado a la máxima capacidad de procesamiento del analizador de protocolo.

La arquitectura de la FIG. 8 está basada en soporte físico y optimizada para aplicaciones de análisis de cabecera, de inspección profunda de paquetes y de modificación de paquetes. En particular, la arquitectura no incorpora diseños de componentes de uso general tales como CPU. Para evitar un rediseño intrusivo del soporte físico, de registros y de soporte lógico de bajo nivel de NP y de conmutadores, una forma sencilla para incorporar esta arquitectura en componentes de serie existentes es integrar la arquitectura en un componente en la capa física (PHY) o en una combinación de la PHY y de la subcapa de control de acceso a los medios (MAC) del modelo de referencia de interconexión de sistemas abiertos (OSI) de siete capas para capas de protocolo de red. Estas capas, moviéndose hacia arriba desde bits no tratados en un canal de comunicaciones hasta protocolos de aplicación utilizados comúnmente por los usuarios finales, incluyen la capa física, la capa de enlace de datos, la capa de red, la capa de transporte, la capa de sesión, la capa de presentación y la capa de aplicación. La división de las capas del modelo de referencia OSI está basado en principios que incluyen una definición clara de las funciones llevadas a cabo por cada capa, una abstracción de capas para minimizar dependencias entre capas y una facilitación de la definición de estándares.

Con referencia a la FIG. 8, la arquitectura de una realización de la invención también soporta la reducción de datos, la gestión basada en la transmisión, sin que medie solicitud, la generación de alertas y el análisis del tiempo de espera de la red y de la fluctuación. Según se ha descrito con referencia a la FIG. 7, estas funciones están soportadas por lógica incluida en la lógica 694 de análisis del tráfico. En una realización, la lógica 694 de análisis del tráfico incluye lógica de soporte físico dedicada para llevar a cabo cada una de estas funciones. Se puede incluir la lógica 694 de análisis del tráfico, junto con el resto de la arquitectura mostrada en la FIG. 8, en un único *chip*. El único *chip* puede ser un sistema en chip, y puede incluir uno o más circuitos integrados. La lógica 694 de análisis del tráfico, junto con el resto de la arquitectura mostrada en la FIG. 8, puede implementarse en circuitería de soporte físico y/o en lógica reconfigurable. De forma alternativa, la lógica 694 de análisis del tráfico puede implementarse en soporte lógico inalterable.

La lógica 694 de análisis del tráfico puede estar configurada para recibir información relacionada con los datos de la red (tal como la información 686 relacionada con los datos de la red descrita con referencia a la FIG. 6) e información de identificación del flujo procedente de las máquinas 1204 de estado controladas por microcódigo. Con referencia a la FIG. 7, una o más de la lógica 700 de reducción de datos, la lógica 702 de transmisión, sin que medie solicitud, la lógica 704 de generación de alertas, la lógica 706 de análisis del tiempo de retraso de la red y de la fluctuación, la lógica 708 de cálculo y la lógica 710 de control están configuradas para procesar la información relacionada con los datos de la red y la información de identificación del flujo como parte del desempeño de sus funciones. Además, la lógica 694 de análisis del tráfico puede estar configurada para recibir información de control (tal como la información 688 de control descrita con referencia a la FIG. 6) procedente del circuito 1202 de distribución. Con referencia a la FIG. 7, la lógica 710 de control puede estar configurada para procesar la información de control, y para convertir la información de control en señales para configurar una o más de la lógica 700 de reducción de datos, la lógica 702 de transmisión, sin que medie solicitud, la lógica 704 de generación de alertas, la lógica 706 de análisis del tiempo de espera de la red y de la fluctuación, y la lógica 708 de cálculo. En una realización, se proporcionan paquetes que incluyen datos de análisis del tráfico de la red generados por la lógica 702 de transmisión, sin que medie solicitud (tal como los datos 690 de análisis del tráfico de la red descritos con referencia a la FIG. 6) a la interfaz 696 de salida en respuesta a la siguiente señal de paquete procedente de la interfaz 696 de salida.

En una realización, las máquinas 1204 de estado controladas por microcódigo pueden ser configurables de forma sensible a la información de control para variar una granularidad de tiempo en la cual se recogen los datos estadísticos no reducidos. Se puede proporcionar la información de control a las máquinas 1204 de estado controladas por microcódigo por medio del circuito 1202 de distribución de una forma similar a cómo se proporcionan segmentos de los paquetes 695 de entrada a las máquinas 1204 de estado controladas por microcódigo.

Las modificaciones de paquetes, según se han descrito anteriormente con referencia a la FIG. 8, también pueden facilitar la medición del tiempo de espera de la red, además, o independientemente, de facilitar la seguridad de la red y la gestión del tráfico. Por ejemplo, los paquetes 695 de entrada incluidos en uno o más flujos de datos (tales como los puertos lógicos 800) pueden ser modificados formando paquetes 697 de salida con un sello de tiempo insertado. El sello de tiempo puede indicar un tiempo de transmisión. El contenido del sello de tiempo puede determinarse en función de una señal de referencia de tiempo proporcionada por una fuente de tiempo acoplada con las máquinas 1204 de estado controladas por microcódigo. Se puede proporcionar el sello de tiempo como parte de la instrucción de modificación al circuito 1206 de agregación.

Con referencia a la FIG. 11, la lógica 1402 de condición puede estar configurada por microcódigo almacenado en el almacenamiento 1406 de control para evaluar una regla para medir el tiempo de espera de la red por paquete asociado con los paquetes 695 de entrada incluidos en uno o más flujos de datos (tales como los puertos lógicos 800).

Con referencia a la FIG. 8, cada motor 1204 de reglas puede interconectarse con un módulo asociado de direccionamiento. La FIG. 14 ilustra un diagrama de bloques lógicos de la interfaz entre motores 1204 de reglas y sus módulos asociados 2400 de direccionamiento, según una realización de la invención. Cada motor 1204 de reglas puede aplicar una regla para extraer uno o más campos de una unidad de entrada de datos de la red, tal como un paquete de entrada. La regla puede tener una granularidad bit a bit en la cabecera y la carga útil del paquete, de forma que los campos extraídos puedan tener una granularidad bit a bit y ser de cualquier porción del paquete. Cada motor 1204 de reglas proporciona los campos extraídos a un módulo 2400 de direccionamiento. En una realización, cada motor 1204 de reglas puede proporcionar un tiempo medido de espera de la red por paquete al módulo 2400 de direccionamiento. Cada módulo 2400 de direccionamiento procesa los datos para generar un identificador de direccionamiento que tiene una anchura deseablemente menor en bits que los campos extraídos proporcionados al módulo 2400 de direccionamiento, y proporciona el identificador de direccionamiento de nuevo al motor 1204 de reglas que proporcionó los campos extraídos. El identificador de direccionamiento puede estar asociado con un tipo de paquete o flujo de paquete o, de forma más general, con cualquier subconjunto de unidades de datos de la red que comparten una propiedad o atributo. Cada módulo 2400 de direccionamiento puede configurarse mediante la interfaz 1212 de gestión. En una realización, se pueden proporcionar los identificadores de direccionamiento a la interfaz 1212 de gestión.

De forma alternativa, cada motor 1204 de reglas puede generar el identificador de direccionamiento como parte de su procesamiento de unidades de entrada de datos de la red. En este caso, la función de los módulos 2400 de direccionamiento es realizada por los motores 1204 de reglas, haciendo que sean innecesarios módulos separados 2400 de direccionamiento.

En una realización, cada motor 1204 de reglas puede aplicar una regla para producir instrucciones de modificación en función de la información de categorización, tal como el identificador de direccionamiento. Las instrucciones de modificación pueden incluir el identificador de direccionamiento. El circuito 1206 de agregación puede combinar las instrucciones de modificación indicadas por los motores 1204 de reglas en una orden de modificación que se proporciona al circuito 696 de salida, según se ha descrito anteriormente. En función de la orden de modificación, el circuito 696 de salida puede añadir el identificador de direccionamiento a la unidad de datos de la red. El

identificador de direccionamiento puede añadirse a cualquier parte de la unidad de datos de la red, tal como la cabecera. En función de la decisión de encaminamiento del circuito 1206 de agregación, el circuito 696 de salida puede proporcionar la unidad modificada de datos de la red a un sistema de gestión mediante la interfaz 1212 de gestión. El circuito 696 de salida también puede transmitir la unidad modificada de datos de la red a dispositivos corriente abajo. Un beneficio de adjuntar información de categorización, tal como un identificador de direccionamiento, a una unidad de datos de la red pasada a otros dispositivos en la red es para que los dispositivos corriente abajo puedan aprovechar las capacidades de análisis y de procesamiento del tráfico de la red de un dispositivo corriente arriba. Los dispositivos corriente abajo pueden no tener las mismas capacidades de análisis y de procesamiento del tráfico que el dispositivo corriente arriba. Los dispositivos corriente abajo también pueden aprovechar la información de categorización asociada con una unidad recibida de datos de la red para simplificar y racionalizar el análisis y el procesamiento del tráfico de la red llevados a cabo en los dispositivos corriente abajo.

Las realizaciones de la invención son rentables, sencillas de utilizar, gestionables y flexibles. Con un algoritmo y un diseño de bloques unificados en el circuito 1202 de distribución, los motores 1204 de reglas y el circuito 1206 de agregación, el aparato lleva a cabo funciones de análisis de la cabecera, de inspección profunda de paquetes y de modificación de paquetes sin el uso de múltiples coprocesadores costosos, tales como NP, para un procesamiento de cabeceras y una modificación de paquetes y una CAM para la correspondencia de patrones. El aparato puede ser desplegado incrementalmente para equilibrar el riesgo con el presupuesto disponible. El aparato puede integrarse como parte de una capa física, una capa de enlace de datos u otra interfaz de capa inferior, y como parte de la misma, para permitir un procesamiento basado en reglas de capa superior en dispositivos rentables de baja potencia que no utilizan ninguno de los recursos de cálculo de los NP y de las CAM. La arquitectura del aparato está adaptada al análisis de cabeceras, a una inspección profunda de paquetes y a una modificación de paquetes a multi Gb/s y a mayores velocidades de entrada. El aparato proporciona una interfaz 1212 para la gestión y la monitorización de la red, la configuración de sus características especializadas y la salida de datos reflejados, y también puede soportar el uso de preprocesadores y de postprocesadores para necesidades específicas del cliente.

Las realizaciones de la invención también tienen un rendimiento predecible y fácilmente verificable, basado en su arquitectura. La implementación del conjunto de motores 1204 de reglas como un tejido de procesamiento en cadena de máquinas de estado de microcódigo que operan de forma simultánea y colaborativa garantiza que se pueden calcular y acotar el caudal de proceso y el tiempo de espera más desfavorable a través del aparato. Como resultado, se pueden realizar predicciones precisas acerca de cuándo se puede hacer funcionar el aparato a velocidad del hilo. La operación de la velocidad de hilo es suficientemente rápida para procesar, sin una pérdida involuntaria de tráfico, la combinación más desfavorable de tamaño de paquete de entrada y de velocidad de transferencia de paquetes en paquetes por segundo dada una regla de máxima complejidad. Además, dado que hay un número determinista más desfavorable de ciclos de reloj para el procesamiento de cualquier segmento de tráfico por medio de un motor 1204 de reglas, el aparato puede tener un pequeño retraso acotado de procesamiento entre mezclas de tipos de tráfico, de tamaños de paquetes y de complejidad de las reglas. Un pequeño retraso acotado significa que el aparato puede utilizar memorias intermedias en chip sencillas en vez de memoria externa o caches que pueden requerir una jerarquía de memoria o estructuras de encolamiento complejas. El uso de memorias intermedias en chip sencillas no solo aumenta el rendimiento del aparato mediante un uso eficaz y óptimo de los recursos de soporte físico, tales como puertas y elementos de memoria, sino que también evita casos diagonales relacionados con diversos patrones de tráfico. También permite la validación utilizando una verificación formal y una cobertura estructural, que reducen la probabilidad de escapes y errores de diseño.

Una persona con un nivel normal de dominio de la técnica comprenderá que las realizaciones descritas en la presente memoria pueden procesar diversas formas de tráfico de red incluyendo, sin limitación, paquetes. Por ejemplo, las realizaciones descritas en la presente memoria pueden procesar células o tramas.

Las realizaciones de la invención pueden permitir una monitorización de la red que puede ser suficientemente completa para identificar fenómenos de la red que pueden no ser identificables por anteriores sistemas de monitorización y de gestión de la red, tales como microrráfagas o nuevos tipos de ataques virales no reconocidos por los cortafuegos o el soporte lógico AV. Una monitorización eficaz requiere una recogida extensa de estadística de la red para permitir un análisis de comportamiento de la red. La recogida de estadística puede complementarse con una copia de instantáneas de toda la estadística recogida en un instante, o la agregación y correlación de información procedente de múltiples aparatos para proporcionar una visión clara del estado y del comportamiento de la red.

La anterior descripción, para los fines de la explicación, ha utilizado nomenclatura específica para proporcionar una comprensión minuciosa de la invención. Sin embargo, será evidente para un experto en la técnica que no se requieren detalles específicos para poner en práctica la invención. Por lo tanto, las anteriores descripciones de realizaciones específicas de la invención se presentan con fines ilustrativos y descriptivos. No se concibe que sean exhaustivas ni que limiten la invención a las formas precisas divulgadas; evidentemente, son posibles muchas modificaciones y variaciones en vista de las anteriores enseñanzas. Las realizaciones han sido escogidas y descritas para explicar de forma óptima los principios de la invención y sus aplicaciones prácticas, por lo tanto, permiten que otros expertos en la técnica utilicen de forma óptima la invención y diversas realizaciones con diversas

modificaciones también son aptas para el uso particular contemplado. Se concibe que las siguientes reivindicaciones y sus equivalentes definan el alcance de la invención.

REIVINDICACIONES

1. Un aparato, que comprende:

una pluralidad de máquinas (1204) de estado controladas por microcódigo, estando configurada al menos una de la pluralidad de máquinas (1204) de estado controladas por microcódigo para generar primeros datos estadísticos medidos en cada uno de una pluralidad de intervalos de tiempo de una primera granularidad de tiempo en función de los datos de la red incluidos en cada uno de una pluralidad de flujos (695) de datos que recorren la al menos una de la pluralidad de máquinas (1204) de estado controladas por microcódigo;

estando el aparato caracterizado por

lógica (700) de reducción de datos configurada para recibir los primeros datos estadísticos, y para obtener segundos datos estadísticos que tienen un volumen reducido con respecto a un volumen de los primeros datos estadísticos en función del desempeño de una operación matemática sobre los primeros datos estadísticos, estando asociados los segundos datos estadísticos con cada uno de la pluralidad de intervalos de tiempo de una segunda granularidad de tiempo, siendo más fina la primera granularidad de tiempo que la segunda granularidad de tiempo; y

lógica (702) de transmisión, sin que medie solicitud, configurada para enviar los segundos datos estadísticos a través de una red con independencia de una solicitud en tiempo real procedente de la red.

2. El aparato de la reivindicación 1, en el que la lógica (700) de reducción de datos es configurable para reducir el volumen de los primeros datos estadísticos para obtener los segundos datos estadísticos, de forma que se mantenga una indicación de una función de los primeros datos estadísticos en los segundos datos estadísticos, en el que la función quedaría enmascarada si los segundos datos estadísticos estuviesen basados en una agregación de los primeros datos estadísticos en cada uno de la pluralidad de intervalos de tiempo de la segunda granularidad de tiempo.

3. El aparato de la reivindicación 2, en el que:

la operación matemática incluye un máximo; y

los segundos datos estadísticos incluyen un resultado de la operación matemática aplicada a los primeros datos estadísticos en cada uno de la pluralidad de intervalos de tiempo de la segunda granularidad de tiempo, de forma que una indicación de variaciones incluidas en los primeros datos estadísticos que son sustancialmente mayores que un valor medio de los primeros datos estadísticos sean visibles tras la representación visual de los segundos datos estadísticos.

4. El aparato de la reivindicación 2, en el que:

la función en los primeros datos estadísticos incluye un pico y un valle, y está indicada por un subconjunto de los primeros datos estadísticos;

el pico se indica mediante una porción del subconjunto de los primeros datos estadísticos; y

el valle se indica mediante una porción restante del subconjunto de los primeros datos estadísticos.

5. El aparato de la reivindicación 1, en el que un volumen de los segundos datos estadísticos es reducido al menos diez veces con respecto a un volumen de los primeros datos estadísticos.

6. El aparato de la reivindicación 1, en el que la operación matemática incluye al menos uno de un mínimo, un máximo y una media.

7. El aparato de la reivindicación 1, en el que la operación matemática incluye al menos uno de una convolución, una media móvil, una suma de los cuadrados, una operación de filtrado lineal y una operación de filtrado no lineal.

8. El aparato de la reivindicación 1, en el que la lógica (702) de transmisión, sin que medie solicitud, es configurable para generar uno o más paquetes que incluyen los segundos datos estadísticos e información de direcciones asociada con un dispositivo ubicado en otro lugar en la red.

9. El aparato de la reivindicación 1, en el que la lógica (702) de transmisión, sin que medie solicitud, es configurable para anunciar la pluralidad de flujos (695) de datos a un dispositivo ubicado en otro lugar en la red.

10. El aparato de la reivindicación 1, en el que:

la pluralidad de flujos (695) de datos recorre un recorrido de los datos que se extiende a través de una porción del aparato; y

la lógica (702) de transmisión, sin que medie solicitud, es operable para enviar, sin que haya solicitud, los segundos datos estadísticos mediante comunicaciones que recorren al menos una porción del recorrido de los datos.

11. El aparato de la reivindicación 1, en el que la solicitud en tiempo real es un sondeo procedente de un dispositivo ubicado en otro lugar en la red.

12. El aparato de la reivindicación 1, que comprende, además, lógica (706) de análisis del tiempo de espera de la red y de la fluctuación configurada para recibir información del tiempo de espera de la red procedente de al menos una de la pluralidad de máquinas (1204) de estado controladas por microcódigo.

13. El aparato de cualquiera de las reivindicaciones 1-12, que comprende, además:

lógica (704) de generación de alertas configurada para generar una indicación de alerta asociada con el al menos uno de la pluralidad de flujos (695) de datos procesando los primeros datos estadísticos para determinar si los primeros datos estadísticos implican una característica asociada con la alerta;

estando configurada la lógica (702) de transmisión, sin que medie solicitud, además, para enviar la indicación de alerta a través de la red con independencia de una solicitud de la red.

14. El aparato de la reivindicación 13, en el que la característica se indica en función de la aparición de un patrón de bits en los datos de la red.

15. El aparato de la reivindicación 13, en el que la característica se indica en función de la aparición de un patrón de variación en una velocidad de transferencia de datos asociada con los datos de la red.

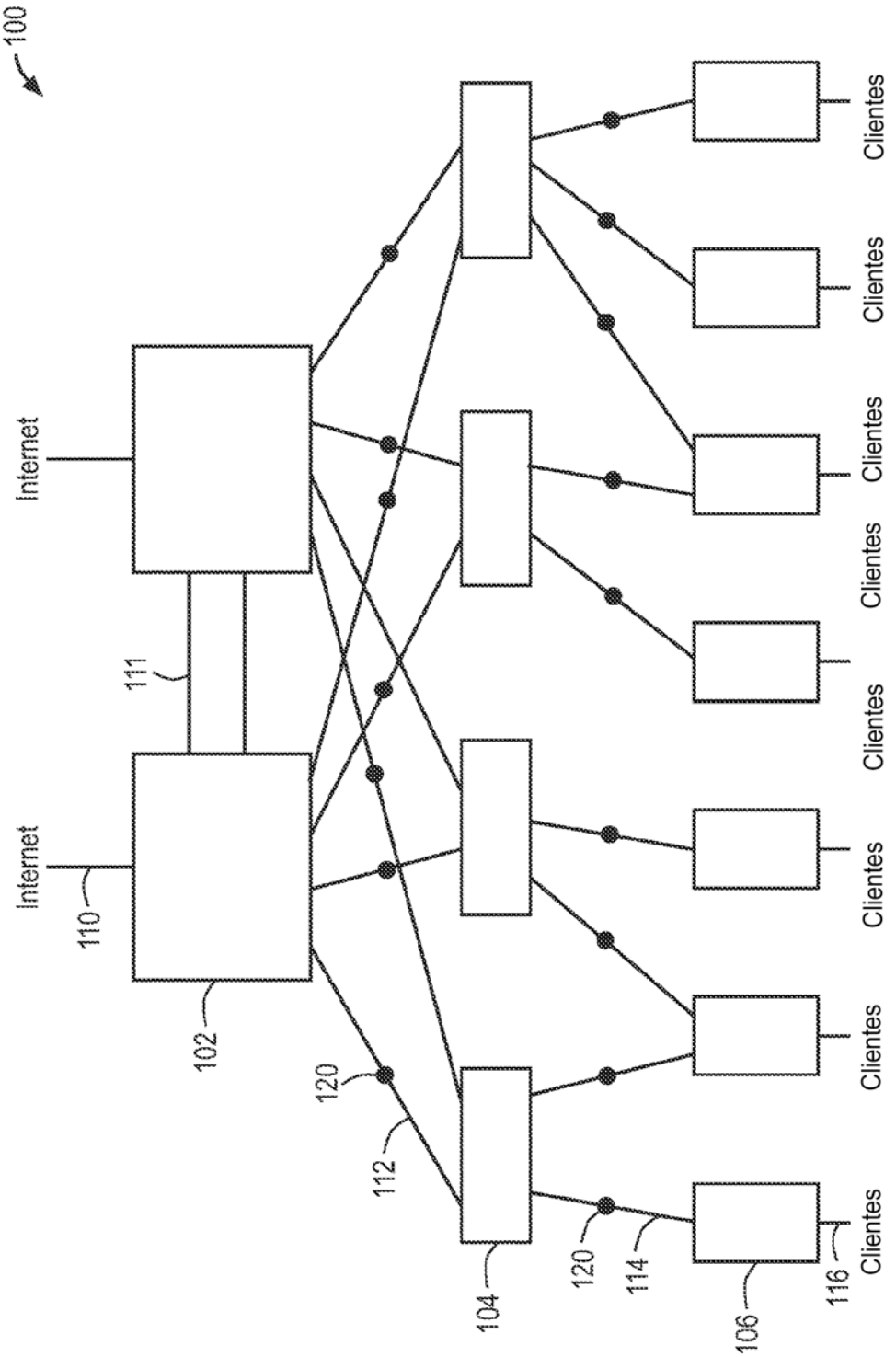
100
Internet
Internet
110
111
102
120
112
104
120
114
106
116
Clientes
Clientes
Clientes
Clientes
Clientes
Clientes
Clientes
Clientes
Clientes

FIG. 1

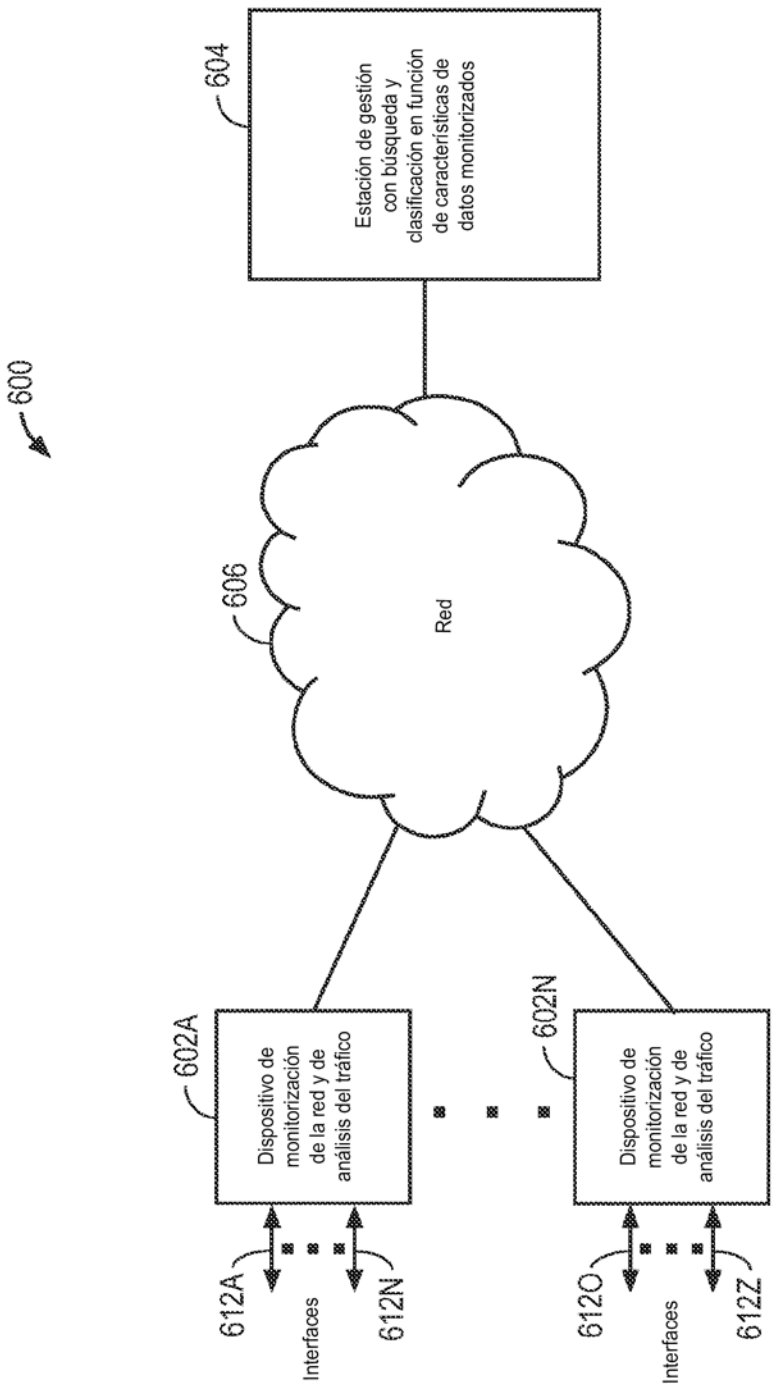
600
604
Estación de gestión con búsqueda y clasificación en función de características de datos monitorizados
606
Red
602A
Dispositivo de monitorización de la red y de análisis del tráfico
602N
Dispositivo de monitorización de la red y de análisis del tráfico
612A
612N
Interfaces
612O
612Z
Interfaces

FIG. 2

Término de búsqueda: Cadena = "AQUA"

Clasificación	Identificador del dispositivo de red	Identificador del puerto	Número de apariciones
1	A	2	18
2	B	7	16
3	C	5	12
4	A	6	11
⋮	⋮	⋮	⋮

FIG. 3A

Término de búsqueda | Condición = "Microrráfaga"

Clasificación	Identificador del dispositivo de red	Identificador del puerto	Número de apariciones
1	B	4	8
2	C	2	7
3	D	6	4
4	C	5	2
...			

FIG. 3B

Término de búsqueda: Condición = "Velocidad transf. datos > 1 Gbps"

Clasificación	Identificador del dispositivo de red	Identificador del puerto	Velocidad medida de transferencia de datos
1	A	4	4 Gbps
2	C	3	3,8 Gbps
3	D	2	3,4 Gbps
4	E	7	3,1 Gbps
...			

FIG. 3C

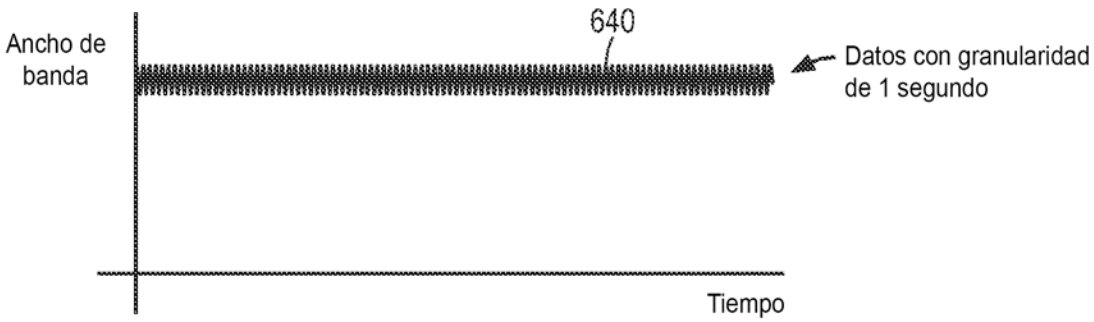

FIG. 4A

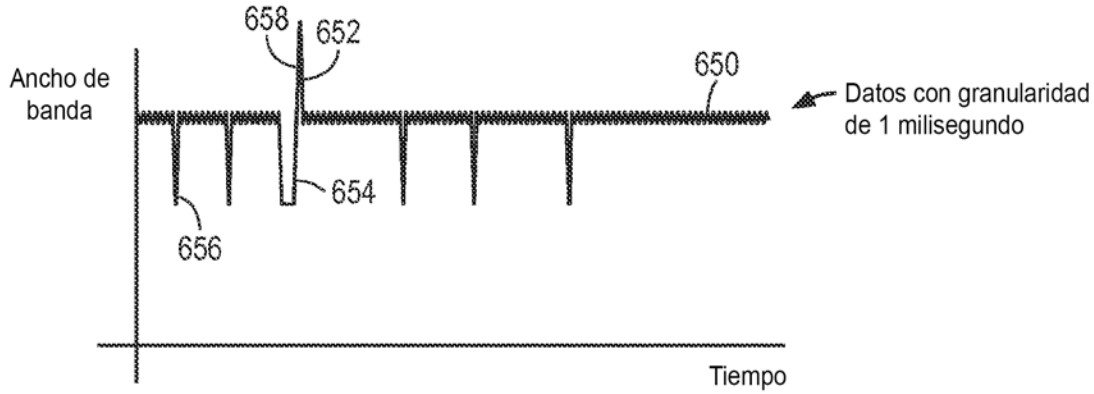

FIG. 4B

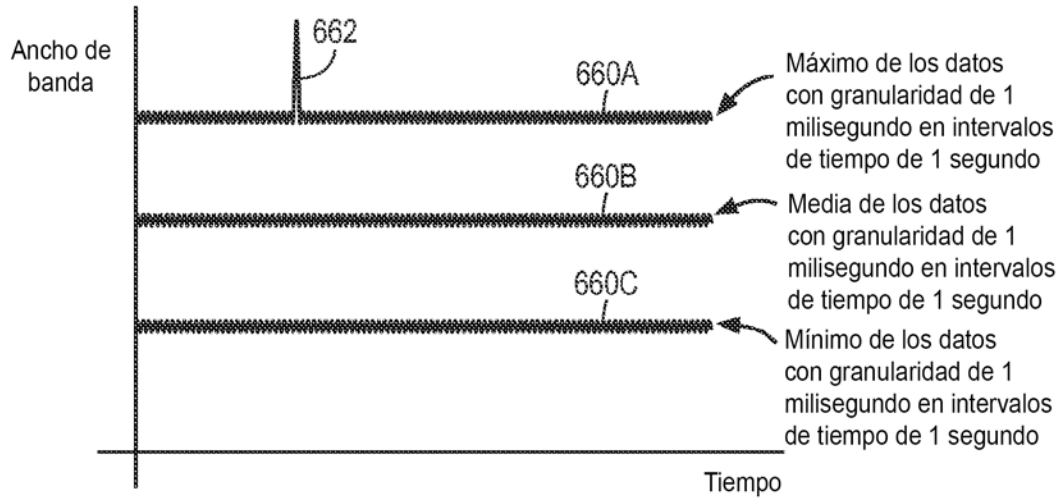

FIG. 4C

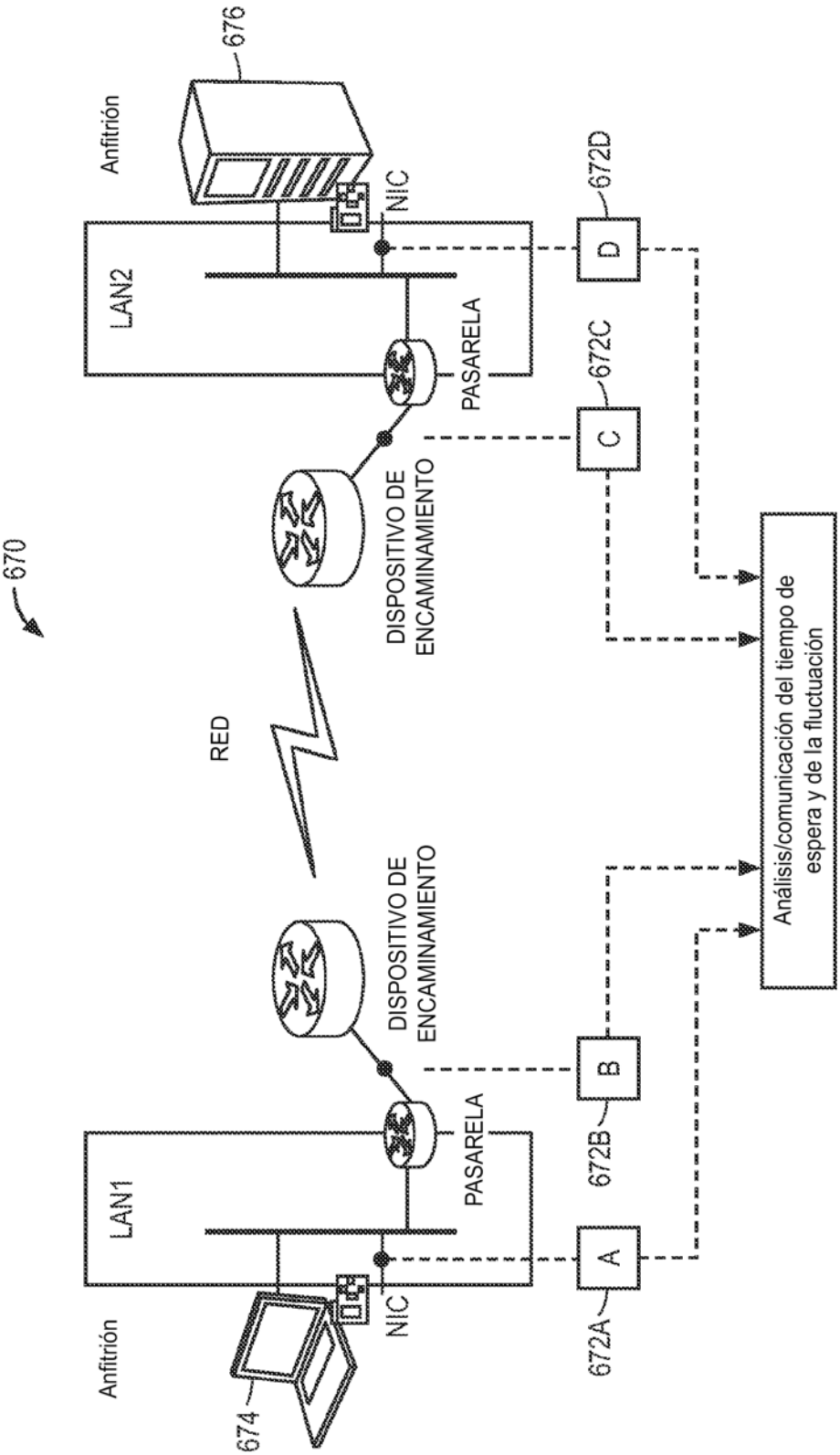
670
Anfitrión
676
NIC
LAN2
PASARELA
672D
D
672C
C
DISPOSITIVO DE ENCAMINAMIENTO
RED
DISPOSITIVO DE ENCAMINAMIENTO
B
672B
PASARELA
LAN1
A
672A
NIC
Anfitrión
674
Análisis/comunicación del tiempo de espera y de la fluctuación

FIG. 5

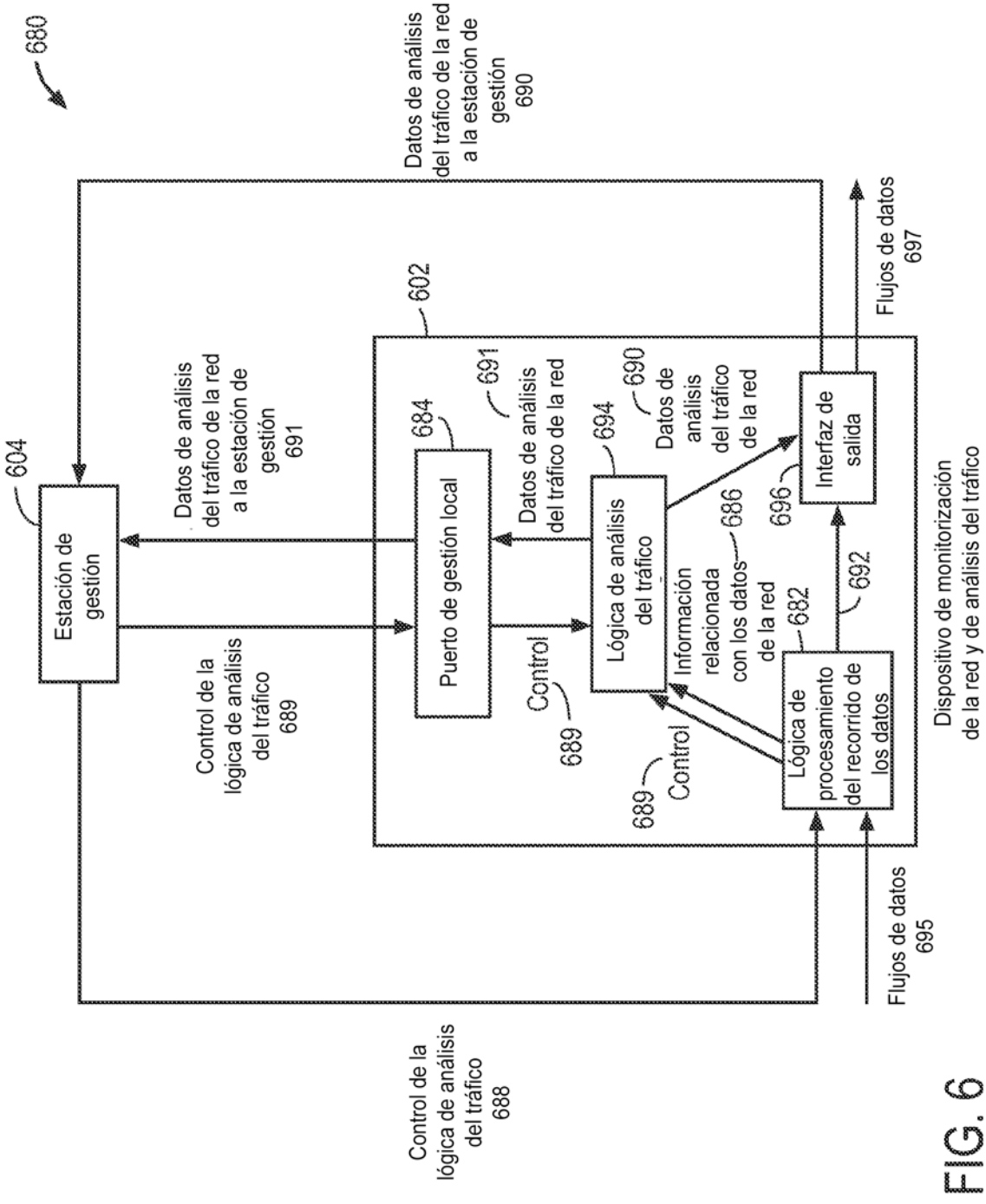
680
Datos de análisis del tráfico de la red a la estación de gestión 690
602
Flujos de datos 697
Datos de análisis del tráfico de la red a la estación de gestión 691
691
684
694
690
Datos de análisis del tráfico de la red
Datos de análisis del tráfico de la red
Datos de análisis del tráfico de la red
604
Estación de gestión
Puerto de gestión local
Lógica de análisis del tráfico
Interfaz de salida
696
686
Información relacionada con los datos de la red
692
682
Control de la lógica de análisis del tráfico 689
Control 689
Control 689
Lógica de procesamiento del recorrido de los datos
Dispositivo de monitorización de la red y de análisis del tráfico
Flujos de datos 695
Control de la lógica de análisis del tráfico 688

FIG. 6

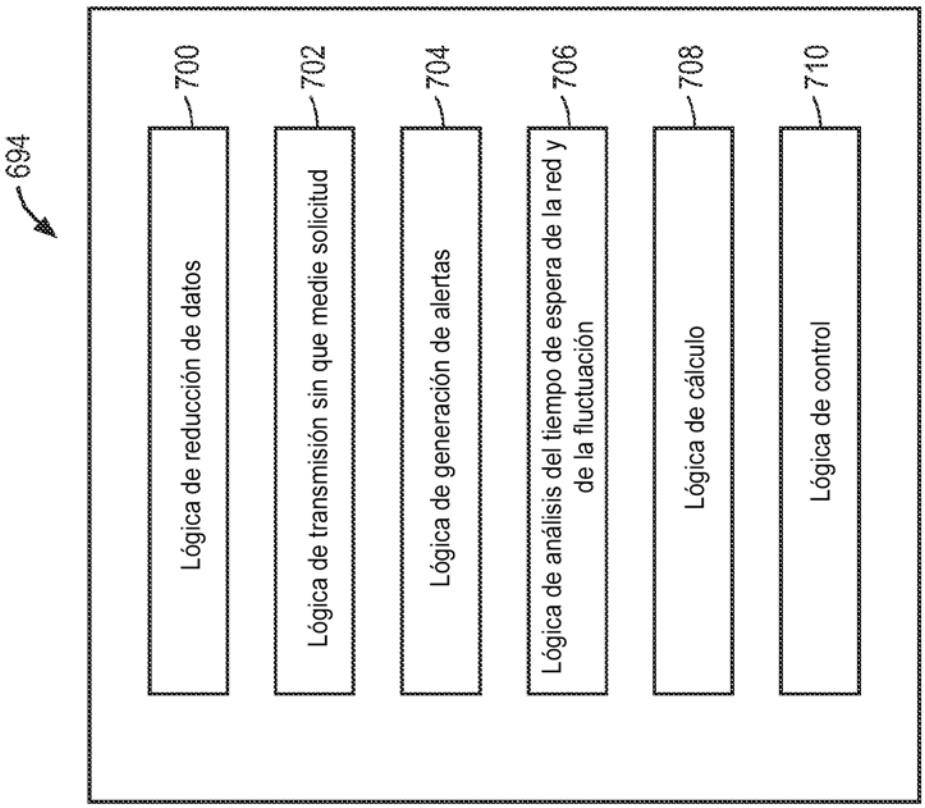
694
700
Lógica de reducción de datos
702
Lógica de transmisión sin que medie solicitud
704
Lógica de generación de alertas
706
Lógica de análisis del tiempo de espera de la red y de la fluctuación
708
Lógica de cálculo
710
Lógica de control

FIG. 7

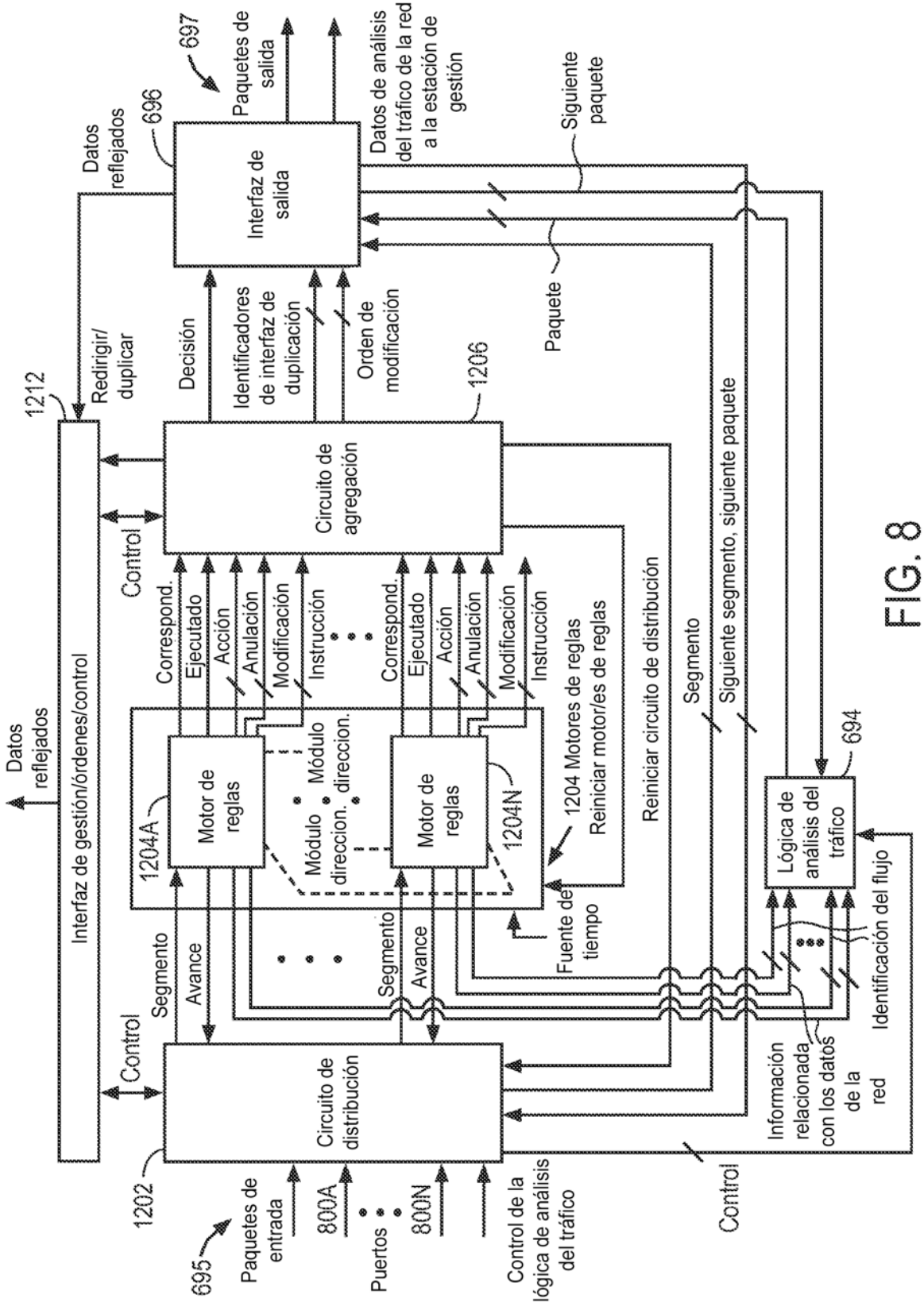
Datos reflejados
Interfaz de gestión/órdenes/control
1212
Redirigir/ duplicar
Datos reflejados
696
Interfaz de salida
697
Paquetes de salida
Datos de análisis del tráfico de la red a la estación de gestión
Siguiente paquete
Paquete
Decisión
Identificadores de interfaz de duplicación
Orden de modificación
1206
Circuito de agregación
Control
Correspond.
Ejecutado
Acción
Anulación
Modificación
Instrucción
1204A
Motor de reglas
Módulo direccion.
1204N
1204 Motores de reglas
Reiniciar motor/es de reglas
Reiniciar circuito de distribución
Segmento
Siguiente segmento, siguiente paquete
Fuente de tiempo
Segmento
Avance
Control
Circuito de distribución
1202
Lógica de análisis del tráfico
694
Información relacionada con los datos de la red
Identificación del flujo
Paquetes de entrada
695
800A
800N
Puertos
Control de la lógica de análisis del tráfico
Control

FIG. 8

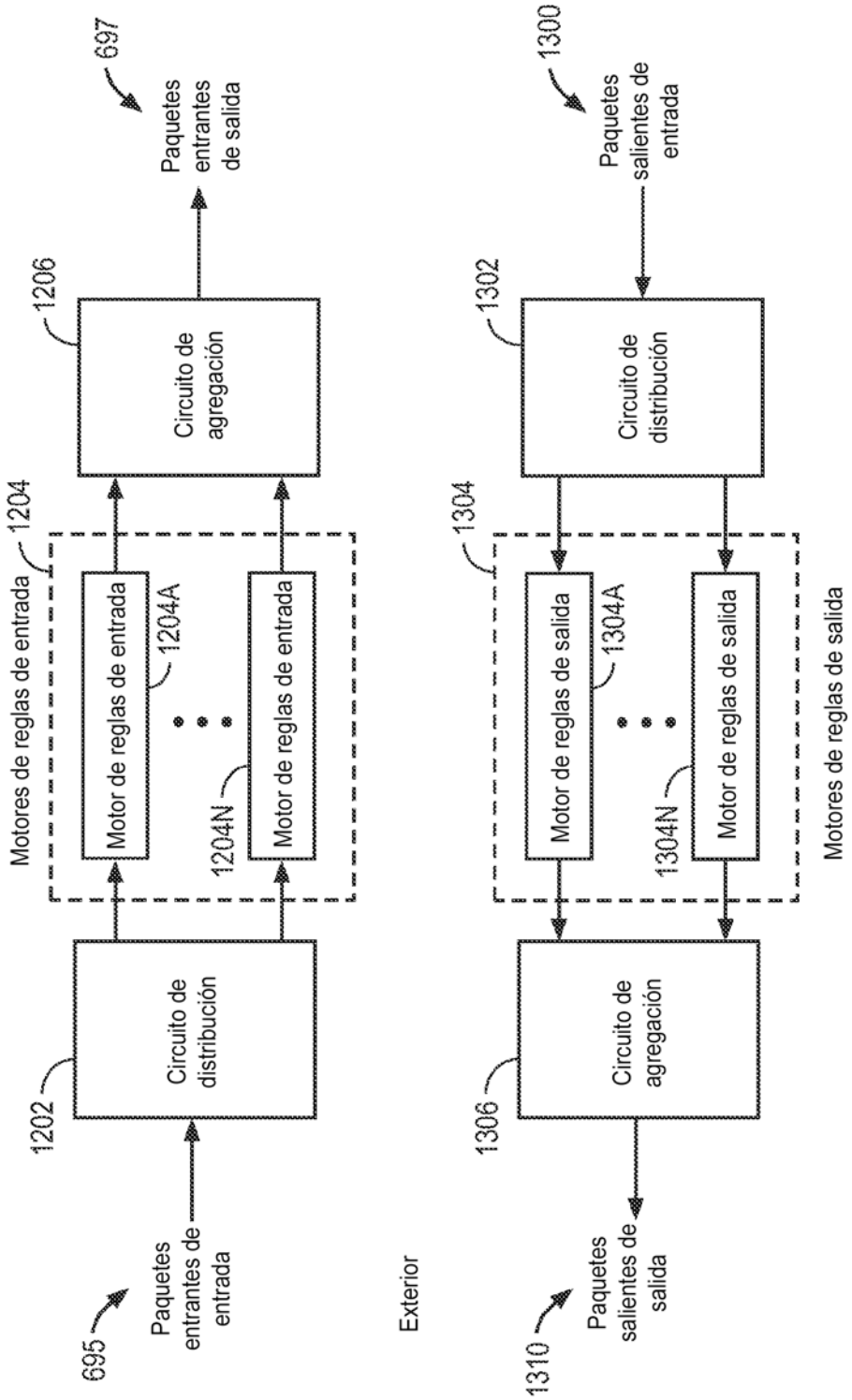
695
Paquetes entrantes de entrada
1202
Circuito de distribución
Motores de reglas de entrada
1204
Motor de reglas de entrada
1204A
1204N
Motor de reglas de entrada
1206
Circuito de agregación
697
Paquetes entrantes de salida
Exterior
1310
Paquetes salientes de salida
1306
Circuito de agregación
Motores de reglas de salida
1304
Motor de reglas de salida
1304A
1304N
Motor de reglas de salida
1302
Circuito de distribución
1300
Paquetes salientes de entrada

FIG. 9

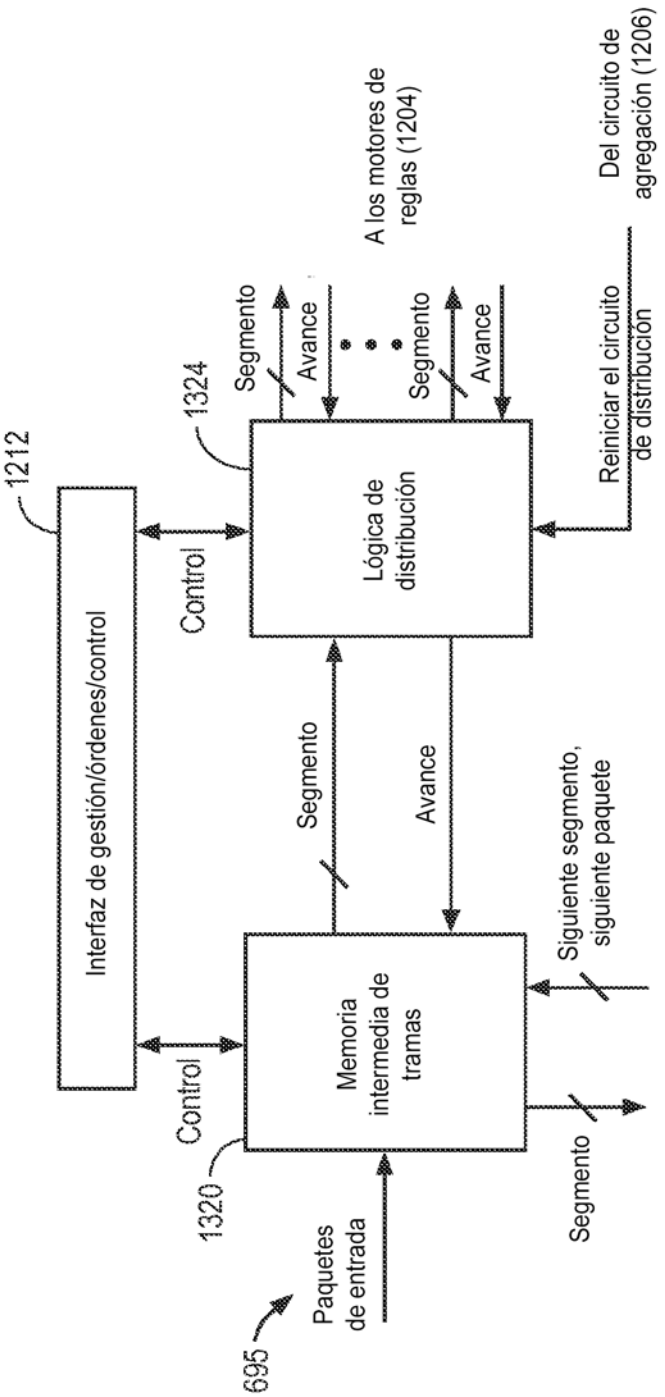
1212
Interfaz de gestión/órdenes/control
Control
1324
Lógica de distribución
Segmento
Avance
Segmento
Avance
A los motores de reglas (1204)
Del circuito de agregación (1206)
Reiniciar el circuito de distribución
Segmento
Avance
Siguiente segmento, siguiente paquete
Control
1320
Memoria intermedia de tramas
Segmento
A/desde la interfaz de salida
696
Paquetes de entrada
695

FIG. 10

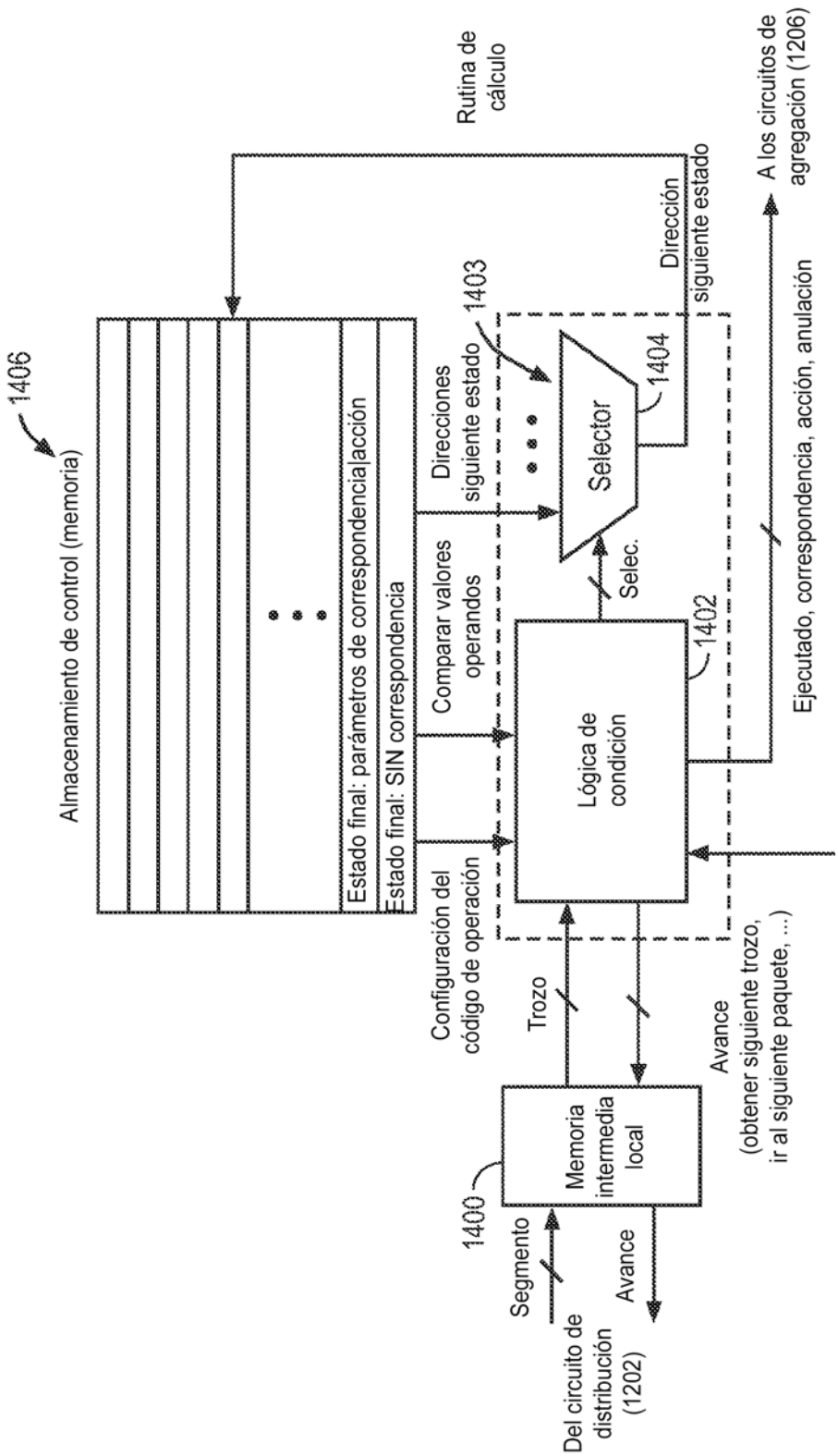
1406
Almacenamiento de control (memoria)
Estado final: parámetros de correspondencia/acción
Estado final: SIN correspondencia
Rutina de cálculo
Direcciones siguiente estado
1403
Selector
1404
Dirección siguiente estado
A los circuitos de agregación (1206)
Comparar valores operandos
Selec.
Lógica de condición
1402
Ejecutado, correspondencia, acción, anulación
Configuración del código de operación
Trozo
Avance (obtener siguiente trozo, ir al siguiente paquete, ...)
Reinicio o información de retorno de las reglas procedente del circuito de agregación (1206)
1400
Memoria intermedia local
Segmento
Avance
Del circuito de distribución (1202)

FIG. 11

Ejemplo de secuencia de ejecución del motor de reglas CWR

ID estado direcc.	Códigos de operación Operación y configuración	Operandos Valores con los que comparar	Siguiente dirección	Control
0	Inicialización y limpieza de estados internos (por ejemplo, establecer control global para anulación ECP, de forma que siguiente (es decir, siguiente dirección) sea 5 si SEGMENTO es un separador entre paquetes) *			
1	Comparar SEGMENTO en busca de igualdad	Con el valor: “ab”	Si es igual: siguiente = 2 de lo contrario: siguiente = 1	avanzar SEGMENTO
2	Comparar SEGMENTO en busca de igualdad	Con el valor: “cd”	Si es igual: siguiente = 3 de lo contrario: siguiente = 1	avanzar SEGMENTO mismo SEGMENTO
3	Comprobación de alcance para el SEGMENTO y comparar SEGMENTO en busca de igualdad	Acotación inferior alcan.:10 Acotación superior alcan. 14 Operando de igualdad: “ab”	caso dentro del alcance: sig. = 4 caso no dentro del alc. e igual: sig. = 2 de lo contrario: sig. = 1	avanzar SEGMENTO avanzar SEGMENTO mismo SEGMENTO
4	Estado final correspondencia		Siguiente = 0	Ejecutado, correspond.
5	Estado final SIN correspondencia		Siguiente = 0	Ejecutado, SIN corresp.

* cuando el SEGMENTO es igual a un separador entre paquetes (”--”) provoca que la siguiente dirección sea estado final SIN correspondencia

FIG. 12

ES 2 652 292 T3

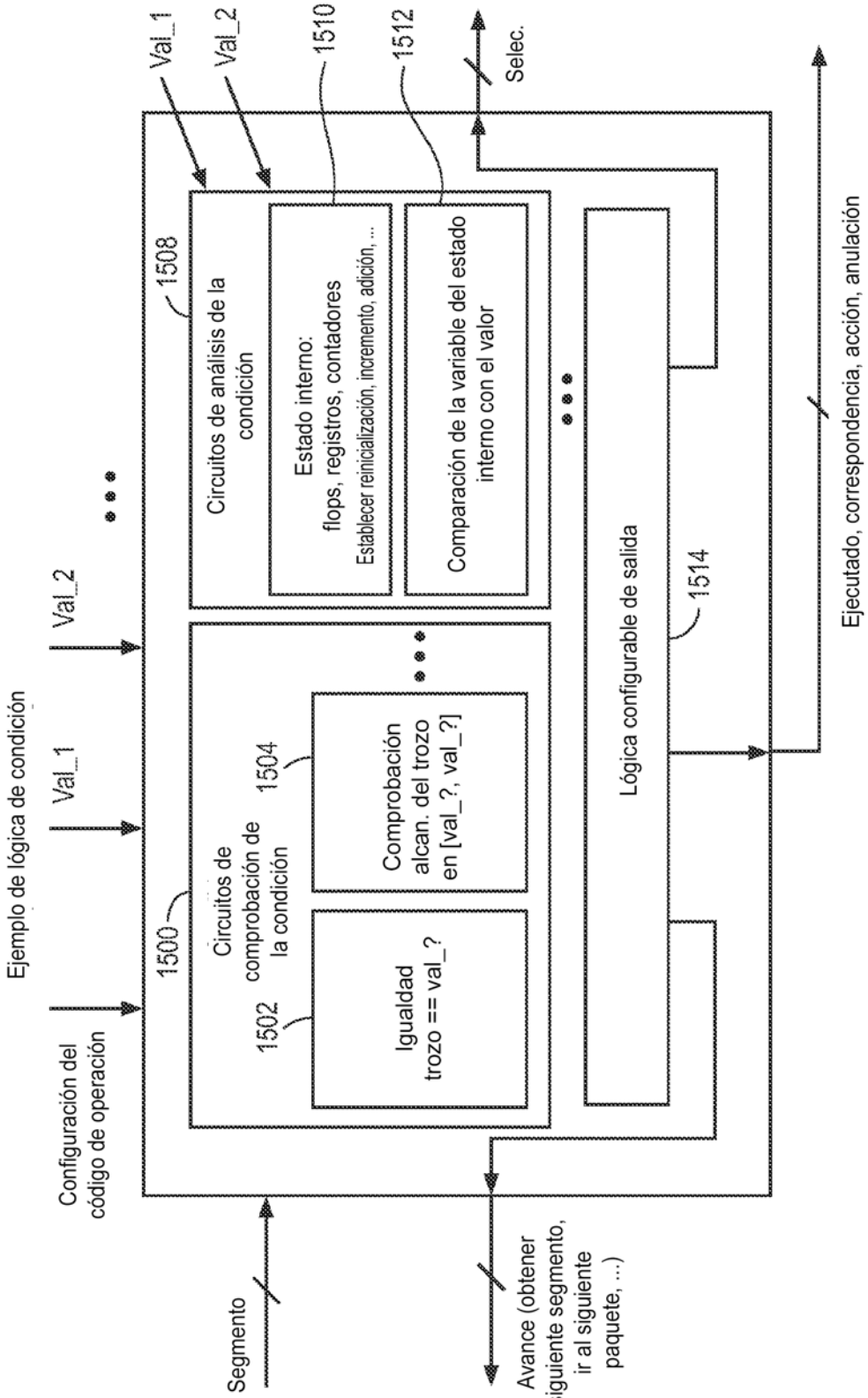
Ejemplo de lógica de condición
Configuración del código de operación
Val_1
Val_2
1500
Circuitos de comprobación de la condición
1502
Igualdad trozo == val_?
1504
Comprobación alcan. del trozo en [val_?, val_?]
1508
Circuitos de análisis de la condición
Estado interno: flops, registros, contadores
Establecer reinicialización, incremento, adición, ...
1510
Comparación de la variable del estado interno con el valor
1512
Selec.
Lógica configurable de salida
1514
Ejecutado, correspondencia, acción, anulación
Segmento
Avance (obtener siguiente segmento, ir al siguiente paquete, ...)

FIG. 13

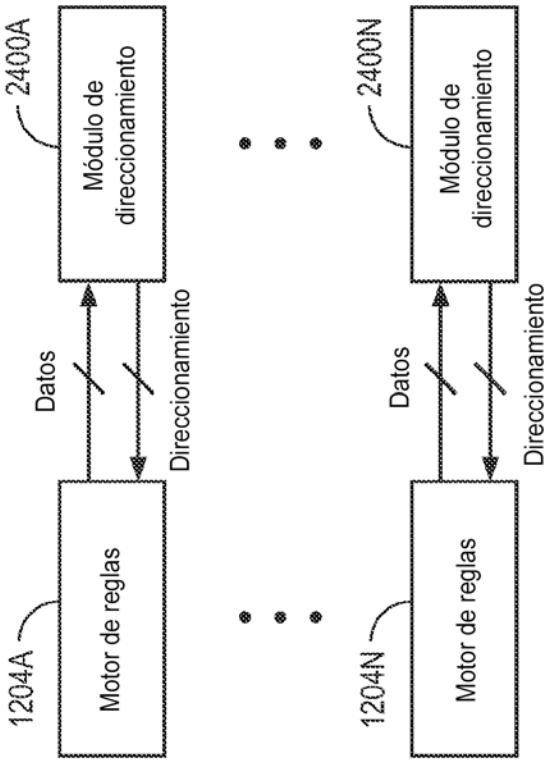
2400A
Módulo de direccionamiento
Datos
Direccionamiento
1204A
Motor de reglas
2400N
Módulo de direccionamiento
Datos
Direccionamiento
1204N
Motor de reglas

FIG. 14