(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 963 965**

(51) Int. Cl.:

H04L 61/4511 (2012.01)
H04L 47/2475 (2012.01)
H04L 45/7453 (2012.01)
H04L 47/2441 (2012.01)
H04L 47/80 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.04.2018 PCT/US2018/030014**

(87) Fecha y número de publicación internacional: **01.11.2018 WO18201084**

(96) Fecha de presentación y número de la solicitud europea: **27.04.2018 E 18790188 (9)**

(97) Fecha y número de publicación de la concesión europea: **16.08.2023 EP 3616075**

(54) Título: **Sistema y procedimiento de seguimiento de nombres de dominio para la gestión de redes**

(30) Prioridad:

28.04.2017 US 201762491581 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.04.2024

(73) Titular/es:

OPANGA NETWORKS, INC. (100.0%)
1201 third Avenue, Suite 2200
Seattle, WA 98101, US

(72) Inventor/es:

BROWN, SEAN;
BURNETTE, JOHN;
HADORN, BEN;
GARZA, HUGO y
NORDNESS, ETHAN

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Sistema y procedimiento de seguimiento de nombres de dominio para la gestión de redes

REFERENCIA CRUZADA A LA SOLICITUD CORRESPONDIENTE

El presente documento de patente reivindica el beneficio de la Solicitud de Patente Provisional de EE. UU. No. 62/491.581, presentada el 28 de abril de 2017.

ANTECEDENTES

Los datos pueden atravesar una red en forma de tráfico de red. El tráfico de red puede incluir uno o más paquetes encapsulados que se transmiten a través de una red entre dos puntos finales. Por ejemplo, un paquete de datos atraviesa una red de datos desde un servidor de contenidos hasta un equipo de usuario.

La identificación del tráfico de red es importante para diversas aplicaciones de gestión y análisis de redes. Históricamente, el tráfico de red ha sido utilizado por los proveedores de servicios de red para comprender los patrones de tráfico y el comportamiento de los consumidores en sus redes.

El tráfico de red puede identificarse mediante una cadena de identificación que define un ámbito de autonomía administrativa, autoridad y/o control dentro de Internet. Por ejemplo, el tráfico de red puede identificarse mediante nombres de host que identifican los puntos finales del tráfico de red.

La información de identificación de red, tal como los nombres de host, puede obtenerse realizando una inspección profunda de paquetes de datos de capa de aplicación de paquetes de datos en flujos de datos individuales. Sin embargo, la identificación del tráfico de red por medios tradicionales se ha vuelto difícil, lenta y problemática con la adopción del cifrado mediante Transport Layer Security (TLS) o Secure Sockets Layer (SSL). Las cargas útiles de los paquetes de datos están ahora cifradas. Como resultado, las implementaciones anteriores que se han basado en técnicas de inspección profunda de paquetes (por ejemplo, la lectura en los datos de la capa de aplicación) ya no son viables debido al cifrado, que ahora oculta la mayor parte de esos datos.

La inspección profunda de paquetes tiene otros inconvenientes. Por ejemplo, la inspección profunda de paquetes también ha sido históricamente una operación computacional costosa con efectos secundarios negativos para las redes.

En consecuencia, una nueva estrategia para identificar el tráfico de red que transporta paquetes de datos cifrados, y que no requiere procedimientos de inspección profunda de paquetes costosos desde el punto de vista computacional, sería ventajosa para realizar técnicas de análisis y gestión de redes. Una solución del estado de la técnica se divulga en el documento US2016/0323186.

BREVE SUMARIO

La invención se define por el objeto de las reivindicaciones independientes. Otras realizaciones están definidas por el objeto de las reivindicaciones dependientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Fig. 1 ilustra una arquitectura de sistema de acuerdo con la invención.
La Fig. 2 ilustra una arquitectura de sistema de acuerdo con la invención.
La Fig. 3A ilustra un dispositivo cliente de acuerdo con la invención.
La Fig. 3B ilustra un sistema de nombres de dominio (DNS) espía de acuerdo con la invención.
La Fig. 3C ilustra un servidor DNS de acuerdo con la invención.
La Fig. 3D ilustra un gestor de transporte de acuerdo con la invención.
La Fig. 3E ilustra un servidor de contenidos de acuerdo con la invención.
La Fig. 4 ilustra un paquete de datos de acuerdo con la invención.
La Fig. 5 ilustra una respuesta DNS de acuerdo con la invención.
La Fig. 6 ilustra una tabla de identificación de acuerdo con la invención.
La Fig. 7 ilustra un procedimiento de extracción de un nombre de host y una dirección de protocolo de Internet (IP) a partir de una respuesta DNS de acuerdo con la invención.
La Fig. 8 ilustra un procedimiento para añadir una nueva entrada a una tabla de identificación de acuerdo con la invención.
La Fig. 9 ilustra un procedimiento para determinar la longitud de un paquete no DNS de acuerdo con la invención.
La Fig. 10 ilustra un procedimiento para determinar una marca de tiempo de un paquete no DNS de acuerdo con la invención.

La Fig. 11 ilustra un procedimiento de actualización de una entrada de una tabla de identificación de acuerdo con la invención.
La Fig. 12 ilustra un procedimiento de gestión de un flujo de datos utilizando una tabla de identificación de acuerdo con la invención.
La Fig. 13 ilustra un procedimiento de identificación y marcaje de un flujo de elefantes utilizando una tabla de identificación de acuerdo con la invención.
La Fig. 14 ilustra un procedimiento para controlar el tamaño de una tabla de identificación de acuerdo con la invención.
La Fig. 15 ilustra un procedimiento de generación, utilización y actualización de una tabla de identificación de acuerdo con la invención.

DESCRIPCIÓN DETALLADA

La invención se refiere a un sistema y procedimiento para identificar respuestas de servicio de nombres de dominio (DNS) transmitidas desde un servidor, analizar las respuestas DNS para crear un mapeo entre la(s) dirección(es) de protocolo de Internet (IP) de un servidor de red de distribución de contenidos (CDN) y el nombre de dominio basado en las respuestas DNS, identificando además un flujo de datos específico desde un cliente a un servidor por este nombre de dominio, aplicar una política de gestión del tráfico o de recopilación de estadísticas basada en la correspondencia entre el nombre de dominio y la dirección IP del servidor, limpiar/expirar las entradas del mapa en función de la importancia de los datos transferidos y de la actividad, recopilar/almacenar datos estadísticos sobre los flujos de datos mencionados anteriormente en su conjunto o determinados por el nombre de dominio, y determinar los nombres de dominio más significativos en una red determinada mediante el análisis de la totalidad de los datos estadísticos recopilados.

De acuerdo con una realización, un dispositivo, un sistema, un procedimiento, o una combinación de los mismos, puede utilizarse para capturar y crear un mapeo, o caché, del nombre de host y las correspondientes direcciones IP de servidor de una variedad de flujos de datos, incluso cuando los datos de paquetes a nivel de aplicación en los flujos de datos están encriptados.

Como se usa en el presente documento, el término "nombre de host" se refiere al nombre de un host específico, proveedor de contenido, contenido, o una combinación de los mismos. Un nombre de host es, por ejemplo, un apodo, un nombre de nodo, un nombre de dominio, una dirección web o una combinación de los mismos.

En la invención, se genera una tabla de búsqueda DNS inversa. Un dispositivo accede a la tabla y utiliza las entradas de la misma para identificar uno o ambos extremos de los flujos de datos que atraviesan una red. El dispositivo implementa políticas de gestión de red basadas en los puntos finales identificados. Por ejemplo, un gestor de transporte accede a la tabla, la utiliza para identificar que un punto final de un flujo de datos específico se ha asociado históricamente con flujos de datos relativamente gravosos, y establece el ritmo del flujo de datos.

La Fig. 1 ilustra una arquitectura del sistema 100 de acuerdo con una realización de la presente divulgación.

El sistema 100 incluye un dispositivo 110 de cliente, una primera red 120, un DNS espía 130, una segunda red 140, y un servidor 150 DNS.

El dispositivo 110 de cliente está configurado para recibir una o más entradas de uno o más usuarios, y para comunicarse con el servidor DNS a través de las redes 120 y 140 primera y segunda. El dispositivo 110 de cliente es, por ejemplo, un ordenador de sobremesa, un ordenador portátil, una tableta, un teléfono inteligente, un lector electrónico, un reloj inteligente, una televisión inteligente o una combinación de los mismos.

La primera red 120 es una red cableada o inalámbrica que conecta el dispositivo 110 de cliente y el DNS espía 130 entre sí. De acuerdo con diversas realizaciones, la primera red 120 puede ser cualquier red que permita la comunicación entre máquinas, bases de datos y dispositivos. En consecuencia, la primera red 120 puede ser una red de acceso amplio (WAN), una red cableada, una red de fibra, una red inalámbrica (por ejemplo, una red móvil o celular), una red celular o de telecomunicaciones (por ejemplo, WiFi, Sistema Global de Comunicaciones Móviles (GSM), Sistema Universal de Telecomunicaciones Móviles (UMTS), red Long Term Evolution (LTE)), o cualquier combinación adecuada de las mismas. La red 130 puede incluir una o más porciones de una red privada, una red pública (por ejemplo, Internet), o cualquier combinación adecuada de las mismas. En una realización específica, la primera red 120 incluye una colección central de subnodos que enlazan con una red de acceso de radio (RAN).

El DNS espía 130 está conectado entre el dispositivo 110 de cliente y el servidor 150 DNS a través de la primera red 120 y la segunda red 140. En diversas realizaciones, el DNS espía 130 está configurado para interceptar respuestas DNS enviadas desde el servidor 150 DNS al dispositivo 110 de cliente, y para generar y/o actualizar una tabla de identificación basada en pares nombre de host/dirección IP en las respuestas DNS. El DNS espía 130 también puede interceptar otros tipos de paquetes que atraviesan la primera red 120, la segunda red 140, o ambas, (por ejemplo, paquetes de datos no DNS) y actualizar la tabla de identificación basándose en las características de los paquetes

interceptados. Por ejemplo, el DNS espía 130 puede actualizar una entrada existente que incluya un par nombre de host/dirección IP con un tamaño, una marca de tiempo, o ambos, derivados de un paquete no DNS interceptado.

La segunda red 140 es una red cableada o inalámbrica que conecta el DNS espía 130 y el servidor 150 DNS entre sí. En una realización específica, la segunda red 140 es Internet.

El servidor 150 DNS es un dispositivo servidor configurado para generar respuestas DNS en respuesta a solicitudes DNS de diversos dispositivos cliente, incluyendo el dispositivo 110 de cliente. Al recibir una solicitud DNS que especifica un nombre de host específico, el servidor 150 DNS busca una dirección IP asociada con el nombre de host específico. A continuación, el servidor 150 DNS transmite la dirección IP al dispositivo solicitante, para que éste pueda acceder a un servidor de contenidos asociado al nombre de host.

En la invención, el dispositivo 110 de cliente transmite una petición DNS al servidor 150 DNS a través de una o más redes, tales como las redes 120 y 140 primera y segunda. La respuesta DNS incluye un nombre de host, por ejemplo, el nombre de un sitio web de alojamiento de vídeos, tal como "YOUTUBE" o "YOUTUBE.COM"

Cuando el servidor 150 DNS recibe la petición DNS, el servidor 150 DNS extrae el nombre de host de la solicitud DNS, y busca una dirección IP asociada al nombre de host. El servidor 150 DNS genera una respuesta DNS que incluye el nombre de host y la dirección IP asociada al nombre de host. El servidor 150 DNS transmite la respuesta DNS de vuelta al dispositivo 110 de cliente a través de las redes 120 y 140 primera y segunda.

El DNS espía 130 intercepta la respuesta DNS. Como la respuesta DNS no está cifrada, el DNS espía 130 extrae el nombre de host y la dirección IP de la respuesta DNS sin realizar el descifrado. A continuación, el DNS espía 130 almacena el par nombre de host/dirección IP en una entrada de una tabla de identificación. El DNS espía 130 asigna múltiples pares nombre de host/dirección IP a entradas de la tabla de identificación interceptando e inspeccionando múltiples respuestas DNS.

De acuerdo con una realización, el DNS espía 130 controla un tamaño de la tabla de identificación eliminando la tabla de identificación cuando se produce un evento desencadenante. Por ejemplo, el DNS espía 130 borra una o más entradas de la tabla de identificación cuando ésta alcanza un tamaño predeterminado.

En diversas realizaciones, el servidor 150 DNS es incapaz de devolver un nombre de host basado en una dirección IP dada. Sin embargo, un dispositivo que acceda a la tabla de identificación (por ejemplo, un gestor de transporte) puede determinar un nombre de host asociado a una dirección IP específica identificando una entrada que incluya la dirección IP específica. La tabla de identificación generada por el DNS espía 130 puede, por tanto, utilizarse para realizar una operación de búsqueda DNS inversa, de acuerdo con diversas realizaciones.

La Fig. 2 ilustra una arquitectura del sistema 200 de acuerdo con una realización de la presente divulgación.

El sistema 200 incluye un dispositivo 210 de cliente, una primera red 220, un DNS espía 230, una segunda red 240, un servidor 250 DNS, una tercera red 260, un gestor 270 de transporte, una cuarta red 280 y un servidor 290 de contenidos. Aunque la Fig. 2 sólo ilustra uno de cada uno de los dispositivos 210 de cliente, la primera red 220, el DNS espía 230, la segunda red 240, el servidor 250 DNS, la tercera red 260, el gestor 270 de transporte, la cuarta red 280, y el servidor 290 de contenidos, el sistema 200 puede incluir una pluralidad de cada uno de, el dispositivo 210 de cliente, la primera red 220, el DNS espía 230, la segunda red 240, el servidor 250 DNS, la tercera red 260, el gestor 270 de transporte, la cuarta red 280, y el servidor 290 de contenidos de acuerdo con diversas realizaciones. Por ejemplo, múltiples dispositivos 210 de cliente pueden estar conectados a la primera red 220, a la tercera red 260, o a ambas, múltiples servidores 250 DNS pueden estar conectados a la segunda red 240, y múltiples servidores 290 de contenido pueden estar conectados a la cuarta red 280.

En diversas realizaciones, el dispositivo 210 de cliente, la primera red 220, el DNS espía 230, la segunda red 240, y el servidor 250 DNS son equivalentes al dispositivo 110 de cliente, la primera red 120, el DNS espía 130, la segunda red 140, y el servidor 150 DNS descritos anteriormente con respecto a la Fig. 1. En ciertas realizaciones, la primera red 220 es la misma que la tercera red 260, y la segunda red 240 es la misma que la cuarta red 280. En consecuencia, el DNS espía 230, el gestor 270 de transporte, o ambos, se encuentran entre el dispositivo 210 de cliente y el servidor 250 DNS, el dispositivo 210 de cliente y el servidor 290 de contenidos, o ambos.

Cuando el dispositivo 210 de cliente recibe una respuesta DNS que incluye una dirección IP solicitada desde el servidor 250 DNS, el dispositivo 210 de cliente genera una solicitud de contenido que incluye la dirección IP. El dispositivo 210 de cliente transmite la solicitud de contenidos al servidor 290 de contenidos a través de las redes 260 y 280 tercera y cuarta.

Los equipos asociados a las redes 260 y 280 tercera y cuarta enrutan la solicitud de contenido al servidor 290 de contenido utilizando la dirección IP. En una realización específica, la tercera red 260 es la primera red 220, y la cuarta red 280 es la segunda red 240.

Cuando el servidor 290 de contenidos recibe la solicitud de contenido, el servidor 290 de contenidos transmite el contenido solicitado al dispositivo 210 de cliente.

En diversas realizaciones, la solicitud de contenido del dispositivo 210 de cliente, el contenido del servidor 290 de contenido, o ambos, se transmiten en forma de uno o más paquetes de datos. Los paquetes de datos son paquetes de datos no DNS, por ejemplo.

El gestor 270 de transporte está configurado para interceptar la solicitud de contenido transmitida desde el dispositivo 210 de cliente al servidor 290 de contenido, el uno o más paquetes de datos transmitidos desde el servidor 290 de contenido al dispositivo 210 de cliente, o ambos. De acuerdo con diversas realizaciones, el gestor 270 de transporte intercepta los paquetes de datos transportados a través de la tercera red 260 entre uno o más dispositivos cliente y uno o más servidores de contenidos.

El gestor 270 de transporte está situado entre el dispositivo 210 de cliente y el servidor 290 de contenidos. En una realización, el gestor 270 de transporte se encuentra en un punto de agregación de tráfico fronterizo que conecta la tercera red 260 con la cuarta red 280. En un ejemplo en el que la tercera red 260 es una red móvil estándar del Proyecto de Asociación de Tercera Generación (3GPP), el punto de agregación forma parte de las Gi-LAN que se conecta al elemento central de la Pasarela de la Red de Paquetes de Datos (PDN) y hacia fuera a Internet. En un ejemplo en el que la tercera red 260 es una red 4G, el punto de agregación forma parte de una Gi-LAN que se conecta a un nodo de soporte GPRS de pasarela (GGSN)-Pasarela y hacia fuera a Internet. Sin embargo, en otras realizaciones, el gestor 270 de transporte está situado en otro lugar.

El gestor 270 de transporte gestiona el tráfico de datos transmitido a través de la tercera red 260. En ciertas realizaciones, el gestor 270 de transporte está configurado para optimizar los recursos de red, aliviar la congestión, realizar otras operaciones de gestión de datos, o una combinación de las mismas, en la tercera red 260 mediante la gestión del tráfico de datos a través de la tercera red 260. Por ejemplo, el gestor 270 de transporte establece el ritmo de un flujo de datos entre el dispositivo 210 de cliente y el servidor 290 de contenidos basándose en una o más políticas almacenadas en el gestor 270 de transporte. El gestor 270 de transporte hace pasar el flujo de datos después de identificar que el flujo de datos es relativamente gravoso para la tercera red 260, determinar que la tercera red 260 está actualmente congestionada, determinar que el flujo de datos es relativamente poco importante en comparación con otros flujos de datos que atraviesan la tercera red 260, o una combinación de los mismos.

El gestor 270 de transporte controla el flujo de datos estrangulando el flujo de datos, almacenando temporalmente paquetes de datos en el flujo de datos, requiriendo que el flujo de datos atraviese una red distinta de la tercera red 260, o una combinación de las mismas. Por ejemplo, el gestor 270 de transporte puede acelerar el flujo de datos requiriendo que los paquetes de datos dentro del flujo de datos atraviesen una red WIFI local, en lugar de la tercera red 260, cuando la red WIFI conecta el dispositivo 210 de cliente al servidor 290 de contenidos.

Pueden encontrarse más detalles sobre el ritmo de flujos de datos en la solicitud comúnmente asignada Solicitud de EE. UU. No. 15/060,486, titulada "SYSTEMS AND METHODS FOR PACING DATA FLOWS", que se presentó el 3 de marzo de 2016, y por la presente se incorpora por referencia en su totalidad.

En diversas realizaciones, el gestor 270 de transporte marca selectivamente el ritmo de los flujos de elefantes que atraviesan la tercera red 260. Un flujo elefante es un flujo de datos relativamente gravoso para la tercera red 260. Por ejemplo, un flujo elefante es un flujo de datos que incluye una cantidad de datos transferidos superior a un umbral, un flujo de datos con una duración superior a una duración umbral, un flujo de datos que incluye paquetes de datos con un tipo de archivo concreto, o una combinación de los mismos.

En algunas realizaciones, un flujo de datos puede identificarse como un flujo elefante mediante la identificación de un nombre de host asociado con el flujo de datos. En una realización, cuando se identifica que un flujo de datos se dirige a o procede de un host del que se sabe previamente que es probable que genere flujos elefante, el gestor 270 de transporte identifica el flujo de datos como un flujo elefante. Por ejemplo, cuando el gestor 270 de transporte identifica que el servidor 290 de contenidos está asociado con un host que transmite paquetes de datos que requieren una cantidad significativa de recursos de red, por ejemplo, un servicio de transmisión de vídeo (por ejemplo, YOUTUBE.COM, NETFLIX.COM, etc.), el gestor 270 de transporte identificará automáticamente un flujo de datos entre el servidor 290 de contenidos y el dispositivo 210 de cliente como un flujo elefante y pondrá ritmo al flujo de datos. En otro ejemplo, cuando el gestor 270 de transporte identifica que el servidor 290 de contenido está asociado con un servicio de juegos (por ejemplo, POKEMON GO, etc.), el gestor 270 de transporte identificará automáticamente el flujo de datos entre el servidor 290 de contenido y el dispositivo 210 de cliente como un flujo de elefante y pondrá ritmo al flujo de datos. Se pueden encontrar más detalles sobre la gestión de flujos de elefantes en la solicitud comúnmente asignada Solicitud de EE. UU. No. 15/703,908, titulada "DIRECTED HANDOVER OF ELEPHANT FLOWS," que fue presentada el 13 de septiembre de 2017, y por la presente se incorpora por referencia en su totalidad.

En la invención, el gestor 270 de transporte identifica un flujo de datos entre el servidor 290 de contenidos y el dispositivo 210 de cliente para su gestión mediante la identificación de un nombre de host asociado con el servidor 290 de contenidos, de acuerdo con diversas realizaciones de la presente divulgación. El gestor 270 de transporte

identifica el nombre de host interceptando los paquetes de datos transmitidos entre el servidor 290 de contenidos y el dispositivo 210 de cliente que atraviesan la tercera red 260.

Aunque los paquetes de datos incluyen información que identifica el nombre de host, esta información está encriptada. Por ejemplo, el nombre de host se incluye en una carga útil cifrada de cada uno de los paquetes de datos.

En lugar de descifrar los paquetes de datos, en una realización, el gestor 270 de transporte identifica el nombre de host del servidor 290 de contenidos extrayendo la dirección IP del servidor 290 de contenidos de uno de los paquetes de datos, accediendo a una tabla de información almacenada en un almacenamiento 232, identificando una entrada en la tabla de información que incluye la dirección IP extraída, y determinando el nombre de host leyendo la entrada identificada. La tabla de información es generada por el DNS espía 230, de acuerdo con diversas realizaciones.

En consecuencia, el gestor 270 de transporte gestiona los flujos de datos que atraviesan la tercera red 260 accediendo a la tabla de información generada por el DNS espía, en lugar de descifrar paquetes de datos individuales dentro de los flujos de datos.

En algunas realizaciones, el DNS espía 230, el gestor 270 de transporte y el almacenamiento 232 son dispositivos separados e interconectados. En otras realizaciones, el DNS espía 230, el gestor 270 de transporte y el almacenamiento 232, son el mismo dispositivo.

Las Figs. 3A a 3E ilustran dispositivos de acuerdo con diversas realizaciones de la presente divulgación. Cualquiera de los dispositivos mostrados en las Figs. 3A a 3E pueden implementarse en un ordenador de propósito general modificado (por ejemplo, configurado o programado) mediante software para que sea un ordenador de propósito especial que realice las funciones descritas en el presente documento para esa máquina, base de datos o dispositivo. Además, dos o más de las máquinas, bases de datos o dispositivos ilustrados en las Figs. 3A a 3E pueden combinarse en una sola máquina, y las funciones descritas en el presente documento para una sola máquina, base de datos o dispositivo pueden subdividirse entre varias máquinas, bases de datos o dispositivos.

La Fig. 3A ilustra un dispositivo 310 de cliente de acuerdo con una realización de la presente divulgación. El dispositivo 310 de cliente puede incluir diversos tipos de dispositivos de usuario, como dispositivos móviles (por ejemplo, ordenadores portátiles, teléfonos inteligentes, tabletas, etc.), dispositivos informáticos, decodificadores, dispositivos informáticos para vehículos, dispositivos de juego, etc. El dispositivo 310 de cliente puede soportar y ejecutar diversos sistemas operativos diferentes, tales como Microsoft® Windows®, Mac OS®, iOS®, Google® Chrome®, Linux®, Unix®, o cualquier otro sistema operativo móvil, incluyendo Symbian®, Palm®, Windows Mobile®, Google® Android®, Mobile Linux®, etc.

El dispositivo 310 de cliente incluye una interfaz 312, un procesador 314, un almacenamiento 316, y una o más aplicaciones 316.

La interfaz 312 incluye, por ejemplo, una pantalla táctil, un teclado, una cámara, uno o más sensores, o una combinación de los mismos. En una realización, el dispositivo 310 de cliente recibe una entrada de un usuario a través de la interfaz 312. En una realización específica, la entrada especifica un nombre de host de una fuente de contenido. Por ejemplo, la entrada especifica la dirección de un localizador universal de recursos (URL) de un sitio web específico en Internet.

El procesador 314 ejecuta comandos de programa. El almacenamiento 316, por ejemplo, almacena los comandos del programa que son ejecutados por el procesador 312. En una realización, el almacenamiento 316 es una memoria local.

El dispositivo 310 de cliente ejecuta una o más aplicaciones 316. En una realización, la una o más aplicaciones 316 incluye una aplicación de navegador de Internet, una aplicación de transmisión de vídeo, una aplicación de videojuegos, etc.

En la invención, el dispositivo 316 de cliente está configurado para solicitar una dirección IP de un servidor de contenidos asociado a un nombre de host conocido y recibir una respuesta DNS que identifica la dirección IP solicitada. El dispositivo 316 de cliente solicita además contenido transmitiendo una solicitud al servidor de contenido utilizando la dirección IP, y recibe el contenido solicitado del servidor de contenido en forma de uno o más paquetes de datos.

La Fig. 3B ilustra un DNS espía 330 de acuerdo con una realización de la presente divulgación. El DNS espía 330 incluye una interfaz 332, un procesador 334, un primer almacenamiento 336 y un segundo almacenamiento 390.

El segundo almacenamiento 390 almacena una tabla 392 de identificación generada por el DNS espía 330. La tabla 392 de identificación incluye una pluralidad de entradas que identifican una pluralidad de pares dirección IP/nombre de host, respectivamente, de acuerdo con una realización. Aunque el segundo almacenamiento 390 se ilustra dentro del DNS espía 330, el segundo almacenamiento 390 puede ser un dispositivo de almacenamiento separado del DNS espía 330, en una realización.

En diversas realizaciones, el DNS espía 330 está situado entre uno o más servidores DNS y uno o más dispositivos cliente. Las respuestas DNS transmitidas desde uno o más servidores DNS y uno o más dispositivos cliente pasan a través del DNS espía 220, o son interceptadas por él. El DNS espía 220 lee los nombres de host y la dirección IP de los registros de recursos (RR) en las respuestas DNS, por ejemplo. El nombre de host y la dirección IP en los RR de la respuesta DNS no están encriptados.

El DNS espía 330 identifica una pluralidad de pares nombre de host/dirección IP a partir de las respuestas DNS. El DNS espía 220 almacena los pares nombre de host/dirección IP en la tabla 392 de identificación en el segundo almacenamiento 390. En una realización, los pares nombre de host/dirección IP se incluyen en entradas respectivas de la tabla 392 de identificación.

En diversas realizaciones, la tabla 392 de identificación es accesible por otros dispositivos, tal como un gestor de transporte. El gestor de transporte, por ejemplo, puede gestionar el tráfico de red leyendo las entradas de la tabla 392 de identificación.

La Fig. 3C ilustra un servidor 350 DNS de acuerdo con una realización de la presente divulgación. El servidor 350 DNS incluye un procesador 352, un almacenamiento 354 y registros 358 DNS.

El procesador 352 ejecuta una o más políticas 356 almacenadas en el almacenamiento 354. Por ejemplo, el procesador 352 ejecuta comandos de programa almacenados en la memoria 354.

Cuando el servidor 350 DNS recibe una petición DNS que incluye un nombre de host, el servidor 350 DNS busca en los registros 358 DNS una dirección IP asociada al nombre de host. La dirección IP es la dirección IP de un servidor de contenidos asociado al nombre de host, por ejemplo. Los registros 358 DNS están estructurados de tal forma que el servidor 350 DNS puede buscar una dirección IP asociada a un nombre de host determinado, pero no puede buscar un nombre de host asociado a una dirección IP determinada.

El servidor 350 DNS genera entonces una respuesta DNS que incluye una pluralidad de RRs que incluyen el nombre de host y la dirección IP. El servidor 350 DNS transmite la respuesta DNS al origen de la solicitud DNS. Por ejemplo, cuando la solicitud DNS se transmite desde un dispositivo cliente, el servidor 350 DNS transmite la respuesta DNS al dispositivo cliente.

La Fig. 3D ilustra un gestor 370 de transporte de acuerdo con una realización de la presente divulgación.

El gestor 270 de transporte está configurado para gestionar el tráfico de datos que atraviesa una red cuando se satisfacen una o más condiciones. En algunas realizaciones, el gestor 370 de transporte es un gestor de entrega que dirige o gestiona la entrega de contenidos a través de una política de entrega que utiliza o usa el ancho de banda excedente de la red o la capacidad excedente de la red. Un excedente de ancho de banda de red o capacidad de red puede ser ancho de banda de red o capacidad de red que se determina que está disponible (por ejemplo, ociosa o libre) en una red en vista de la capacidad total de la red y/o y el uso total de la red. En algunas realizaciones, un proveedor de red determina la cantidad de capacidad de red excedente disponible en una red en vista de la capacidad total de la red y/o y el uso total de la red. La capacidad excedente de red puede determinarse de forma estática o dinámica y, por lo tanto, una capacidad excedente de red determinada para una red puede variar sustancial y/o aleatoriamente a lo largo del tiempo (por ejemplo, durante periodos de uso máximo), para escalas de tiempo largas o cortas, y/o entre un proveedor de servicios y otro.

La capacidad excedente, por tanto, puede ser el ancho de banda o capacidad libre entre un uso real y/o actual del ancho de banda una capacidad total (o, un porcentaje predeterminado de la capacidad total). Por lo tanto, el gestor 370 de transporte puede dirigir o gestionar la entrega de contenido entre proveedores de contenido (por ejemplo, servidores de contenido), cachés de borde de red y dispositivos cliente a través de diversas políticas o protocolos de entrega seleccionados que utilizan anchos de banda o capacidades libres, disponibles, ociosos o excedentes de redes, tal como rutas o protocolos que entregan datos a través de redes actualmente infrautilizadas que de otro modo no estarían en uso, y/o sin impactar o alterar sustancialmente el rendimiento del transporte asociado con otro tráfico de datos que comparte la red.

Pueden encontrarse más detalles sobre la entrega de contenidos utilizando capacidad de red excedentaria en la patente comúnmente asignada de EE. UU. No. 7,500,010, expedida el 3 de marzo de 2009titulada ADAPTIVE FILE DELIVERY SYSTEM AND METHOD, Pat. de EE.UU No. 8,589,585, emitida el 19 de noviembre de 2013titulada ADAPTIVE FILE DELIVERY SYSTEM AND METHOD, Solicitud de Patente Publicada en EE. UU. No. 2010/0198943, presentada el 15 de abril de 2010titulada SYSTEM AND METHOD FOR PROGRESSIVE DOWNLOAD USING SURPLUS NETWORK CAPACITY, y Solicitud de Patente Publicada en EE. UU. No. 2013/0124679, presentada el 3 de enero de 2013titulada SYSTEM AND METHOD FOR PROGRESSIVE DOWNLOAD WITH MINIMAL PLAY LATENCY.

El gestor 370 de transporte incluye una interfaz 372, un procesador 374, una cola 376, un gestor 378 y un almacenamiento 380.

El procesador 374 ejecuta una o más políticas 382 almacenadas en el almacenamiento 380. Por ejemplo, el procesador 374 ejecuta comandos de programa almacenados en la memoria 380. Diversas funciones del gestor 370 de transporte son ejecutadas por el procesador 374.

El gestor 370 de transporte identifica las características de los flujos de datos que atraviesan una red, y las características de la propia red, y gestiona los flujos de datos basándose en las características. En una realización, el gestor 370 de transporte identifica un flujo de datos para su gestión interceptando un paquete de datos en el flujo de datos, leyendo una dirección IP de una fuente del paquete de datos desde el paquete de datos, e identificando un nombre de host de la fuente del paquete de datos accediendo a una tabla de identificación.

Por ejemplo, cuando el gestor 370 de transporte determina que un flujo de datos que atraviesa una red es un flujo de elefante basándose en un nombre de host de una fuente del flujo de datos, el gestor 370 de transporte pondrá ritmo al flujo de datos. En un ejemplo específico, el gestor 370 de transporte almacena temporalmente datos que incluyen paquetes del flujo elefante en la cola 376, y libera selectivamente los paquetes a su destino a través de la capacidad de red excedente de una red, cuando la capacidad de red excedente está disponible.

La Fig. 3E ilustra un servidor 390 de contenidos de acuerdo con una realización de la presente divulgación. El servidor 390 de contenidos incluye una interfaz 392, un procesador 394 y un almacenamiento 396.

El procesador 394 ejecuta una o más políticas 392 almacenadas en el almacenamiento 396. Por ejemplo, el procesador 394 ejecuta comandos de programa almacenados en la memoria 396. Diversas funciones del servidor 390 de contenidos son ejecutadas por el procesador 394.

El servidor 390 de contenidos recibe una solicitud de contenido de una fuente y transmite uno o más de los archivos 398 almacenados en el almacenamiento 396 en respuesta a la solicitud. El servidor 390 de contenidos transmite el uno o más archivos 398 en forma de una pluralidad de paquetes de datos, por ejemplo.

El servidor 390 de contenidos puede proporcionar una variedad de medios diferentes y otros tipos de contenidos, tal como contenidos de vídeo (por ejemplo, películas, programas de televisión, programas de noticias, videoclips), contenidos de imagen (por ejemplo, presentaciones de imágenes o fotografías), contenidos de audio (por ejemplo, programas de radio, música, podcasts), etc. El servidor 390 de contenidos puede entregar, transferir, transportar y/o proporcionar de otra forma archivos multimedia y otros contenidos a cachés de borde de red (no mostrados), que pueden entregar, transferir, transportar y/o proporcionar de otra forma el contenido a dispositivos solicitantes (por ejemplo, equipos 110 a-c de usuario) a través de diversos protocolos de transferencia de medios (por ejemplo, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), HTTP Live Streaming (HLS), HTTP Dynamic Streaming (HDS), HTTP Smooth Streaming (HSS), Dynamic Adaptive Streaming over HTTP (DASH), Real Time Streaming Protocol (RTSP), etc.).

La Fig. 4 ilustra un paquete 400 de datos de acuerdo con una realización de la presente divulgación. El paquete 400 de datos incluye un cabezal 410 y una carga 420 útil.

El cabezal 410 incluye una dirección 412 IP de origen y una dirección 414 IP de destino. La dirección 412 IP de origen es una dirección IP de un origen del paquete 400 de datos, y la dirección 414 IP de destino es una dirección IP de un destino del paquete 400 de datos. El cabezal 410 no está encriptada, de acuerdo con una realización.

La carga 420 útil incluye uno o más archivos 422. La carga 420 útil incluye, por ejemplo, datos de la capa de aplicación. La carga 420 útil está encriptada.

En la invención, el paquete 400 de datos se transmite entre un servidor de contenidos y un dispositivo cliente, y es interceptado por un gestor de transporte.

La Fig. 5 ilustra una respuesta 500 DNS de acuerdo con la invención.

La respuesta 500 DNS incluye una pluralidad de RRs 510. Por ejemplo, los RR 510 incluyen un campo 512 RDATA y un campo 514 NOMBRE. El campo 512 RDATA incluye una dirección IP, y el campo 514 NOMBRE incluye un nombre de host asociado a la dirección IP.

En una realización, la respuesta 500 DNS se transmite desde un servidor DNS a un dispositivo cliente. Además, la respuesta 500 DNS no está cifrada. Un DNS espía, por ejemplo, intercepta la respuesta 500 DNS transmitida desde el servidor DNS al dispositivo cliente, y lee la dirección IP del campo 512 RDATA y el nombre de host del campo 514 NOMBRE sin realizar el descifrado.

La Fig. 6 ilustra una tabla 600 de identificación de acuerdo con la invención.

La tabla 600 de identificación incluye una pluralidad de entradas 610_1 a 610_N, donde N es un tamaño de la tabla

600 de identificación. Cada una de las entradas 610_1 a 610_N corresponde a un par específico de nombre de host/dirección IP. La tabla 600 de identificación es una tabla de caché indexada por las direcciones IP de los pares nombre de host/dirección IP, en una realización.

Cada una de las entradas 610_1 a 610_N incluye una dirección IP, un nombre de host, un último tiempo activo de un paquete de datos desde la dirección IP, y una cantidad de bytes acumulados asociados con el tráfico de datos transmitido desde la dirección IP.

En esta divulgación, campos como el último tiempo activo y la cantidad de bytes acumulados pueden denominarse "características" de los correspondientes pares nombre de host/dirección IP. En una realización, las características son utilizadas por un DNS espía para identificar una o más entradas menos significativas en la tabla 600 de identificación. El DNS espía puede entonces eliminar las entradas menos significativas de la tabla 600 de identificación en una operación de eliminación.

En algunas realizaciones, las características son utilizadas por un gestor de transporte para identificar pares nombre de host/dirección IP asociados con flujos de datos relativamente pesados. Por ejemplo, el gestor de transporte identifica las entradas que incluyen cantidades relativamente grandes de bytes acumulados como probablemente asociadas a flujos de elefantes.

De acuerdo con diversas realizaciones, cada una de las entradas 610_1 a 610_N es generada y actualizada por un DNS espía y almacenada en un depósito.

La Fig. 7 ilustra un procedimiento 700 de extracción de un nombre de host y una dirección IP de una respuesta DNS de acuerdo con la invención.

El procedimiento 700 puede ser realizado por un DNS espía, por ejemplo.

En S710, se recibe un paquete. En una realización, el paquete se intercepta mientras se transmite desde un servidor DNS a un dispositivo de cliente.

El paquete se identifica como una respuesta DNS en S720.

Después de identificar el paquete como una respuesta DNS, se extrae un nombre de host y una dirección IP de la respuesta DNS en S730. El nombre de host y la dirección IP se leen de las RR en la respuesta DNS. Por ejemplo, el nombre de host se lee de un campo NOMBRE en los registros de recursos, y la dirección IP se lee de un campo RDATA en los registros de recursos

La Fig. 8 ilustra un procedimiento 800 de adición de una nueva entrada a una tabla de identificación de acuerdo con una realización de la presente divulgación. En una realización, el procedimiento 800 es ejecutado por un DNS espía.

En S810 se determina un par de nombre de host y dirección IP. Por ejemplo, el nombre de host y la dirección IP se leen a partir de una respuesta DNS.

La Fig. 9 ilustra un procedimiento 900 para determinar la longitud de un paquete no DNS de acuerdo con una realización de la presente divulgación. El procedimiento 900 es realizado por un DNS espía, por ejemplo.

En S910, se recibe un paquete de datos. En una realización, el paquete de datos se intercepta mientras se transmite entre un servidor de contenidos y un dispositivo cliente.

El paquete de datos es identificado como un paquete no-DNS en S920. El paquete de datos no es una solicitud DNS ni una respuesta DNS. El paquete no DNS es, por ejemplo, un paquete de transmisión de vídeo.

En S930, se determina un tamaño del paquete de datos. Por ejemplo, se determina el número de bytes que contiene el paquete.

La Fig. 10 ilustra un procedimiento 1000 de determinación de una marca de tiempo de un paquete no DNS de acuerdo con una realización de la presente divulgación. El procedimiento 1000 es realizado por un DNS espía, por ejemplo.

En S1010, se recibe un paquete de datos. En una realización, el paquete de datos se intercepta mientras se transmite entre un servidor de contenidos y un dispositivo cliente.

El paquete de datos es identificado como un paquete no-DNS en S1020. El paquete de datos no es una solicitud DNS ni una respuesta DNS. El paquete no DNS es, por ejemplo, un paquete de transmisión de vídeo.

A continuación, en S1030, se determina una marca de tiempo asociada al paquete. Por ejemplo, la marca de tiempo

es la hora a la que se recibe el paquete de datos. En otro ejemplo, la marca de tiempo se obtiene directamente del paquete no DNS.

La Fig. 11 ilustra un procedimiento 1100 de actualización de una entrada de una tabla de identificación de acuerdo con una realización de la presente divulgación. El procedimiento 1100 es realizado por un DNS espía, por ejemplo.

En S1110, se determinan una dirección IP y una característica de un paquete no DNS. En una realización, el paquete no DNS se intercepta entre un servidor de contenidos y un dispositivo cliente. En un ejemplo, la dirección IP es una dirección IP de una fuente del paquete de datos, y se determina leyendo la dirección IP de un cabezal no cifrado del paquete no DNS. De acuerdo con una realización, la característica es un tamaño del paquete de datos, una marca de tiempo del paquete de datos, o una combinación de las mismas.

En S1120, se identifica una entrada en una tabla de identificación. La entrada incluye la dirección IP y un nombre de host asociado a la dirección IP, por ejemplo.

La entrada se actualiza en función de la característica en S1130. Por ejemplo, cuando la entrada incluye un campo de dirección IP, un campo de nombre de host, un campo de última hora activa y un campo de número de bytes acumulados, el campo de última hora activa se actualiza en función de la marca de tiempo del paquete de datos, y el campo de número de bytes acumulados se actualiza en función del tamaño del paquete de datos.

La Fig. 12 ilustra un procedimiento 1200 de gestión de un flujo de datos utilizando una tabla de identificación de acuerdo con una realización de la presente divulgación. El procedimiento 1200 lo realiza, por ejemplo, un gestor de transporte.

En S1210, se recibe un paquete en un flujo de datos. El paquete es, por ejemplo, un paquete de datos que incluye un cabezal y una carga útil. El cabezal no está cifrado. La carga útil está cifrada e incluye datos de la capa de aplicación.

En S1220, se identifica una dirección IP a partir del cabezal del paquete. La dirección IP indica el destino del paquete. En una realización, la dirección IP de la fuente del paquete se obtiene leyendo el cabezal del paquete. La dirección IP es la dirección IP de un servidor de contenidos, por ejemplo.

En S1230, se determina un nombre de host asociado con la dirección IP identificada accediendo a una tabla de identificación. La tabla de identificación incluye una pluralidad de pares dirección IP/nombre de host en una pluralidad de entradas. En una realización, la tabla de identificación es una tabla de caché que está indexada por las direcciones IP. En consecuencia, el nombre de host asociado con la dirección IP identificada puede determinarse identificando una entrada en la tabla de identificación que incluya la dirección IP identificada, y leyendo el nombre de host correspondiente en la entrada identificada.

El flujo de datos se gestiona basándose en el nombre de host identificado en S1240. Por ejemplo, se le aplica ritmo al flujo de datos cuando se determina que el nombre de host identificado corresponde a un host que se ha asociado históricamente con tráfico de datos gravoso para una red. En un ejemplo específico, el flujo de datos se identifica como un flujo de elefante basado en el nombre de host identificado, y se le aplica un ritmo.

La Fig. 13 ilustra un procedimiento 1300 de identificación y aplicación de ritmo de un flujo de elefante utilizando una tabla de identificación de acuerdo con una realización de la presente divulgación. El procedimiento 1300 lo realiza, por ejemplo, un gestor de transporte.

En S 1310, se recibe un paquete en un flujo de datos. El paquete es un paquete de datos no DNS, por ejemplo. En una realización, una copia del paquete se almacena temporalmente en caché, y el propio paquete se libera, para que pueda llegar a su destino sin retrasos significativos.

En S1320, se identifica una dirección IP a partir del cabezal del paquete. En una realización, la dirección IP indica un destino del paquete o un origen del paquete. En diversas realizaciones, se determinan tanto una dirección IP que indica el destino del paquete como una dirección IP que indica el origen del paquete. La dirección IP es, por ejemplo, la dirección IP de un servidor de contenidos.

Un nombre de host asociado con la dirección IP identificada se determina en S1330 accediendo a una tabla de identificación. La tabla de identificación almacena una pluralidad de pares nombre de host/dirección IP previamente identificados, y está indexada por dirección IP. En una realización, el nombre de host se recupera de una entrada que incluye la dirección IP identificada.

En S 1340, se determina que el flujo de datos es un flujo elefante basándose en el nombre de host. Por ejemplo, el flujo de datos se identifica como un flujo elefante cuando el nombre de host indica un host de transmisión de vídeo conocido.

Después de que se determina que el flujo de datos es un flujo de elefante, se le aplica ritmo al flujo de datos en S1350.

En una realización, una pluralidad de paquetes de datos en el flujo de datos que atraviesa una red se gestiona después de que se determine que el flujo de datos es un flujo elefante. Por ejemplo, los paquetes de datos del flujo de datos pueden enrutarse selectivamente a través de la capacidad excedente de la red. En una realización específica, los paquetes de datos de ese flujo de datos se enrutan selectivamente a través de una red diferente cuando la red diferente está disponible, tal como una red WIFI que está conectada a un dispositivo cliente que recibe paquetes de datos en el flujo de datos.

La Fig. 14 ilustra un procedimiento 1400 de control de un tamaño de una tabla de identificación de acuerdo con una realización de la presente divulgación. El procedimiento 1400 es realizado por un DNS espía, por ejemplo.

En S1410, se añade una nueva entrada a una tabla de identificación. La nueva entrada incluye un par de nombre de host/dirección IP. Por ejemplo, la nueva entrada incluye un par nombre de host/dirección IP que no estaba incluido previamente en la tabla de identificación.

En S1420, se determina que un tamaño de la tabla de identificación excede un tamaño predeterminado. En diversas realizaciones, el tamaño se define como un número de índices, una cantidad de memoria necesaria para almacenar la tabla de identificación, o una combinación de los mismos.

En S1430, una o más entradas de la tabla de identificación son eliminadas de la tabla de identificación. Por ejemplo, las una o más entradas se borran de la tabla de identificación.

La una o más entradas eliminadas pueden identificarse de diversas maneras. En algunas realizaciones, la una o más entradas son las entradas menos significativas de la tabla de identificación. Las entradas menos significativas pueden identificarse basándose en los campos de características de la tabla de identificación. Por ejemplo, si cada una de las entradas incluye una marca de tiempo que indica el paquete de datos observado más reciente correspondiente a los pares nombre de host/dirección IP, las entradas con las marcas de tiempo más antiguas se eliminan de la tabla de identificación. En otro ejemplo, si cada una de las entradas incluye un número de bytes transferidos que se observa que corresponden a pares nombre de host/dirección IP, las entradas con el menor número de bytes transferidos se eliminan de la tabla de identificación. En algunas realizaciones, la una o más entradas se identifican basándose en una combinación de múltiples criterios.

Varias de las una o más entradas eliminadas también pueden identificarse de diversas maneras. Por ejemplo, cuando la tabla de identificación alcanza su tamaño máximo, se elimina un porcentaje predeterminado de entradas de la tabla de identificación.

La Fig. 15 ilustra un procedimiento 1500 de generación, uso y actualización de una tabla de identificación de acuerdo con una realización de la presente divulgación.

En S1510, se recibe un paquete. Por ejemplo, el paquete se intercepta mientras se transmite a un dispositivo cliente.

En S1512 y S1520, el paquete es inspeccionado e identificado como una respuesta DNS, un paquete de carga útil TCP o UDP, o ninguno de los dos.

Cuando el paquete es una respuesta DNS, el paquete es analizado y un nombre de host y una o más direcciones IP son extraídas de la respuesta DNS en S1530. de acuerdo con una realización, los datos extraídos se ponen en cola para que un procedimiento independiente los analice después de que se libere el paquete, para limitar la cantidad de tiempo que el paquete es retenido por el sistema y eliminar cualquier impacto en la latencia de la comunicación cliente/servidor.

Cuando el paquete no es una respuesta DNS, el paquete es examinado para determinar si el paquete es un paquete no DNS, tal como un protocolo de control de transmisión (TCP) o un paquete de protocolo de datagrama de usuario (UDP), en S1520.

Cuando el paquete es un paquete TCP/UDP, en S1524 se examina la longitud de la carga útil del paquete. El paquete se pone en cola y se libera, de modo que la longitud de la carga útil se examina en un procedimiento independiente para limitar la cantidad de tiempo que el paquete es retenido por el sistema y eliminar cualquier impacto en la latencia de la comunicación cliente/servidor. Por ejemplo, el paquete se pone en cola y se trata de manera similar al procedimiento independiente realizado en S1330, de modo que la longitud de la carga útil se determina y analiza después de que se libera el paquete.

Si el paquete no es ni una respuesta DNS ni un paquete TCP/UDP, el paquete es liberado en S1522.

En S1532, se determina la presencia de la dirección IP extraída en una tabla de identificación. Por ejemplo, cada uno de los elementos en cola se lee y se compara con una pluralidad de entradas de la tabla de identificación.

En el caso de que no exista ninguna entrada en la tabla que incluya la dirección IP extraída, se determina si la tabla de identificación está llena o no en S1540.

Cuando la tabla de identificación no está llena, se crea una nueva entrada en la tabla en S1542. De acuerdo con diversas realizaciones, la creación de nuevas entradas en la tabla construye efectivamente la tabla de identificación como una caché DNS, en la que diversos pares nombre de host/dirección IP se asignan entre sí.

En el caso de que exista una entrada, la entrada se actualiza basándose en el paquete en S1534. La entrada de la tabla, en algunos ejemplos, incluye los siguientes campos: Dirección IP, nombre de dominio, última hora activa y bytes acumulados. Las entradas se almacenan en la tabla de identificación. La tabla de identificación es, por ejemplo, una tabla hash, indexada por la dirección IP.

Cuando la tabla de identificación está llena, una o más entradas menos significativas en la tabla de identificación son eliminadas en S1544. Es decir, la tabla hash tiene una longitud máxima configurable, para que la tabla de identificación no supere un tamaño determinado. Cuando la tabla de identificación tiene la longitud máxima, la tabla de identificación puede eliminarse a un porcentaje de su tamaño, en una realización. En otra realización, se elimina un número predeterminado de entradas. Las entradas se eliminan borrándolas de la tabla de identificación, por ejemplo.

En diversas realizaciones, las entradas menos significativas se eliminan de la tabla de identificación. En una realización, las entradas menos significativas son entradas que incluyen el menor número de bytes acumulados registrados, el último tiempo activo más temprano registrado, o una combinación de los mismos. Por ejemplo, se elimina primero un porcentaje de las entradas correspondientes al menor número de bytes acumulados y, en caso de empate, se eliminan las entradas correspondientes a la Última Hora Activa más antigua.

Cuando se determina que se han eliminado una o más entradas en S1546, el procedimiento 1500 vuelve a S 1542, de manera que se genera una nueva entrada en la tabla de identificación basada en el paquete sin exceder el tamaño máximo de la tabla de identificación.

En diversas realizaciones, el tráfico de datos a través de una red se gestiona accediendo a la tabla de identificación. A la tabla de identificación se accede consultando por dirección IP, lo que permitirá a otro sistema (o sistema con integración de DNS espía) obtener el nombre de dominio de dicha dirección IP. En una versión, estos datos se ponen a disposición de un sistema de recogida de estadísticas, que activa la recogida de estadísticas granulares sobre todo el tráfico con un dominio específico. A su vez, estas estadísticas pueden utilizarse para determinar los n dominios principales de una red específica.

Algunos ejemplos de los datos estadísticos granulares que pueden recopilarse sobre un dominio específico incluyen (pero no se limitan a): Bytes totales ascendentes/descendentes, latencia, caudal, buen caudal, tipo de acceso por radio, índice de congestión, bytes transferidos en flujos que alcanzaron un umbral de bytes transferidos acumulados especificado (flujos estándar, flujos elefante, etc.), estadísticas desglosadas por hora del día y/o por ubicación, o una combinación de ambas.

Las realizaciones proporcionan un sistema y procedimiento para entregar contenido de datos en paquetes a través de redes de acceso compartido de una manera que distribuye más uniformemente el tráfico de usuario agregado en el tiempo, por ejemplo, moviendo el tráfico de los momentos de congestión de la red de cuello de botella a los siguientes momentos adyacentes de capacidad de red excedente. El efecto neto de esta redistribución del tráfico puede reducir los intervalos de picos de uso y congestión (cuando la red es incapaz de suministrar suficiente capacidad de caudal para todos los usuarios), lo que puede dar lugar a una mayor utilización agregada permitida de la red antes de que la calidad del servicio de red se degrade para los usuarios.

El término "capacidad de red excedente" (también conocido como "capacidad ociosa") se entiende en algunas realizaciones como capacidad de red compartida (por ejemplo, ancho de banda de red, recursos de red) que puede ser utilizada por realizaciones de la invención para transferir porciones o la totalidad de los datos a través de una red, pero que de otro modo no se utiliza. En otras palabras, si la capacidad de la red es X y la carga de tráfico agregada actual de la red es Y, entonces la capacidad excedente disponible es X-Y, donde Y no puede ser mayor que X. En una realización, uno de los objetivos del uso de la capacidad excedente de la red es utilizar parte o toda la capacidad Y para transferir datos, lo que implica que, si Y es cero, la transferencia se ralentiza o se detiene y cede el canal al tráfico de otros usuarios que comparten la red. En algunos escenarios, la capacidad de red excedente en redes de datos compartidas multiusuario es transitoria y puede fluctuar aleatoriamente de un momento a otro. Además, el uso del excedente tal como se define puede ser distinto de un uso compartido competitivo justo o similar de la capacidad de la red (por ejemplo, cuando la carga de tráfico agregada supera el límite de capacidad de la red X, cada uno de los N usuarios que comparten la red recibe una parte X/N de la capacidad de la red).

En una realización específica, el sistema puede identificar de forma única un flujo de tráfico de datos basado en su dirección IP de cliente asociada y la dirección IP del servidor de destino. A continuación, el sistema puede caracterizar

el tráfico como un gran flujo basándose en parámetros tal como el rendimiento, los bytes entregados, otras características o una combinación de ellas. El sistema es un gestor de transportes, por ejemplo.

El sistema puede consultar la tabla de identificación generada por el DNS espía, y determinar que el nombre de host al que está asociada la dirección IP del servidor pertenece a un proveedor de vídeo conocido (por ejemplo, YOUTUBE). Por tanto, se podría llegar a la conclusión de que el flujo de datos es en realidad un vídeo debido a su tamaño y destino conocido.

Esta información puede ponerse a disposición de un gestor de transporte, que permite aplicar reglas de gestión específicas a un subconjunto concreto de tráfico (tal como un vídeo en este ejemplo) que puede pertenecer o no a un dominio específico (como YOUTUBE en este ejemplo). Las reglas pueden incluir políticas que garanticen que el tráfico gestionado cede ancho de banda compartido a otro tráfico (es decir, utiliza la capacidad de red sobrante), se prioriza de otro modo o se marca para no aplicar ninguna gestión específica.

De acuerdo con diversas realizaciones, el DNS espía opera con una serie de características, tales como 1) la separación del procedimiento de resolución de nombres de host DNS/direcciones IP de los procedimientos de caracterización/gestión/estadística de tráfico, 2) su capacidad para realizar la recogida de estadísticas granulares sobre flujos de tráfico encriptados, 3) la creación de una caché DNS dinámica que se adapta a los cambios en las asignaciones de nombres de host/direcciones IP en tiempo real sin requerir manipulación externa, y 4) la aplicación de la asignación de nombres de host/direcciones IP a la gestión del tráfico para mejorar la eficiencia de la red.

De acuerdo con una realización, un sistema construye una caché DNS virtual para su propio uso interno, pero no actúa como un servidor DNS virtual. El sistema intercepta los paquetes de respuesta DNS enviados a través de una red, extrae información de los paquetes de respuesta DNS, construye una tabla basada en la información extraída, pero no modifica ni manipula los paquetes de respuesta DNS enviados a través de la red.

Las realizaciones de la presente divulgación podrían utilizarse para identificar y rastrear el tráfico hacia y desde nombres de host específicos. En una versión, la información recopilada sobre nombres de dominio podría proporcionarse a un sistema que recoge estadísticas sobre subconjuntos de tráfico, flujos únicos de tráfico, o ambos. En otra versión, la información podría proporcionarse a un sistema que gestiona la entrega de contenidos a y desde terminales UE, que aplicaría políticas de gestión especificadas basadas en el nombre de dominio.

El sistema y los procedimientos que comprenden diversas realizaciones de la presente divulgación se utilizan para analizar y gestionar el tráfico de datos entre diversos dispositivos cliente y servidores de contenido, pero no requieren modificación de una aplicación de usuario instalada en los dispositivos cliente que solicita contenido, o de un servidor de contenido que proporciona contenido, lo que permite un rápido despliegue en redes comerciales, tales como redes celulares móviles.

Diversas realizaciones de la presente divulgación abordan múltiples problemas tecnológicos asociados con la entrega de contenidos, las redes inalámbricas, la seguridad y otros campos tecnológicos.

Por ejemplo, al generar una tabla de identificación que mapea direcciones IP a nombres de host, el tráfico de red puede analizarse efectivamente y los flujos de datos pueden identificarse para su gestión sin realizar operaciones de descifrado computacionalmente costosas.

Por ejemplo, gestionando selectivamente los flujos de datos que atraviesan una red basándose en los nombres de host asociados a los flujos de datos, los recursos de la red pueden conservarse eficientemente y la congestión de la red puede prevenirse eficientemente.

Por ejemplo, eliminando selectivamente las entradas menos significativas de la tabla de identificación, el tamaño de la tabla de identificación no se vuelve inmanejable, pero la tabla de identificación mantiene registros de direcciones IP y nombres de host que son probablemente relevantes para gestionar nuevos flujos de datos que atraviesan la red.

REIVINDICACIONES

1. Un procedimiento, que comprende:

interceptar un primer paquete de datos que se transmite desde un servidor de sistema de nombres de dominio, DNS, a un primer dispositivo de cliente, incluyendo el primer paquete de datos una respuesta DNS (S1512);
extraer (S1530) una primera dirección de protocolo de Internet (IP) y un primer nombre de host de la respuesta DNS;
crear una primera entrada en una tabla (S 1542) de identificación, cada entrada de la tabla de identificación incluye una dirección IP, un nombre de host, un campo de última hora activa y un campo (600) de número de bytes acumulados;
almacenar la primera dirección IP y el primer nombre de host en la primera entrada de la tabla (S1542) de identificación;
interceptar un segundo paquete de datos que se transmite en un flujo de datos desde un servidor de contenidos a un segundo dispositivo (S1210) de cliente;
identificar una segunda dirección IP en un cabezal del segundo paquete de datos, siendo la segunda dirección IP una fuente del segundo paquete (S1220) de datos;
determinar que la segunda dirección IP está en la primera entrada en respuesta a que la primera dirección IP almacenada en la primera entrada es idéntica a la segunda dirección (S 1230) IP;
en respuesta a la determinación de que la segunda dirección IP se encuentra en la primera entrada:
determinar, basándose en el primer nombre de host de la primera entrada, si debe aplicarse una política de gestión del tráfico al flujo (S1240) de datos, y
en respuesta a la determinación de que debe aplicarse la política de gestión del tráfico de datos, aplicar la política de gestión del tráfico al flujo de datos para entregar el segundo paquete de datos al segundo dispositivo (S1240) de cliente; **caracterizado porque**:
cuando la tabla de identificación supera un tamaño (S1420) predeterminado, identificar una segunda entrada de la tabla de identificación que tenga el campo de número de bytes acumulados con un valor más bajo, y eliminar la segunda entrada de la tabla (S1430) de identificación,
en respuesta a la determinación de que la segunda dirección IP se encuentra en la primera entrada, y
determinar una característica del segundo paquete de datos, siendo la característica una cantidad de bytes en el segundo paquete de datos y una marca de tiempo que indica la hora de recepción del segundo paquete (S1110) de datos,
actualizar un último campo de tiempo activo de la primera entrada de acuerdo con la marca de tiempo de la característica (S1130), y
actualizar un campo de número de bytes acumulados de la primera entrada de acuerdo con la cantidad de bytes de la característica (S1130).

2. El procedimiento de la reivindicación 1, en el que la identificación de la segunda entrada de la tabla de identificación incluye, cuando una pluralidad de entradas de la tabla de identificación tienen respectivos campos de número de bytes acumulativos con el valor más bajo, la identificación como segunda entrada de una entrada que tiene la última hora activa más temprana registrada entre la pluralidad de entradas que tienen respectivos campos de número de bytes acumulativos con el valor (S1544) más bajo.

3. El procedimiento de la reivindicación 1, en el que la gestión del flujo de datos incluye hacer que el flujo de datos se transfiera al segundo dispositivo de usuario a través de la capacidad de red excedente de una red, siendo la capacidad de red excedente una capacidad disponible de la red en vista de una capacidad total de la red y un uso total de la red.

4. El procedimiento de la reivindicación 1, en el que una carga útil de los segundos datos está cifrada, y en el que la segunda dirección IP se extrae del cabezal sin realizar el descifrado.

5. El procedimiento de la reivindicación 1, en el que la extracción de la dirección IP y el nombre de host de la respuesta DNS incluye la lectura de la dirección IP y el nombre de host de los registros de recursos (RR) en la respuesta DNS.

6. El procedimiento de la reivindicación 5, en el que la lectura de la dirección IP y el nombre de host de los RR en la respuesta DNS incluye la lectura de la dirección IP en un campo "RDATA" de la respuesta DNS y la lectura del nombre de host en un campo "NOMBRE" de la respuesta DNS.

7. Un sistema, que comprende: un procesador; y una memoria que almacena comandos de programa que, cuando son ejecutados por el procesador, hacen que el primer procesador lleve a cabo el procedimiento de la reivindicación 1.

8. Un medio de almacenamiento legible por ordenador que comprende instrucciones que, cuando son ejecutadas por un ordenador, hacen que el ordenador lleve a cabo el procedimiento de la reivindicación 1.

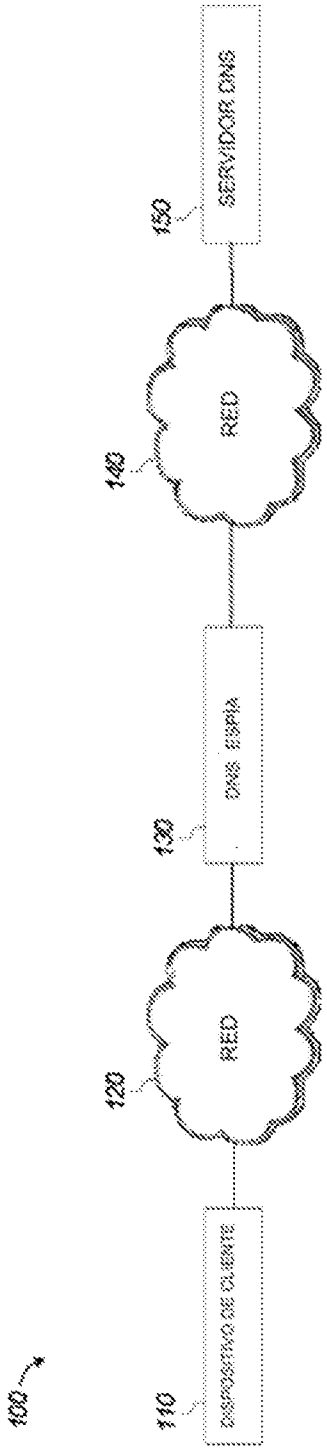
100
110
DISPOSITIVO DE CLIENTE
120
RED
130
DNS ESPÍA
140
RED
150
SERVIDOR DNS

Fig. 1

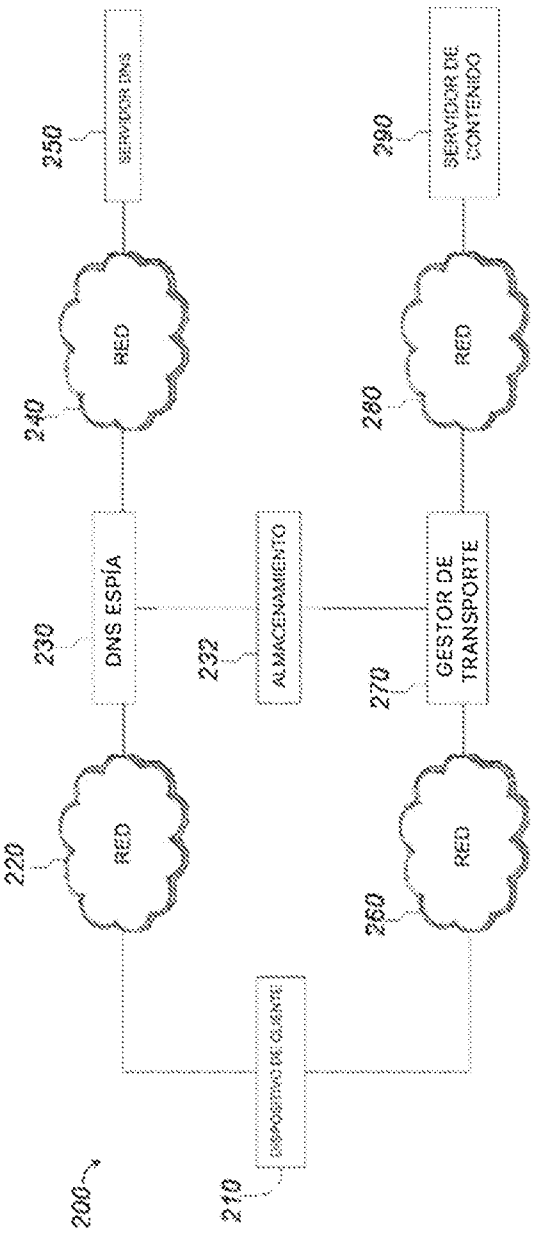
200
210
DISPOSITIVO DE CLIENTE
220
RED
230
DNS ESPÍA
232
ALMACENAMIENTO
240
RED
250
SERVIDOR DNS
260
RED
270
GESTOR DE TRANSPORTE
280
RED
290
SERVIDOR DE CONTENIDO

Fig. 2

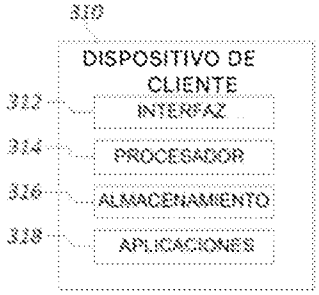

Fig. 3A

Fig. 3B

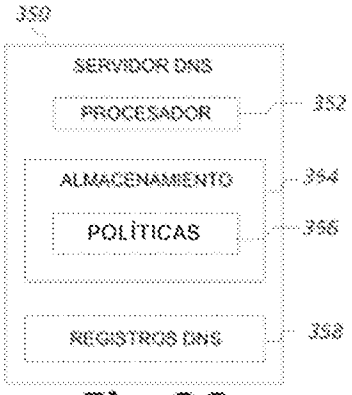

Fig. 3C

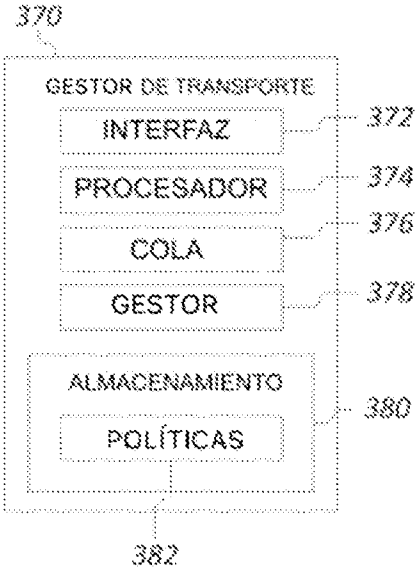
370
GESTOR DE TRANSPORTE
INTERFAZ
372
PROCESADOR
374
COLA
376
GESTOR
378
ALMACENAMIENTO
POLÍTICAS
380
382

Fig. 3D

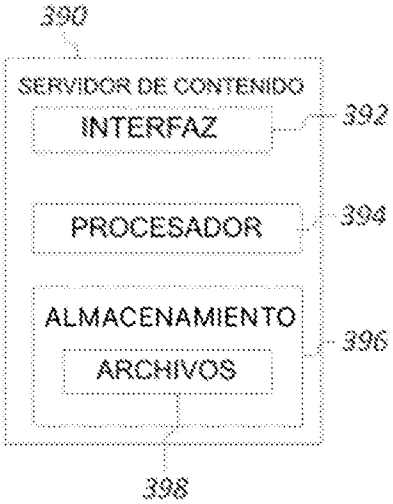
390
SERVIDOR DE CONTENIDO
INTERFAZ
392
PROCESADOR
394
ALMACENAMIENTO
ARCHIVOS
396
398

Fig. 3E

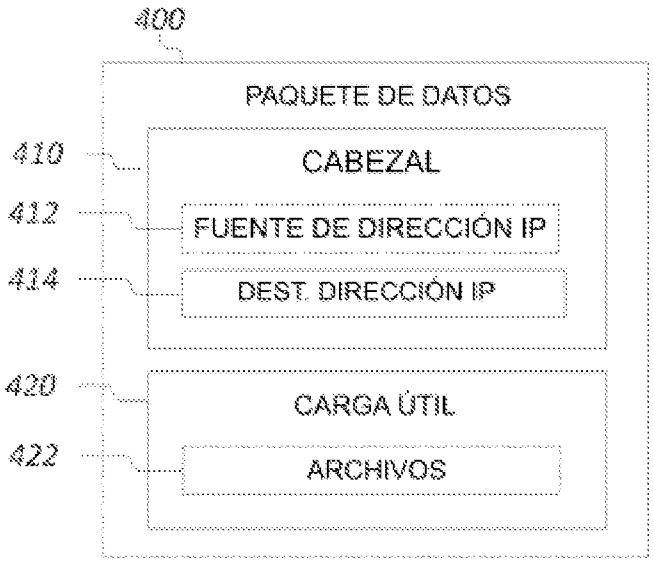
400
PAQUETE DE DATOS
410
CABEZAL
412
FUENTE DE DIRECCIÓN IP
414
DEST. DIRECCIÓN IP
420
CARGA ÚTIL
422
ARCHIVOS

Fig. 4

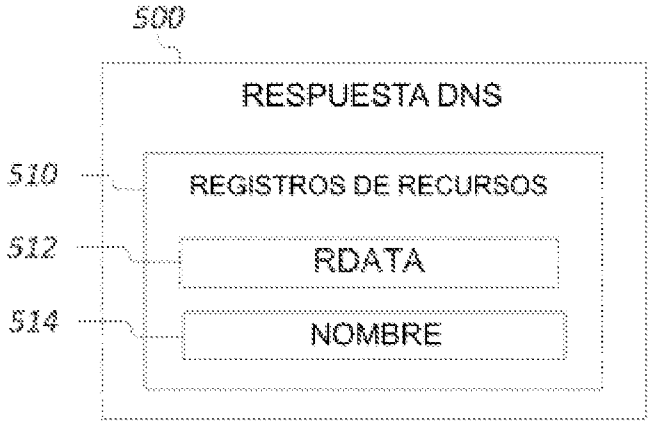
500
RESPUESTA DNS
510
REGISTROS DE RECURSOS
512
RDATA
514
NOMBRE

Fig. 5

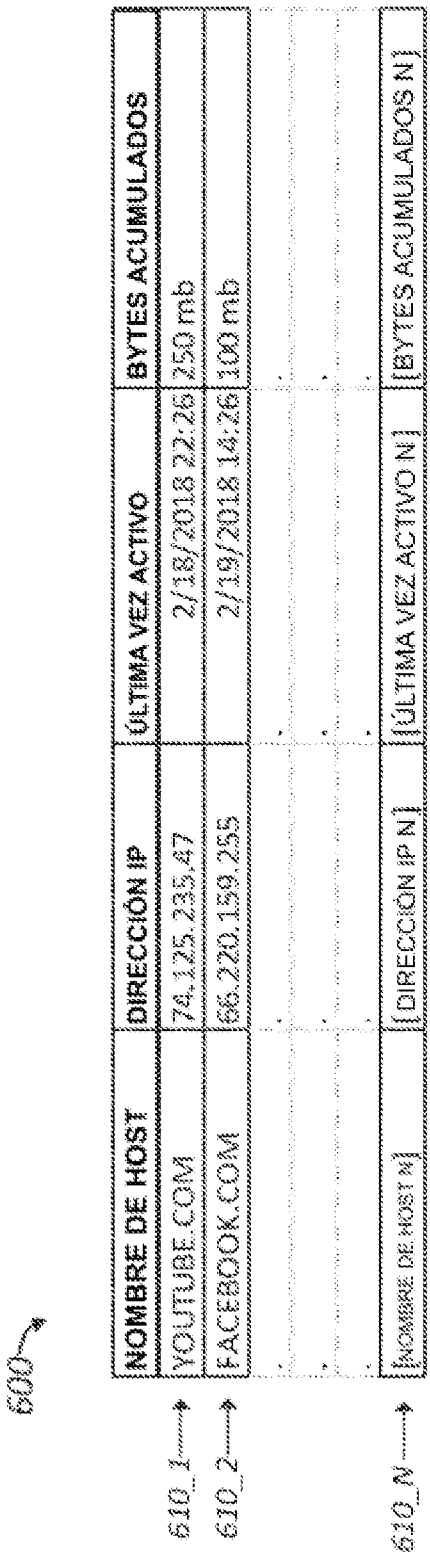
600
610_1
610_2
610_N
NOMBRE DE HOST
DIRECCIÓN IP
ÚLTIMA VEZ ACTIVO
BYTES ACUMULADOS
YOUTUBE.COM
74.125.235.47
2/18/2018 22:26
250 mb
FACEBOOK.COM
66.220.159.255
2/19/2018 14:26
100 mb
[NOMBRE DE HOST N]
[DIRECCIÓN IP N]
[ÚLTIMA VEZ ACTIVO N]
[BYTES ACUMULADOS N]

Fig. 6

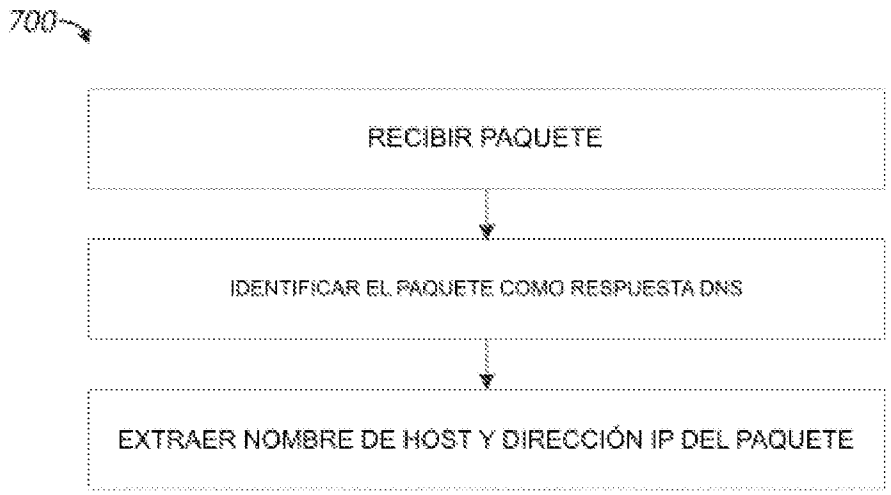
700
RECIBIR PAQUETE
IDENTIFICAR EL PAQUETE COMO RESPUESTA DNS
EXTRAER NOMBRE DE HOST Y DIRECCIÓN IP DEL PAQUETE

Fig. 7

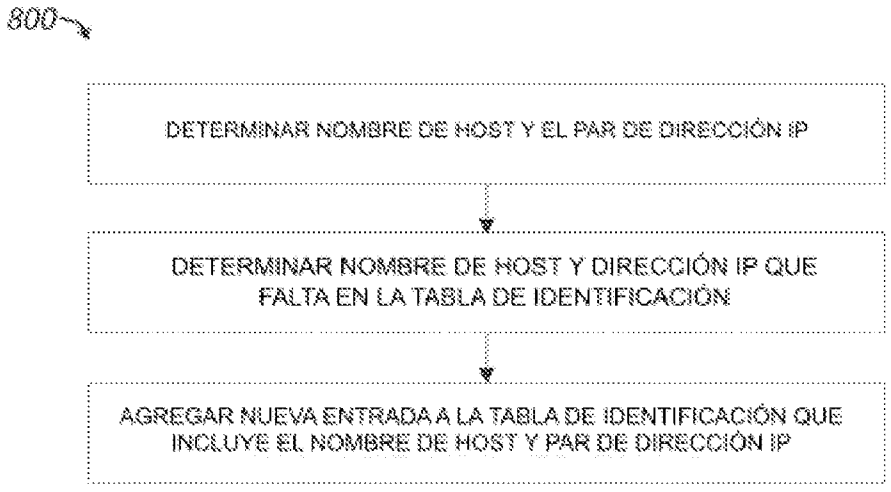
800
DETERMINAR NOMBRE DE HOST Y EL PAR DE DIRECCIÓN IP
DETERMINAR NOMBRE DE HOST Y DIRECCIÓN IP QUE FALTA EN LA TABLA DE IDENTIFICACIÓN
AGREGAR NUEVA ENTRADA A LA TABLA DE IDENTIFICACIÓN QUE INCLUYE EL NOMBRE DE HOST Y PAR DE DIRECCIÓN IP

Fig. 8

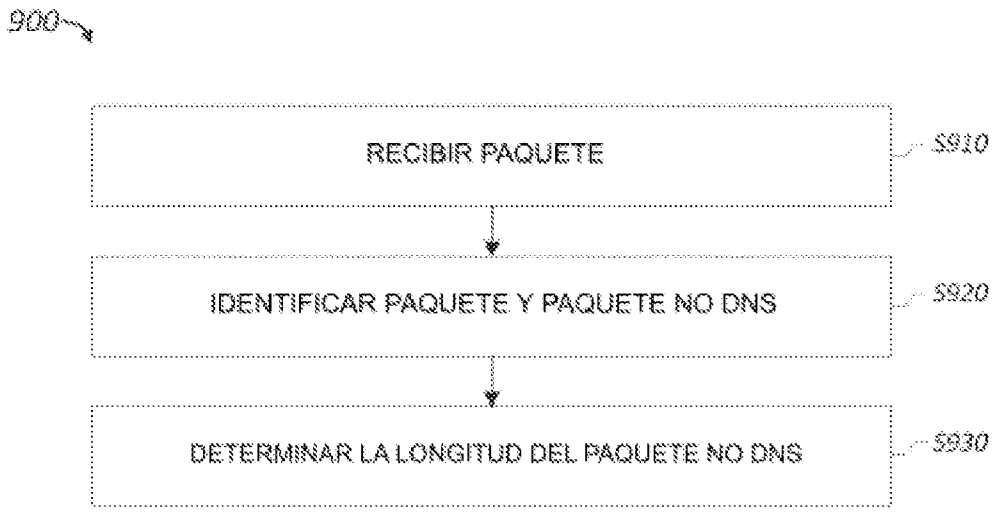
900
RECIBIR PAQUETE
S910
IDENTIFICAR PAQUETE Y PAQUETE NO DNS
S920
DETERMINAR LA LONGITUD DEL PAQUETE NO DNS
S930

Fig. 9

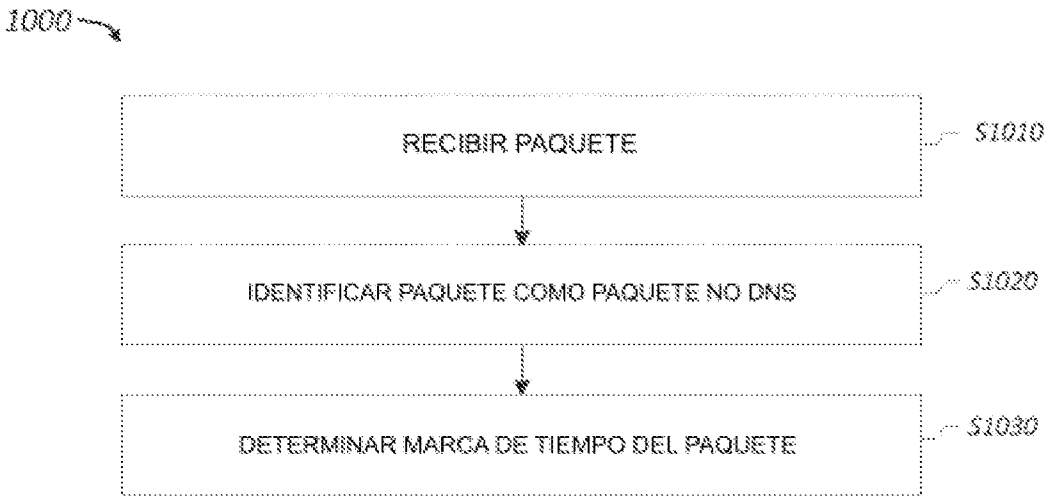
1000
RECIBIR PAQUETE
S1010
IDENTIFICAR PAQUETE COMO PAQUETE NO DNS
S1020
DETERMINAR MARCA DE TIEMPO DEL PAQUETE
S1030

Fig. 10

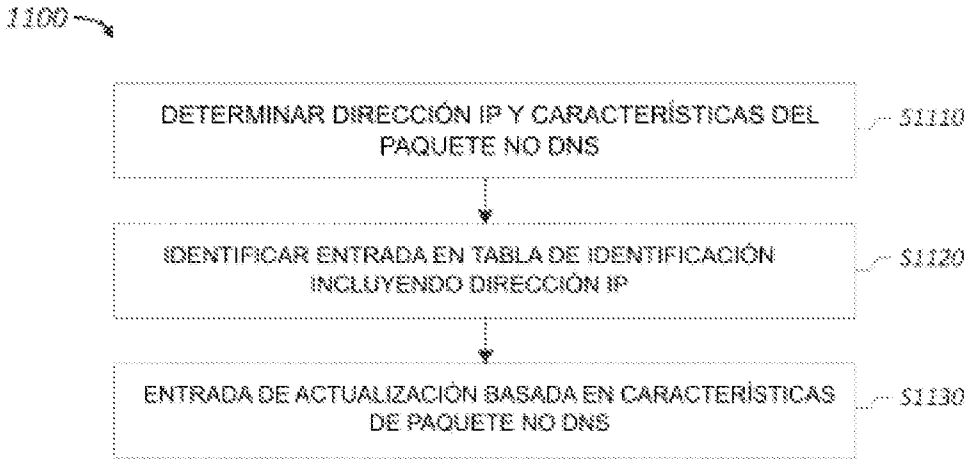
1100
DETERMINAR DIRECCIÓN IP Y CARACTERÍSTICAS DEL PAQUETE NO DNS
S1110
IDENTIFICAR ENTRADA EN TABLA DE IDENTIFICACIÓN INCLUYENDO DIRECCIÓN IP
S1120
ENTRADA DE ACTUALIZACIÓN BASADA EN CARACTERÍSTICAS DE PAQUETE NO DNS
S1130

Fig. 11

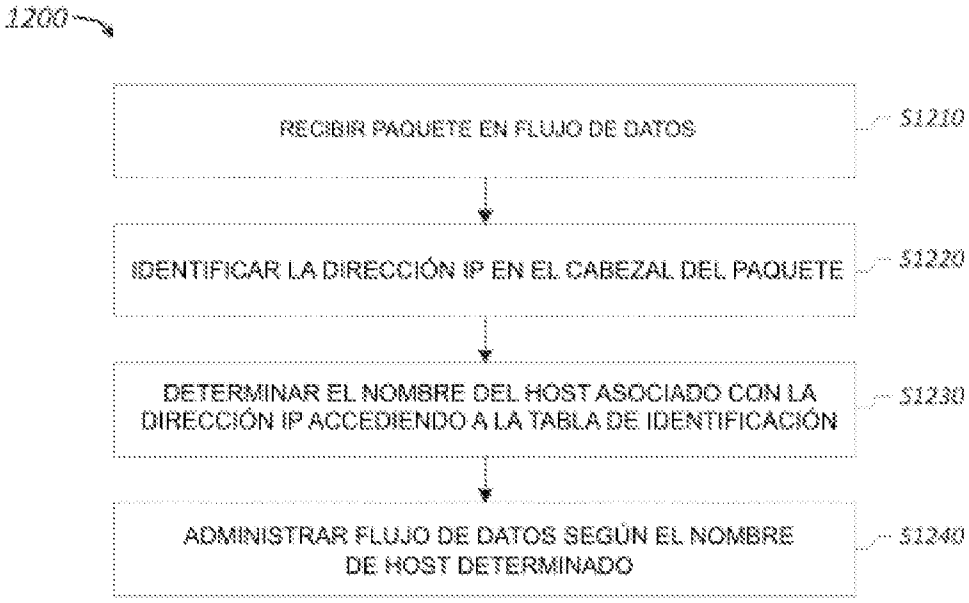
1200
RECIBIR PAQUETE EN FLUJO DE DATOS
S1210
IDENTIFICAR LA DIRECCIÓN IP EN EL CABEZAL DEL PAQUETE
S1220
DETERMINAR EL NOMBRE DEL HOST ASOCIADO CON LA DIRECCIÓN IP ACCEDIENDO A LA TABLA DE IDENTIFICACIÓN
S1230
ADMINISTRAR FLUJO DE DATOS SEGÚN EL NOMBRE DE HOST DETERMINADO
S1240

Fig. 12


1300
RECIBIR PAQUETE EN FLUJO DE DATOS
S1310
IDENTIFICAR LA DIRECCIÓN IP EN EL CABEZAL DEL PAQUETE
S1320
DETERMINAR EL NOMBRE DEL HOST ASOCIADO CON LA DIRECCIÓN IP ACCEDIENDO A LA TABLA DE IDENTIFICACIÓN
S1330
DETERMINAR QUE EL FLUJO DE DATOS ES FLUJO DE ELEFANTE BASADO EN EL NOMBRE DEL HOST
S1340
RITMO DEL FLUJO DEL ELEFANTE
S1350

Fig. 13

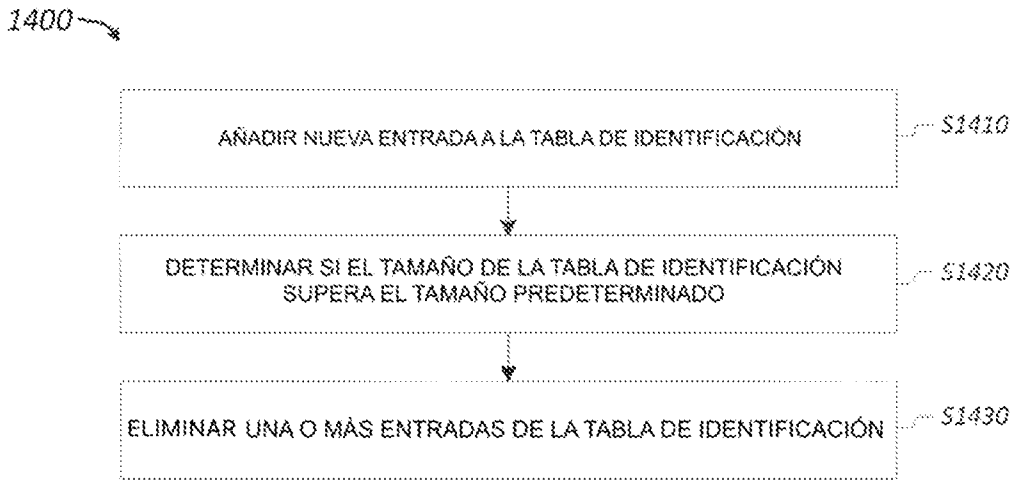
1400
AÑADIR NUEVA ENTRADA A LA TABLA DE IDENTIFICACIÓN
S1410
DETERMINAR SI EL TAMAÑO DE LA TABLA DE IDENTIFICACIÓN SUPERA EL TAMAÑO PREDETERMINADO
S1420
ELIMINAR UNA O MÁS ENTRADAS DE LA TABLA DE IDENTIFICACIÓN
S1430

Fig. 14

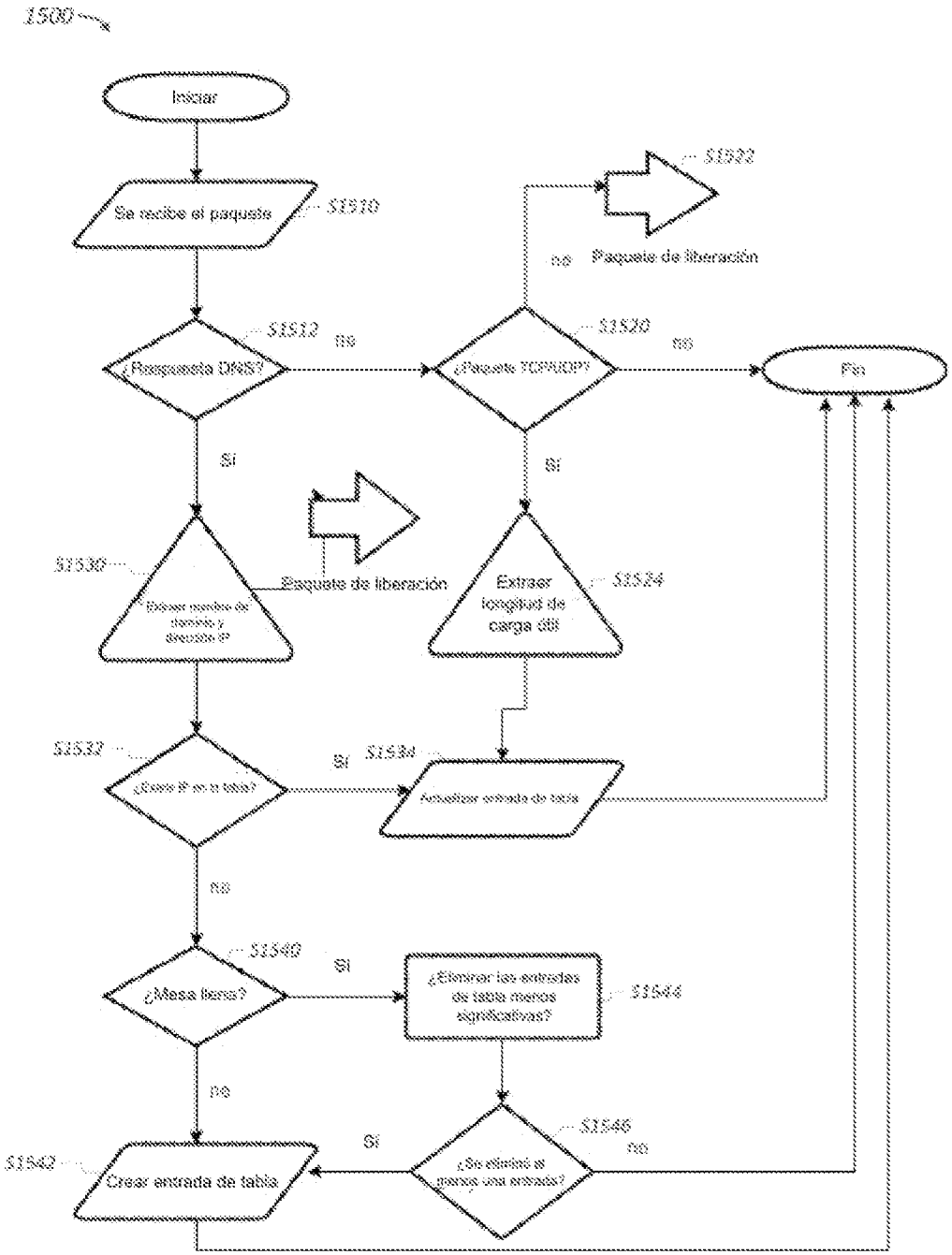
1500
Iniciar
Se recibe el paquete
S1510
S1512
¿Paquete DNS?
no
S1520
¿Paquete TCP/UDP?
no
Fin
S1522
Paquete de liberación
no
Sí
Sí
S1530
Paquete de liberación
Extraer longitud de carga útil
S1524
S1532
Sí
S1534
Actualizar entrada de tabla
no
S1540
¿Mesa llena?
Sí
¿Eliminar las entradas de tabla menos significativas?
S1544
no
S1546
Sí
no
S1542
Crear entrada de tabla

Fig. 15