(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 746 044**

(51) Int. CI.:

H04L 29/10 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.08.2011 PCT/CN2011/079006**

(87) Fecha y número de publicación internacional: **01.03.2012 WO12025063**

(96) Fecha de presentación y número de la solicitud europea: **26.08.2011 E 11819438 (0)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2019 EP 2569922**

(54) Título: **Protocolo de optimización de estratos cruzados**

(30) Prioridad:

24.08.2011 US 201113216808
26.08.2010 US 377352 P
26.08.2010 US 377361 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2020

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

LEE, YOUNG y
XIA, YANGSONG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Protocolo de optimización de estratos cruzados

ANTECEDENTES DE LA INVENCIÓN

Las portadoras de red, también referidas, a veces, como operadores de telecomunicaciones o proveedores de servicios de comunicaciones, que ejecutan redes existentes, desean optimizar la utilización de la red para el tráfico de paso, tal como el tráfico del Protocolo Internet (IP), a través de una red física, p.ej., a través de capas de red 1 a 5. El tráfico optimizado puede incluir tráfico para servicios de triple ejecución (p.ej., vídeo, voz y/o datos) y cualquier tipo de datos masivos. En redes existentes, los servicios de extremo a extremo generalmente se configuran mediante Sistemas de Soporte Operativo (OSS) o aplicaciones de servicios de gestión de red específica del proveedor. Los operadores de red han sugerido dos escenarios operativos diferentes para optimizar la utilización y el tráfico de la red: optimizar los servicios de red existentes y habilitar servicios de aplicación de red nuevos/emergentes.

El documento WO 02/11459 A1 describe una pasarela de Parlay que incluye un bus CORBA, una capa interna de APIs de Parlay, una capa externa de la interfaz de servicio de red para controlar los recursos de red, una interfaz de aplicación y unas APIs de Parlay que están situadas en plataformas distantes que, además, alojan aplicaciones que desean acceder a los recursos de la red.

SUMARIO DE LA INVENCIÓN

En una forma de realización, la presente invención incluye un aparato que comprende una pasarela (ACG) de optimización de estratos cruzados de aplicación (CSO) acoplada a una capa de aplicación que gestiona una pluralidad de servidores, una pasarela CSO de red (NCG) acoplada a una capa de red que gestiona una pluralidad de nodos de red y está configurada para comunicarse con la ACG utilizando un protocolo CSO (CSOP), y una interfaz CSO establecida entre la ACG y la NCG; en donde la ACG (314) está configurada para comunicarse con la NCG (324) por intermedio de la interfaz CSO y para proporcionar información de recurso de la aplicación y limitaciones de acceso a entidades externas en la capa de red (120, 220, 320, 420); en donde la NCG (324) está configurada para comunicarse con la ACG (314) por intermedio de la interfaz CSO, y para proporcionar información de recurso de red y limitaciones de acceso a las entidades de capa de aplicación; en donde se intercambia una pluralidad de mensajes CSOP por intermedio de la interfaz CSO entre la ACG y la NCG para la asignación, el aprovisionamiento y la optimización de recursos de la red de aplicación común.

En otra forma de realización, la idea inventiva incluye un componente de red que comprende un receptor configurado para recibir un primer mensaje CSOP por intermedio de una interfaz CSO establecida entre una capa de aplicación y una capa de red, y un controlador de plano configurado para habilitar CSO entre la capa de aplicación y la capa de red mediante el procesamiento del primer mensaje CSOP para asignar, aprovisionar u optimizar el recurso de red de aplicación común, y un transmisor configurado para enviar un segundo mensaje CSOP por intermedio de la interfaz CSO en respuesta al primer mensaje CSOP, o para la finalidad de CSO; en donde el primer mensaje CSOP y el segundo mensaje CSOP proporcionan mecanismos de abstracción y resumen para garantizar el intercambio de información necesaria para conseguir la CSO mientras se evita el intercambio de información privada o segura, que no está autorizada a otras entidades, redes y/o estratos.

Estas y otras características se entenderán más claramente a partir de la siguiente descripción detallada tomada en conjunción con los dibujos y reivindicaciones adjuntos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para un entendimiento más completo de esta descripción, se hace referencia ahora a la siguiente breve descripción, tomada en relación con los dibujos adjuntos y la descripción detallada, en donde los números de referencia similares representan partes similares.

La Figura 1 es un diagrama esquemático de una forma de realización de una arquitectura CSO.

La Figura 2 es un diagrama esquemático de otra forma de realización de una arquitectura CSO.

La Figura 3 es un diagrama esquemático de otra forma de realización de una arquitectura CSO.

La Figura 4 es un diagrama esquemático de un sistema CSOP.

La Figura 5 es un diagrama esquemático de una forma de realización de una cabecera de mensaje CSOP.

La Figura 6 es un diagrama esquemático de una forma de realización de un objeto de perfil de autenticación.

La Figura 7 es un diagrama esquemático de una forma de realización de un objeto de perfil de servicio.

La Figura 8 es un diagrama esquemático de una forma de realización de un objeto de perfil de rendimiento.

La Figura 9 es un diagrama esquemático de una forma de realización de un objeto de perfil de ancho de banda.

La Figura 10 es un diagrama esquemático de una forma de realización de un objeto de perfil de modo de conectividad.

La Figura 11 es un diagrama esquemático de una forma de realización de un objeto de perfil de localización.

La Figura 12 es un diagrama esquemático de una forma de realización de un Tipo/Longitud/Valor (TLV) opcional.

La Figura 13 es un diagrama esquemático de otra forma de realización de un TLV opcional.

La Figura 14 es un diagrama esquemático de una forma de realización de un objeto de perfil de protección.

La Figura 15 es un diagrama esquemático de otra forma de realización de un TLV opcional.

La Figura 16 es un diagrama esquemático de una forma de realización de un objeto de ruta.

La Figura 17 es un diagrama esquemático de otra forma de realización de un TLV opcional.

La Figura 18 es un diagrama esquemático de otra forma de realización de un TLV opcional.

La Figura 19 es un diagrama esquemático de otra forma de realización de un TLV opcional.

La Figura 20 es un diagrama esquemático de una forma de realización de un objeto de topología de red virtual (VNT).

La Figura 21 es un diagrama esquemático de otra forma de realización de un TLV opcional.

La Figura 22 es un diagrama esquemático de otra forma de realización de un TLV opcional.

La Figura 23 es un diagrama de protocolo de una forma de realización de un intercambio de mensajes CSOP.

La Figura 24 es un diagrama esquemático de una forma de realización de una unidad de red.

La Figura 25 es un diagrama esquemático de una forma de realización de un sistema informático de finalidad general.

DESCRIPCIÓN DETALLADA

Ha de entenderse desde el principio que, aunque a continuación se da a conocer una puesta en práctica ilustrativa de una o más formas de realización, los sistemas y/o métodos descritos se pueden realizar utilizando cualquier número de técnicas, ya sean actualmente conocidas o existentes. La presente invención no debe limitarse, en modo alguno, a las puestas en práctica ilustrativas, dibujos y técnicas ilustradas a continuación, incluidos los diseños y realizaciones que se ilustran y describen aquí a modo de ejemplo, sino que puede modificarse dentro del alcance de las reivindicaciones adjuntas junto con el alcance completo de sus equivalentes.

El suministro y funcionamiento de aplicaciones nuevas/emergentes puede implicar la resolución del problema de selección de servidor (SS) en el estrato de la aplicación, así como el aprovisionamiento de la red en el estrato de red subyacente. El estrato de aplicación puede incluir las aplicaciones y servicios, que se ponen en práctica, o se ejecutan, sobre la aplicación y la capa de red, y el estrato de red puede incluir el transporte, la red, el enlace y las capas físicas o combinaciones de los mismos. La gestión y la coordinación del aprovisionamiento de servicios, tanto en el estrato de aplicación como en el estrato de red, es diferente de la gestión de servicios tradicionales, tales como el aprovisionamiento de red de servicios de telecomunicaciones de extremo a extremo.

La CSO puede habilitar nuevos servicios, p.ej., utilizando la optimización multi-dominio y/o multi-dispositivo. Los nuevos servicios pueden incluir sistemas de distribución de ficheros, servicios de transmisión de vídeo, servicios de vídeoconferencia y servicios informáticos en malla. Estos servicios pueden utilizar tanto dispositivos móviles como dispositivos fijos. Los sistemas y servicios de distribución de ficheros comenzaron acelerando la descarga de páginas web, tales como aquellas que contienen imágenes y, a continuación, se expandieron para incluir la entrega de ficheros de software, audio y vídeo. Los servicios de transmisión pueden separarse en dos tipos, servicios en directo y bajo demanda. Se pueden crear, además, múltiples variantes entre estos dos tipos cuando la funcionalidad de pausa o reproducción se incluye en un servicio de transmisión en directo. La transmisión en directo puede ser el

caso en el que el cliente está dispuesto a recibir la transmisión en su punto de reproducción actual en lugar de en algún punto de inicio previamente existente. Los servicios bajo demanda pueden producir desafíos técnicos adicionales. Es posible que los proveedores de servicios deseen evitar retardos prolongados en el inicio del servicio con el fin de retener a los clientes mientras que, al mismo tiempo, las demandas conjuntas de lotes economizan los costes de servidores. La vídeoconferencia se mueve desde el escenario operativo de distribución de contenido de transmisión en directo de punto a multipunto a una situación de multipunto a multipunto. Además, puede haber una restricción adicional de Calidad de Servicio (QoS) en la latencia. Servicios informáticos en malla pueden tener requisitos para una transferencia considerablemente grande de ficheros con separación reducida y mayores tamaños de ficheros.

Un problema en las interacciones entre el estrato de aplicación y el estrato de red es la falta de una interfaz estándar abierta que permita una señalización proxy entre los estratos de aplicación y red. Esto puede limitar el intercambio de información entre estratos cruzados, el mecanismo de realimentación entre estratos y la asignación y reconfiguración de recursos integrados/sincronizados. Esta falta de coordinación entre los estratos de aplicación y red puede aumentar el potencial de desperdicio de recursos, lo que puede traducirse en un mayor costo tanto para la aplicación como para las operaciones de la red.

En el presente documento se describe un sistema y métodos para proporcionar una especificación de protocolo para el soporte de CSO, al que se hace referencia en este documento como CSOP. La CSO puede implicar la optimización integrada de la aplicación y los recursos de red al proporcionar una interfaz para las interacciones e intercambios entre los dos estratos. La CSO puede incluir, además, la coordinación de la aplicación y los recursos de red. La CSO se puede lograr independientemente de cualquier optimización posible para aplicaciones o servicios existentes que se ejecutan en una red.

Algunos de los términos utilizados y descritos a continuación, con respecto a las características de la CSO, incluyen: ACG, NCG, CSOP y perfil. La ACG puede ser una entidad de CSO en el estrato de aplicación, que es responsable de reunir la carga y la utilización de los recursos de aplicación, tomar decisiones de asignación de recursos e interactuar con la NCG. La NCG puede ser una entidad de CSO en el estrato de red, que es responsable de interactuar con la ACG, con la activación de la función de demanda de servicio para transportar la entidad de red responsable del aprovisionamiento, configuración, estimación/cálculo de ruta y otras funciones de gestión/control de red. El CSOP puede ser un protocolo que se ejecuta en una interfaz entre una ACG y una NCG, tal como se describe más adelante. El perfil puede incluir información que describe el requisito de servicio para una aplicación. El perfil se puede generar por una ACG y comunicarse a una NCG a través del CSOP, tal como aquí se describe.

La Figura 1 ilustra formas de realización de una arquitectura CSO 100. La arquitectura CSO 100 puede comprender un estrato de aplicación 110 y un estrato de red 120. El estrato de aplicación 110 puede implicar comunicaciones entre una pluralidad de servidores 112, que pueden estar configurados para poner en práctica, o ejecutar, aplicaciones para usuarios finales o clientes (no ilustrados). El estrato de red 120 puede implicar comunicaciones entre una pluralidad de nodos de red 122, tales como puentes, enrutadores y/o conmutadores, para el reenvío de datos, por ejemplo, paquetes, asociados con las aplicaciones. Los servidores 112 pueden estar situados en un centro de datos y los nodos de red 122 pueden estar ubicados en una red acoplada al centro de datos. Los servidores 112 se pueden comunicar con los nodos de red 122 para permitir el servicio de aplicaciones del usuario y el reenvío o transporte de los datos asociados. La CSO se puede poner en práctica para optimizar las diferentes operaciones de los servidores 112 y los nodos de red 122. Los servidores 112 pueden estar situados en el mismo centro de datos, o un subconjunto de servidores 112 puede situarse en múltiples centros de datos.

En una forma de realización, los centros de datos utilizados para proporcionar servicios de aplicación, tales como los denominados servicios informáticos en la nube, y otros servicios en la nube, en el estrato de aplicación 110 a los usuarios finales, se pueden distribuir geográficamente alrededor del estrato de red 120. Por lo tanto, numerosas decisiones sobre el control y la gestión de servicios de aplicaciones, tales como dónde realizar la instanciación de otra instancia de servicio, o a qué centro de datos se asigna un nuevo cliente, pueden tener un impacto significativo en el estado de la red. Las capacidades y el estado de la red pueden tener, además, un impacto en el rendimiento de la aplicación.

Actualmente, las decisiones de aplicación se pueden tomar con poca, o ninguna, información referente a la red subyacente que se utiliza para proporcionar dichos servicios. En consecuencia, tales decisiones pueden ser sub-óptimas a partir tanto de la aplicación y la utilización de los recursos de red como desde el logro de los objetivos de QoS. La CSO puede proporcionar un método y un sistema para coordinar la asignación de recursos entre el estrato de aplicación 110 y el estrato de red 120, p.ej., en el contexto de servicios informáticos en la nube y las redes de centros de datos. A modo de ejemplo, los objetivos de la CSO pueden admitir la consulta del estrato de red 110 desde la aplicación, el aprovisionamiento conjunto entre la aplicación y la red, y/o la reasignación conjunta de recursos, en caso de anomalía, tanto en la aplicación como en la red. Los objetivos de las CSO pueden proporcionar, además, una red con reconocimiento de aplicaciones, aplicación con reconocimiento de red y capacidad de equilibrio de carga global. Algunos de los objetivos para optimizar las operaciones y/o interacciones entre el estrato de aplicación 110 y el estrato de red 120, p.ej., entre los servidores 112 y los nodos de red 122, pueden incluir la mejora de las capacidades de red, la topología, el aprovisionamiento, la supervisión de uso, la

supervisión de fallos, o combinaciones de los mismos. Por ejemplo, los objetivos de CSO 100 pueden mejorar el intercambio de una, o ambas, capacidades de red o información de demanda/recurso de aplicación, información relacionada con la topología y/o ingeniería de tráfico entre las capas (virtualización/abstracción), o ambas. Los objetivos de las CSO pueden mejorar, además, el inicio del servicio de instanciación de la aplicación a la red con intercambio de perfil (aprovisionamiento), intercambio de información de congestión/fallo de la red/aplicación (supervisión), o ambos.

La Figura 2 ilustra otra forma de realización de una arquitectura CSO 200 que puede comprender un estrato de aplicación 210 y un estrato de red 220. El estrato de aplicación 210 puede gestionar comunicaciones entre una pluralidad de servidores 212, y el estrato de red 220 puede gestionar comunicaciones entre una pluralidad de nodos de red 222, que pueden ser prácticamente similares a los servidores 112 y los nodos de red 122, respectivamente. La arquitectura CSO 200 puede incluir, además, una interfaz de CSO que permite mejores interacciones y/o comunicaciones entre los servidores 112 y/u otros componentes (no ilustrados) del estrato de aplicación 210, y los nodos de red 122 y/u otros componentes (no ilustrados) del estrato de red 220. La interfaz CSO puede ser una interfaz abierta entre los dos estratos y puede habilitar las características de CSO utilizando el CSOP, tal como se describe a continuación. En el estrato de aplicación 210, la interfaz abierta puede permitir una identificación de cliente/consumidor de algún tipo, p.ej., dirección IP, tipos de servidor e identificación, flujos de datos de aplicación y requisitos de QoS que pueden ser de naturaleza estadística y variar con el tiempo, y/o carga de servidor y condiciones de fallo operativo. En el estrato de red 220, la interfaz abierta puede permitir, además, el intercambio de topología de red, ubicaciones de cliente y servidor dentro de esa topología, capacidades de red y capacidades con respecto a QoS, ancho de banda, información de latencia y/u otras características relacionadas con la red, carga de red y condiciones de fallo operativo, o combinaciones de los mismos.

La Figura 3 ilustra otra forma de realización de una arquitectura CSO 300 que puede incluir un estrato de aplicación 310 y un estrato de red 320. El estrato de aplicación 310 puede incluir interacciones entre una pluralidad de servidores 312, y el estrato de red 320 puede incluir interacciones entre una pluralidad de nodos de red 322, que pueden ser prácticamente similares a los servidores 112 y los nodos de red 122, respectivamente. La arquitectura CSO 300 puede comprender, además, una interfaz CSO que puede establecerse entre una ACG 314 en el estrato de aplicación 310, y una NCG 324 en el estrato de red 320.

La ACG 314 se puede configurar para acceder a datos y procesos relacionados con la aplicación en el estrato de aplicación 310, comunicarse con la NCG 324, por intermedio de la interfaz CSO, y proporcionar información de recursos de la aplicación y limitaciones de acceso a entidades externas en las entidades de estrato de red 320. La NCG 324 puede configurarse para acceder a datos relacionados con la red (en el estrato de red 320), comunicarse con la ACG 314 por intermedio de la interfaz CSO, comunicarse con procesos de red tales como control de admisión, reserva de recursos y/o procesamiento de conexión, y proporcionar información de recurso de red y limitaciones de acceso a entidades del estrato de aplicación 310. Además, la ACG 314 y la NCG 324 se pueden comunicar con los servidores 312 y los nodos de red 322, respectivamente. La interfaz CSO entre la ACG 314 y la NCG 324 puede admitir el uso del CSOP para habilitar las diferentes funcionalidades de la ACG 314 y la NCG 324 anteriores, y las comunicaciones relacionadas, p.ej., señalización, mensajería e intercambio de información.

La Figura 4 ilustra una forma de realización de un sistema CSOP 400, que puede ponerse en práctica utilizando la interfaz CSO entre una ACG y una NCG, a modo de ejemplo, en las arquitecturas CSO anteriores. Se puede enviar un perfil de usuario desde un usuario o plano de usuario 401 a un estrato de aplicación 410. El perfil de usuario puede definir características del usuario y puede comprender un identificador de usuario, un identificador de dispositivo de usuario, información de códec de dispositivo de usuario, si es aplicable, preferencia de usuario si está disponible, capacidad de usuario o combinaciones de los mismos. El identificador de usuario puede ser un identificador de usuario único (ID), tal como un ID virtual. El identificador del dispositivo del usuario puede corresponder a la dirección, p.ej., dirección de IP y/o de Control de Acceso al Soporte (MAC), para cada dispositivo de usuario. Puede haber múltiples dispositivos de usuario dependiendo de la localización del usuario. La preferencia del usuario puede conocerse, a priori, tal como una localización preferida del servidor para el usuario. La capacidad del usuario puede incluir el ancho de banda máximo que el dispositivo del usuario puede gestionar, a modo de ejemplo, para enlace ascendente y/o enlace descendente.

El estrato de aplicación 410 puede reenviar, a continuación, el perfil de usuario, p.ej., después del procesamiento, a un estrato de red 420. De forma adicional o como alternativa, el estrato de aplicación 410 puede reenviar un perfil de aplicación a un estrato de red 420. El perfil de aplicación se puede obtener sobre la base del perfil de usuario y puede definir características de la aplicación para el usuario. El perfil de la aplicación puede incluir al menos uno de entre un perfil de seguridad, un perfil de localización, un perfil de QoS, un perfil de conectividad, un perfil de direccionalidad, un perfil de ancho de banda, un perfil de duración del servicio y un perfil de restablecimiento.

El perfil de seguridad puede incluir una red privada virtual de extremo a extremo dedicada (VPN), tal como la asignación de recursos y la asignación de recursos físicos dedicados. El perfil de localización puede indicar ubicaciones tanto de los clientes como de las fuentes. El perfil de QoS puede comprender un límite de tolerancia de retardo, un límite de tolerancia de fluctuación de fase, tolerancia de relación de entrega de paquetes, disponibilidad de red y/u otra información relacionada con QoS. El perfil de conectividad puede indicar una conectividad de punto a

punto (P-P), de punto a multipunto (P-MP), de multipunto a multipunto (MP-MP), y/o cualquier otra conectividad o sistema de transmisión. El perfil de direccionalidad puede indicar una comunicación unidireccional o una comunicación bidireccional. El perfil de ancho de banda puede indicar los requisitos de ancho de banda máximo, medio y/o mínimo para la conectividad, la tasa de ráfaga máxima, la duración máxima de la ráfaga y/u otra información relacionada con el ancho de banda. La duración del perfil de servicio puede indicar un tiempo de servicio de la aplicación, p.ej., una vez que se configura. El perfil de restablecimiento puede indicar que se requiere un redireccionamiento, no es requerido un redireccionamiento y/u otra información relacionada con el restablecimiento de la conectividad.

Dependiendo de la aplicación, su naturaleza y la calidad de servicio relacionada, el estrato de red subyacente 420 puede tener diferentes capacidades. El estrato de red 420 puede reenviar su información de capacidad de red al estrato de aplicación 410, por ejemplo, en respuesta a la recepción de una demanda y/o el perfil de aplicación. La capacidad de red puede incluir capacidades de ancho de banda, QoS y acuerdo de nivel de servicio (SLA), configurabilidad y adaptabilidad. Las capacidades de ancho de banda pueden indicar la capacidad de la red para cumplir con los requisitos del perfil de ancho de banda del servicio de aplicación. La QoS y el SLA pueden indicar la capacidad de la red para realizar la entrega, de conformidad con los requisitos del perfil de QoS y los SLAs correspondientes. La capacidad de configuración puede indicar la capacidad para reconfigurar/volver a optimizar varios aspectos de la red y los momentos en que se pueden producir cambios. La información de adaptabilidad puede indicar la capacidad de adaptar cambios debido a cambios en la demanda del servicio, o la congestión/fallo de la aplicación/red.

Aunque la Figura 4 ilustra un sistema de CSOP 400 en donde se envía un perfil de usuario a un estrato de aplicación, no todas las formas de realización incluyen la etapa de información de perfil de usuario. A modo de ejemplo, puesto que algunas aplicaciones (p.ej., copia de seguridad de almacenamiento) no requieren información de perfil de usuario, el sistema de CSOP para dichas aplicaciones es estrictamente entre un centro de datos a otro (o varios centros de datos, dependiendo del número de copias de seguridad).

Las comunicaciones de CSOP, en cualquiera de las arquitecturas o sistemas anteriores, pueden comprender comunicaciones verticales entre el plano de usuario y el estrato de aplicación, y comunicaciones verticales entre el estrato de aplicación y el estrato de red. La funcionalidad de CSOP puede incluir estimación de ruta, reserva de ruta, consulta de topología de red/topología de máquina virtual (VMT), supervisión/notificación y/u otras funciones que se describen a continuación. El CSOP puede operar a través de un protocolo de control de transmisión (TCP), p.ej., utilizando puertos TCP registrados que pueden tener determinados números de puerto. Sin embargo, el funcionamiento de CSOP no está limitado a TCP, sino que se puede poner en práctica utilizando otros protocolos, tales como, a modo de ejemplo, OpenFlow. En consecuencia, todos los mensajes de CSOP pueden enviarse a través de los puertos TCP registrados. El CSOP puede proporcionar, además, medios para garantizar el intercambio de información necesaria para lograr la CSO al tiempo que evita el intercambio de información privada o segura, que puede no estar autorizada para otras entidades, redes y/o estratos. El CSOP puede proporcionar los mecanismos de abstracción y resumen con el fin de evitar revelar detalles innecesarios (p.ej., entre la capa/estrato de aplicación y la capa/estrato de red) y para proporcionar, además, una escalabilidad mejorada. Los mecanismos de abstracción y resumen se pueden proporcionar utilizando formatos de mensajes CSOP, tal como se describe, en detalle, a continuación.

Los mensajes de CSOP pueden incluir un mensaje de Inicialización, un mensaje de mantenimiento activo (KeepAlive), un mensaje de Demanda, un mensaje de Respuesta, un mensaje de Liberación, un mensaje de Configuración de Liberación (ReleaseConf), un mensaje de Notificación, un mensaje de error de CSOP (CSOPErr), un mensaje de sesión de CSOP (CLOSE) o combinaciones de los mismos. El masaje de Inicialización se puede utilizar para iniciar una sesión de CSOP con un procedimiento de autenticación entre una ACG y una NCG. El mensaje de KeepAlive se puede utilizar para mantener una sesión de CSOP. El mensaje de Demanda se puede utilizar para solicitar una configuración de ruta desde una ACG a una NCG, una estimación de ruta con, o sin, compromiso de reserva/asignación real desde una ACG a una NCG, y una topología de red virtual procedente de una ACG a una NCG. El mensaje de Respuesta se puede utilizar en respuesta a un mensaje de Demanda de una NCG a una ACG. El mensaje de Liberación se puede utilizar para solicitar la liberación de cualquier ruta existente. Se envía desde una ACG a una NCG. El mensaje de configuración de liberación ReleaseConf se puede utilizar en respuesta a un mensaje de liberación Release para confirmar la liberación de cualquier ruta existente. El mensaje ReleaseConf se puede enviar desde una NCG a una ACG. El mensaje de notificación Notify se puede utilizar para notificar cualquier evento específico. El mensaje de notificación se puede enviar por una ACG a una NCG, o enviarse por una NCG a una ACG. Cuando una NCG envía a una ACG, el mensaje de notificación se puede utilizar con una finalidad de supervisión para los servicios de transporte existentes. El mensaje de error de CSOP CSOPErr puede usarse para indicar cualquier condición de error de protocolo asociada con CSOP. El mensaje de sesión de CSOP CLOSE se puede utilizar para terminar una sesión CSOP.

La Figura 5 ilustra una forma de realización de una cabecera de mensaje CSOP 500, que puede incluirse en los mensajes CSOP intercambiados. El mensaje de CSOP puede comprender la cabecera de CSOP 500 seguida de un cuerpo de longitud variable, que puede incluir un conjunto de objetos que pueden ser obligatorios u opcionales, tal como se describe más adelante. La cabecera de mensaje de CSOP 500 puede comprender un campo de versión 502, un campo reservado 504, un campo de tipo de mensaje 506 y un campo de longitud de mensaje 508. El campo

de versión 502 puede incluir, aproximadamente, 3 bits e indicar un número de versión de CSOP. La versión actual puede ser la versión 1. El campo reservado 504 puede comprender aproximadamente 5 bits, que se pueden establecer a cero y no pueden utilizarse, p.ej., reservados para uso futuro. El campo de tipo de mensaje 506 puede incluir, aproximadamente, 8 bits, e indicar uno de los siguientes tipos de mensaje definidos utilizando el valor correspondiente, como sigue:

Valor	Tipo de mensaje
1	Inicializar
2	Mantenimiento activo
3	Demanda
4	Respuesta
5	Liberación
6	ReleaseConf
7	Notificar
8	Error
9	Sesión

El campo de longitud de mensaje 508 puede comprender aproximadamente 16 bits e indicar la longitud total del mensaje de CSOP que incluye la cabecera del mensaje de CSOP 500, p.ej., en bytes.

A modo de ejemplo, la cabecera del mensaje de CSOP 500 puede ser parte de un mensaje de Demanda de CSOP enviado desde una ACG a una NCG, y ser parte de un mensaje de Respuesta de CSOP enviado, en respuesta, desde la NCG a la ACG. El mensaje de Demanda puede tener el siguiente formato:

<Mensaje de Demanda>::=<Cabecera común>

<Perfil de autenticación>

<Perfil de servicio>

[<Perfil PerformACG>]

[<Perfil de ancho de banda>]

<Perfil de modo de conectividad>

<Perfil de localización>

[<Perfil de protección>].

El mensaje de Respuesta puede tener el siguiente formato:

<Mensaje de respuesta>::=<Cabecera común>

<Perfil de autenticación>

<Ruta>

<VNT>

El mensaje de respuesta puede incluir cualquiera de <Ruta> o <VNT> dependiendo de la demanda de servicio original en el mensaje de Demanda. Los mensajes de CSOP también pueden incluir, además, un conjunto o perfiles definidos en el marco de CSO, que pueden ser entendidos por las capas/redes de transporte para proporcionar una demanda de servicio pertinente procedente de la ACG. Los objetos CSO en el mensaje de CSOP se pueden utilizar para transmitir información de perfil.

La Figura 6 ilustra una forma de realización de un objeto de perfil de autenticación 612, que puede incluirse en un mensaje de CSOP 600. La información de perfil de autenticación, en el objeto de perfil de autenticación 612, se puede proporcionar para garantizar intercambios de mensajes entre una ACG y una NCG, o entre una NCG y otra NCG (p.ej., en otro dominio). El mensaje de CSOP 600 puede comprender un campo de versión 602, un campo

reservado 604, un campo de tipo de mensaje 606 y un campo de longitud de mensaje 608, p.ej., en una cabecera de mensaje de CSOP, que puede estar configurada de forma prácticamente similar a los correspondientes componentes de la cabecera del mensaje de CSOP 500. El mensaje CSOP 600 puede comprender, además, uno o más objetos distintos 610 además del objeto de perfil de autenticación 612, tal como cualquiera de los objetos descritos más adelante. El objeto de perfil de autenticación 612 puede ser el último objeto en el mensaje de CSOP 600.

El objeto de perfil de autenticación 612 puede incluir un campo de clase de objeto de autenticación 614, un campo de longitud 616, un campo de sub-tipo 618, un campo reservado 620, un campo de Índice de Parámetro de Seguridad (SPI) 622 y un testigo informático denominado token 624. El campo de clase de objeto de autenticación 614 puede comprender un valor definido que indica que el objeto es un objeto de perfil de autenticación. El campo de longitud 616 puede indicar la longitud del objeto de perfil de autenticación 612, p.ej., en bytes. El campo de sub-tipo 618 puede identificar el modo de autenticación y la entidad homóloga para la autenticación del mensaje (p.ej., ACG-NCG o NCG-NCG, respectivamente). El campo reservado 620 no puede usarse y todos los bits dentro del campo reservado 620 pueden establecerse a cero. El campo SPI 622 puede ser una cantidad de 4 bytes, por ejemplo, en el rango [0-4294967296], en donde el rango [0-255] puede estar reservado. Más concretamente, el SPI puede seleccionar el algoritmo de autenticación y la clave compartida utilizada para calcular el token 624. Con el fin de garantizar la interoperabilidad, una forma de puesta en práctica puede asociar cualquier valor de SPI con cualquier algoritmo de autenticación. Además, todas las realizaciones pueden poner en práctica un algoritmo de autenticación predeterminado, por ejemplo, el Algoritmo 1 de Hash Seguro (SHA1)-Código de Autenticación de Mensaje basado en Hash (HMAC). Están permitidos otros algoritmos.

El token 624 puede incluir la información para autenticar la entidad homóloga. La asociación de seguridad basada en clave compartida entre ACG y NCG, o entre una NCG y otra NCG, puede comprender un SPI, una clave compartida y un algoritmo de autenticación. La clave compartida puede incluir un valor arbitrario y puede tener aproximadamente 20 octetos (bytes) de longitud. La clave compartida puede configurarse de forma manual o mediante negociación dinámica. A modo de ejemplo, el valor del token se puede generar como sigue: Token = Primero (96, HMAC-SHA1 (Clave compartida, Datos del Mensaje)). Los datos del mensaje se pueden generar de la siguiente manera: Datos del mensaje = dirección IP de origen | dirección IP de destino | Cuerpo del mensaje de CSOP. La forma funcional "Primero(tamaño, entrada)" utilizada para generar el valor del token que indica la truncación de los datos de "entrada" de modo que solamente se sigan utilizando los primeros bits de "tamaño". El cuerpo del mensaje de CSOP utilizado para generar el valor del token puede comenzar desde el campo "Ver" hasta el valor de SPI inclusive del objeto de autenticación.

La ACG puede incluir el objeto de perfil de autenticación 612 en un mensaje de Demanda si la ACG tiene una asociación de seguridad basada en clave compartida con la NCG. La NCG puede incluir el objeto de perfil de autenticación 612 en un mensaje de Respuesta si la NCG recibe el objeto de perfil de autenticación 612 en un mensaje de Demanda correspondiente, y si la NCG tiene una asociación de seguridad basada en clave compartida con la ACG. La ACG o NCG que recibe el objeto de perfil de autenticación 612 puede verificar el valor de token en el campo de token 624 del objeto de perfil de autenticación 612. Si falla la autenticación, la NCG puede enviar un mensaje de Respuesta con el Código de Estado CSOP-AUTH-FAIL. Si la NCG no tiene una asociación de seguridad basada en clave compartida con la ACG, la NCG puede rechazar el mensaje de Demanda. La NCG puede, además, registrar tales eventos.

La Figura 7 ilustra una forma de realización de un objeto de perfil de servicio 700 que puede incluirse en un mensaje CSO, p.ej., el mensaje CSO 600. El objeto de perfil de servicio 700 se puede utilizar para indicar una demanda de servicio específico en un mensaje de Demanda. Los siguientes servicios pueden ser definidos por el objeto de perfil de servicio 700:

Reserva de ruta: Esta demanda de servicio puede requerir la reserva de ruta en una red de transporte que garantice el ancho de banda para la conexión.

Modificación de ruta: Esta demanda de servicio se puede utilizar para indicar modificaciones para una ruta existente que se ha reservado.

Estimación de ruta: Esta demanda de servicio se puede utilizar para una estimación de cálculo de ruta en una red de transporte sin compromiso real de reserva/asignación en la red de transporte.

Demanda de VNT: Esta demanda de servicio puede solicitar una topología de red virtual de la red de transporte para un conjunto determinado de orígenes y destinos.

El objeto de perfil de servicio 700 puede comprender un campo de tipo de servicio (S) 702, una pluralidad de indicadores 704, un campo reservado 706 y un número de identificación ID de demanda de servicio 708. El campo S 702 puede comprender, aproximadamente, 8 bits y puede incluir un valor para indicar un tipo de servicio como sigue:

0: Reserva de ruta

1: Modificación de ruta

2: Estimación de ruta

3: Demanda de VNT

4-255: Reservado.

Los indicadores 704 pueden incluir, aproximadamente, 16 bits y pueden definirse para diversos fines. El campo reservado 706 puede comprender aproximadamente 8 bits que se pueden establecer a cero en la transmisión e ignorarse en la recepción. El número de identificación ID de demanda de servicio 708 puede comprender aproximadamente 32 bits y puede incluir un valor que identifica, de forma única, la demanda de servicio. Cada vez que se envía una nueva demanda a una NCG, puede aumentarse el número de ID de demanda de servicio.

La Figura 8 ilustra una forma de realización de un objeto de perfil de rendimiento 800 que puede estar incluido en un mensaje CSO, p.ej., el mensaje CSO 600. El objeto de perfil de rendimiento 800 puede indicar el objetivo de rendimiento deseado asociado con una demanda de reserva. El objeto de perfil de rendimiento 800 puede comprender un campo de límite de retardo unidireccional máximo 802, un campo de límite de retardo de ida y vuelta máximo 804, un campo de límite de fluctuación de fase de retardo máximo 806 y un campo de tasa de pérdida de paquetes 808.

El campo de límite de retardo unidireccional máximo 802 puede comprender aproximadamente 32 bits e indicar el límite o contorno de retardo unidireccional máximo demandado, que puede codificarse en 32 bits en el formato de coma flotante del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y expresarse en milisegundos. El campo de límite de retraso de ida y vuelta máximo 804 puede comprender aproximadamente 32 bits e indica el límite o contorno de retraso de ida y vuelta máximo solicitado, que puede codificarse en 32 bits en el formato de coma flotante del IEEE y expresarse en milisegundos. El campo de límite de fluctuación de fase de retardo máximo 806 puede incluir, aproximadamente, 32 bits e indicar el límite de fluctuación de fase de retardo máximo solicitado, que se puede codificar en 32 bits en el formato de coma flotante de IEEE y expresarse en milisegundos. El campo de tasa de pérdida de paquetes 808 puede comprender, aproximadamente, 32 bits e indicar la tasa de pérdida de paquetes solicitada, que se puede codificar en 32 bits en el formato de coma flotante de IEEE y expresarse en la forma de porcentaje.

La Figura 9 ilustra una forma de realización de un objeto de perfil de ancho de banda 900 que puede incluirse en un mensaje CSO, p.ej., el mensaje CSO 600. El objeto de perfil de ancho de banda 900 se puede utilizar para especificar el ancho de banda requerido para una ruta (por ejemplo, una ruta de etiqueta conmutada (LSP)). El objeto de perfil de ancho de banda 900 puede comprender un campo de capa de transporte 902, una pluralidad de indicadores 904, un bit indicador de ancho de banda asimétrico (A) 906, un campo reservado 908, un campo de flujo descendente de ancho de banda bidireccional 910 y un campo de ancho de banda de flujo ascendente 912.

El campo de capa de transporte 902 puede comprender, aproximadamente, 8 bits y puede establecerse en 0 para indicar que la capa de transporte no está especificada por ACG. En caso contrario, este campo se puede codificar en el formato de "Tipo de Codificación de LSP", tal como se define en el Protocolo de Reserva de Recursos (RSVP)-Ingeniería de tráfico (TE), y se puede utilizar por la ACG para especificar en qué capa de transporte establecer la ruta. Los indicadores 904 pueden comprender, aproximadamente, 16 bits y pueden definirse para diversos fines. El bit A 906 puede comprender aproximadamente 1 bit y se puede establecer para indicar que la conexión es bidireccional con ancho de banda asimétrico. El campo reservado 908 no puede usarse y puede establecerse a cero. El campo de flujo descendente de ancho de banda bidireccional 910 puede comprender aproximadamente 32 bits y puede indicar el ancho de banda de flujo descendente solicitado (es decir, desde el origen al destino) en el caso en que se establece el bit A 906 o la conexión es unidireccional, o puede indicar el ancho de banda bidireccional demandado en otros casos. El campo de ancho de banda de flujo ascendente 912 puede comprender, aproximadamente, 32 bits y puede indicar el ancho de banda de flujo ascendente demandado (es decir, desde el destino al origen). El campo de ancho de banda de flujo ascendente 912 puede incluirse, o usarse, solamente cuando se establece el bit A 906. El campo de flujo descendente de ancho de banda bidireccional 910, y el campo de ancho de banda de flujo ascendente 912, se pueden codificarse en 32 bits en el formato de coma flotante de IEEE y expresarse en bytes por segundo.

La Figura 10 ilustra una forma de realización de un objeto de perfil de modo de conectividad 1000 que puede incluirse en un mensaje CSO, p.ej., el mensaje CSO 600. El objeto de perfil de modo de conectividad 1000 se puede utilizar para especificar el tipo de conexión que se asocia con la demanda de ruta. Se definen los siguientes tipos de conectividad: P-P, P-MP, MP-MP y Anycast (Multi-destino). El objeto de perfil de modo de conectividad 1000 puede comprender un campo de conectividad (C) 1002, una pluralidad de indicadores 1004, un bit de direccionalidad (D) 1006 y un campo reservado 1008.

El campo C 1002 puede incluir, aproximadamente, 8 bits y puede comprender un valor que indica uno de los tipos de

conectividad de la forma siguiente:

0: P-P (punto a punto)

1: P-MP (punto a multipunto)

2: MP-MP (multipunto a multipunto)

3: Anycast (multidestino)

4-255: Reservado.

Los indicadores 1004 pueden incluir, aproximadamente, 16 bits y pueden definirse para diversos fines. El bit D 1006 puede comprender aproximadamente 1 bit que se puede establecer para indicar que la conexión es unidireccional. El campo reservado 1008 puede comprender, aproximadamente, 8 bits que pueden establecerse en cero en la transmisión e ignorarse en la recepción.

La Figura 11 ilustra una forma de realización de un objeto de perfil de localización 1100 que se puede incluir en un mensaje CSO, p.ej., el mensaje CSO 600. El objeto de perfil de localización 1100 se puede utilizar para indicar las direcciones IP de los recursos de capa de aplicación correspondientes (por ejemplo, servidores, almacenamiento, etc.), p.ej., para cada uno de los modos de conectividad definidos en el objeto de perfil de modo de conectividad 1000. Por ejemplo, el objeto de perfil de localización 1100 puede indicar uno de los Orígenes y Destinos para P-P, el Origen y el Conjunto de Destinos para P-MP, el Conjunto de Orígenes y el Destino para MP-P, el Conjunto de Orígenes y el Conjunto de Destinos para MP-MP y el Conjunto de Destinos Candidato para Anycast o Multi-Destino. El objeto de perfil de localización 1100 puede comprender un campo de perfil de localización (L) 1102, un campo de número de fuentes 1104, un campo de número de destinos 1106, una versión del campo de protocolo IP (V) 1108, una pluralidad de indicadores 1110, un campo reservado 1112, y uno de más TLVs opcionales 1114.

El campo L 1102 puede comprender, aproximadamente, 4 bits e indicar un valor basado en el modo, o tipo, de conectividad de la forma siguiente:

0: P-P

1: P-MP

2: MP-P

3: MP-MP

4: Anycast (Multi-destino)

5-15: Reservado.

El campo de número de fuentes 1104 puede comprender, aproximadamente, 8 bits e indicar el número de fuentes. El campo de número de destinos 1106 puede incluir, aproximadamente, 8 bits e indicar el número de destinos. El campo V 1108 puede incluir aproximadamente 2 bits e indicar la versión del protocolo IP. A modo de ejemplo, el campo V 1108 se puede establecer a cero en el caso de IP versión 4 (IPv4) o en 1 en el caso de IP versión 6 (IPv6). Los indicadores 1110 pueden comprender aproximadamente 4 bits y pueden definirse para diversos fines. El campo reservado 1112 puede incluir, aproximadamente, 16 bits que se pueden establecer a cero en la transmisión e ignorarse en la recepción. Los TLVs opcionales 1114 se pueden utilizar para indicar las direcciones IP asociadas con el perfil de localización, tal como se describe con más detalle a continuación.

La Figura 12 ilustra una forma de realización de un TLV opcional 1200 que se puede utilizar en el objeto de perfil de localización 1100, a modo de ejemplo, cuando el campo L 1102 se establece a 0 (p.ej., en el caso de P-P), y el campo V 1108 se establece a 0 (p.ej., en el caso de IPv4). El TLV opcional 1200 puede comprender un campo de dirección IPv4 de origen 1202 que indica la dirección IPv4 del origen, y un campo de dirección IPv4 de destino 1204 que indica la dirección IPv4 del destino. La Figura 13 ilustra una forma de realización de otro TLV opcional 1300 que se puede usar en el objeto de perfil de localización 1100, a modo de ejemplo, cuando el campo L 1102 se establece a 1 (p.ej., en el caso de P-MP), el campo de números de destino 1106 se establece en 4 y el campo V 1108 se establece a 0 (p.ej., en el caso de IPv4). El TLV opcional 1300 puede incluir un campo de dirección IPv4 de origen 1302 que indica la dirección IPv4 del origen, y cuatro campos de dirección IPv4 de destino 1304 que indican, cada uno, la dirección IPv4 de uno de los 4 destinos. De forma similar, otros TLVs opcionales 1114 se pueden utilizar para otros casos. En los casos en donde el campo V 1108 se establece a 1 (p.ej., en el caso de IPv4), cada dirección IPv6 puede incluir, de forma aproximada, 16 bytes.

La Figura 14 ilustra una forma de realización de un objeto de perfil de protección 1400 que puede incluirse en un

mensaje CSO, p.ej., el mensaje CSO 600. El objeto de perfil de protección 1400 se puede utilizar para indicar el nivel de protección requerido para una demanda de reserva de ruta. Los niveles de protección pueden incluir sin protección, protección 1+1 y protección compartida. En el caso de protección 1+1 y protección compartida, el objeto de perfil de protección 1400 puede indicar el diferencial de ruta de protección a partir de la ruta diseñada, tal como en términos de retardo, saltos operativos, distancia, etc. El objeto de perfil de protección 1400 puede comprender un campo de nivel de protección (P) 1402 y una pluralidad de indicadores 1404, que pueden incluir un bit de diversidad (S) de grupo de enlace de lista compartida (SRLG) 1406, un bit de diversidad de nodo (N) 1408, y un bit de diversidad de enlace (L) 1410. El objeto de perfil de protección 1400 puede incluir, además, un campo reservado 1412, y uno o más TLVs opcionales 1414.

El campo P 1402 puede comprender, aproximadamente, 8 bits e indicar un valor asociado con un nivel de protección como sigue:

0: Sin protección

1: 1+1

2: Protección compartida

3-255: Reservado.

Los indicadores 1404 pueden incluir, aproximadamente, 16 bits y se pueden utilizar para diferentes propósitos. Más concretamente, el bit S 1406 puede establecerse cuando se requiere que la ruta de protección sea SRLG diferente a partir de la ruta diseñada para una protección de tipo 1+1 o compartida. El bit N 1408 puede establecerse cuando se requiere que la ruta de protección sea un nodo diferente a partir de la ruta diseñada para una protección de tipo 1+1 o compartida. El bit L 1410 se puede establecer cuando se requiere que la ruta de protección sea un enlace diferente a partir de la ruta diseñada para una protección de tipo 1+1 o compartida. El campo reservado 1412 puede comprender, aproximadamente, 8 bits, que pueden establecerse en cero en la transmisión e ignorarse en la recepción. Los TLVs opcionales 1414 se pueden utilizar para indicar el diferencial de ruta de protección a partir de la ruta diseñada, p.ej., en términos de retardo, conteo de saltos operativos y distancia, tal como se describe a continuación. Los campos TLVs opcionales 1414 pueden llenarse cuando el campo P 1402 se establece para ser 1 o 2.

La Figura 15 ilustra una forma de realización de un TLV opcional 1500 que se puede usar en el objeto de perfil de protección 1400, a modo de ejemplo, cuando el campo P 1402 se establece a 1 o 2. El TLV opcional 1500 puede incluir un campo de diferencial de retardo 1502, un campo de diferencial de conteo de saltos operativos 1504, y un campo de diferencial de distancia 1506. El campo de diferencial de retardo 1502 puede comprender, aproximadamente, 32 bits, y puede codificarse en el formato de coma flotante de IEEE expresado en la forma de porcentaje. El campo de diferencial de retardo 1502 puede indicar el diferencial de retardo de la ruta de protección a partir de la ruta diseñada. Por ejemplo, un valor del 50 % puede indicar que la ruta de protección no puede tener más que el 50 % del retardo de la ruta diseñada. El campo de diferencial de conteo de saltos operativos 1504 puede comprender aproximadamente 32 bits y se puede codificarse en el formato de coma flotante de IEEE expresado en la forma de porcentaje. El campo de diferencial de conteo de saltos operativos 1504 puede indicar el diferencial de conteo de saltos operativos de la ruta de protección a partir de la ruta diseñada. El campo de diferencial de distancia 1506 puede incluir 32 bits aproximadamente, y se puede codificar en el formato de coma flotante de IEEE expresado en porcentaje. El campo de diferencial de distancia 1506 puede indicar el diferencial de distancia de la ruta de protección a partir de la ruta diseñada.

La Figura 16 ilustra una forma de realización de un objeto de ruta 1600 que puede incluirse en un mensaje CSO, p.ej., el mensaje CSO 600. El objeto de ruta 1600 se puede utilizar para proporcionar la información de ruta en respuesta a una estimación de ruta original, o una demanda de reserva/modificación de ruta en un mensaje de demanda. El objeto de ruta 1600 puede incluirse en un mensaje de Respuesta. El objeto de ruta 1600 puede comprender un campo de tipo de servicio (S) 1602, una pluralidad de indicadores 1604 que pueden incluir un bit de protección (P) 1606, un campo reservado 1608, un número de ID de demanda de servicio 1610 y al menos un TLV opcional 1612.

El campo S 1602 puede comprender, aproximadamente, 8 bits y tener un valor que indica un tipo de servicio, tal como sigue:

0: Reserva de ruta

1: Modificación de ruta

2: Estimación de ruta.

Los indicadores 1604 pueden incluir, aproximadamente, 16 bits, y se pueden utilizar para diferentes propósitos. Más

concretamente, el bit P 1606 se puede establecer para indicar que la ruta es una ruta de protección. El bit P 1606 se puede utilizar cuando el campo S 1602 se establece a 0 (para indicar un tipo de servicio de reserva de ruta). El campo reservado 1608 puede comprender 8 bits aproximadamente, que se pueden establecer a cero en la transmisión e ignorarse en la recepción. El número de ID de demanda de servicio 1610 puede comprender, aproximadamente, 32 bits e indicar un número de ID de demanda de servicio que se puede proporcionar en el objeto de perfil de servicio 700 en un mensaje de Demanda. El número de ID de demanda de servicio puede identificar la demanda de ruta original. El contenido del TLV opcional 1612 puede variar dependiendo del campo S 1602, tal como se describe a continuación.

La Figura 17 ilustra una forma de realización de un TLV 1700 opcional que se puede usar en el objeto de ruta 1600, para, a modo de ejemplo, cuando el campo S 1602 se establece a 0. El TLV opcional 1700 puede comprender un campo de identificador de ruta 1702, una dirección IPv4 de origen de aplicación 1704, una dirección IPv4 de origen de red 1706, una dirección IPv4 de destino de aplicación 1708, una dirección IPv4 de origen de red 1710 y un ancho de banda reservado 1712. El campo de identificador 1702 puede comprender aproximadamente 32 bits e identificar la ruta reservada en una red de transporte. El campo de identificador 1702 puede ser asignado por la NCG. El ancho de banda reservado 1712 puede indicar un ancho de banda para una ruta reservada.

La Figura 18 ilustra una forma de realización de otro TLV opcional 1800 que se puede utilizar en el objeto de ruta 1600, por ejemplo, cuando el campo S 1602 se establece a 1. El TLV opcional 1800 puede incluir un campo identificador de ruta 1802, una dirección IPv4 de origen de aplicación 1804, una dirección IPv4 de origen de red 1806, una dirección IPv4 de destino de aplicación 1808, una dirección IPv4 de origen de red 1810 y un ancho de banda modificado 1812. El campo de identificador 1802 puede configurarse, de forma prácticamente similar, al campo de identificador 1702. El ancho de banda modificado 1812 puede indicar un ancho de banda para una ruta modificada.

La Figura 19 ilustra una forma de realización de otro TLV opcional 1900 que se puede utilizar en el objeto de ruta 1600, por ejemplo, cuando el campo S 1602 se establece a 2. El TLV opcional 1900 puede incluir un campo de identificador de ruta 1902, una dirección IPv4 de origen de aplicación 1904, una dirección IPv4 de origen de red 1906, una dirección IPv4 de destino de aplicación 1908, una dirección IPv4 de origen de red 1910 y un ancho de banda estimado 1912. El campo de identificador 1902 puede configurarse, de forma prácticamente similar, al campo de identificador 1702. El ancho de banda modificado 1912 puede indicar un ancho de banda para una ruta estimada.

La Figura 20 ilustra una forma de realización de un objeto de VNT 2000 que puede incluirse en un mensaje CSO, p.ej., el mensaje CSO 600. El objeto de VNT 2000 se puede utilizar para proporcionar la abstracción de la topología en respuesta a una demanda de VNT original. La información relativa a la demanda de VNT original se puede transmitir a través del objeto de perfil de localización 1100, y el objeto de perfil de servicio 700, en un mensaje de Demanda. El objeto de VNT 2000 puede proporcionar un ID de demanda de servicio asociado con una demanda original e información de topología de red virtual (p.ej., el ancho de banda disponible) para cada perfil de localización solicitado. El perfil de localización proporcionado en la demanda de VNT original puede incluir direcciones IP de las localizaciones de aplicación. En respuesta a dicha demanda, el objeto de VNT 2000, en un mensaje de respuesta, puede proporcionar el ID de localización de aplicación original y su ID de nodo de red correspondiente (p.ej., direcciones IP) para permitir que la ACG consulte la información proporcionada por la NCG. El VNT se define aquí como el ancho de banda disponible para un par de nodos dado.

El objeto de VNT 2000 puede comprender un campo L 2002, un campo de número de orígenes 2004, un campo de número de destinos 2006, un campo V 2008, una pluralidad de indicadores 2010 y un campo reservado 2012, que puede configurarse, de forma prácticamente similar, al campo L 1102, el campo de número de orígenes 1104, el campo de número de destinos 1106, los indicadores 1110 y el campo reservado 1112, respectivamente. El objeto de VNT 2000 puede comprender, además, un número de ID de demanda de servicio 2014 y uno o más TLVs opcionales 2016. El número de ID de demanda de servicio 2014 puede comprender aproximadamente 32 bits, e indicar el valor del número de ID de demanda de servicio que identifica, de forma exclusiva, la demanda de servicio original que se proporciona en el objeto de perfil de servicio 700 en un mensaje de demanda. Los TLVs opcionales 2016 se pueden utilizar para proporcionar información detallada de VNT, tal como se describe con más detalle a continuación.

La Figura 21 ilustra una forma de realización de un TLV opcional 2100 que se puede utilizar en el objeto VNT 2000, por ejemplo, cuando el campo L 2002 se establece a 0 (p.ej., en el caso de P-P), y el campo V 2008 se establece a 0 (p.ej., en el caso de IPv4). El TLV opcional 2100 puede comprender un campo de dirección IPv4 de origen de aplicación 2102, un campo de dirección de IPv4 de origen de red 2104, un campo de dirección de IPv4 de destino de aplicación 2106, un campo de dirección de IPv4 de origen de red 2108 y un campo de ancho de banda disponible 2110. La Figura 22 ilustra una forma de realización de otro TLV opcional 2200 que se puede utilizar en el objeto de VNT 2000, por ejemplo, cuando el campo L 2002 se establece a 1 (p.ej., en el caso de P-MP), y el campo V 2008 se establece a 0 (p.ej., en el caso de IPv4). El TLV opcional 2200 puede incluir un campo de dirección IPv4 de primer origen de aplicación (nº 1) 2202, un campo de dirección IPv4 de primer origen de red (nº 1) 2204, un campo de dirección IPv4 de primer destino de aplicación (nº 1) 2206, un campo de dirección IPv4 de primer origen de red (nº 1) 2208, y un campo de primer campo de ancho de banda disponible 2210. Además, el TLV opcional 2200 puede

incluir un campo de dirección IPv4 de segundo origen de aplicación (nº 2) 2212, un campo de dirección IPv4 de segundo origen de red (nº 2) 2214, un campo de dirección IPv4 de segundo destino de aplicación (nº 2) 2216, un campo de dirección de IPv4 de segundo origen de red (nº 2) 2218 y un campo de segundo ancho de banda disponible 2220.

La Figura 23 ilustra una forma de realización de un intercambio de mensaje de CSOP 2300 que puede establecerse entre una ACG 2310 y una NCG 2320 usando la interfaz CSO y CSOP. La ACG 2310 puede enviar, en primer lugar, un mensaje de Demanda 2301, que puede incluir al menos algunos de los objetos y TLVs opcionales descritos anteriormente, a la NCG 2320. La NCG 2320 puede recibir y procesar el mensaje de demanda 2301 y a continuación, reenviar un mensaje de Respuesta 2302 a la ACG 2310. El mensaje de respuesta 2302 puede comprender al menos algunos de los objetos y TLVs opcionales, tal como se describió con anterioridad. En otras formas de realización, la ACG 2310 y la NCG 2320 pueden intercambiar otros mensajes de CSO, tales como un mensaje de Inicialización, un mensaje KeepAlive, un mensaje de Liberación, un mensaje de ReleaseConf., Un mensaje de Notificación, un mensaje de CSOPErr, un mensaje de CLOSE, o combinaciones de los mismos. En dichas formas de realización, el intercambio de mensaje de CSOP 2300 se puede iniciar por la ACG 2310 o la NCG 2320.

La Figura 24 ilustra una forma de realización de una unidad de red 2400, que puede ser cualquier dispositivo que transporte y procese datos a través de la red. La unidad de red 2400 puede incluir uno o más puertos o unidades de entrada 2410 acoplados a un receptor (Rx) 2412, con el fin de recibir señales y tramas/datos procedentes de otros componentes de la red. La unidad de red 2400 puede comprender una unidad lógica 2420 para determinar a qué componentes de red enviar datos. La unidad lógica 2420 se puede poner en práctica utilizando hardware, software o ambos. La unidad de red 2400 puede comprender, además, uno o más puertos o unidades de salida 2430 acoplados a un transmisor (Tx) 2432, con el fin de transmitir señales y tramas/datos a los otros componentes de red. El receptor 2412, la unidad lógica 2420 y el transmisor 2432 pueden, además, poner en práctica o soportar el sistema de CSOP 400 y el intercambio de mensaje de CSOP 2300. Los componentes de la unidad de red 2400 pueden estar dispuestos tal como se muestra en la Figura 24.

Los componentes de red descritos anteriormente se pueden poner en práctica en cualquier componente de red de propósito general, tal como un ordenador o componente de red con suficiente potencia de procesamiento, recursos de memoria y capacidad de rendimiento de red para la gestión de la carga de trabajo necesaria puesta sobre él. La Figura 25 ilustra un componente de red típico de uso general 2500 adecuado para realizar una o más formas de realización de los componentes aquí dados a conocer. El componente de red 2500 incluye un procesador 2502 (que puede denominarse como una unidad central de procesador o CPU), que está en comunicación con dispositivos de memoria que incluyen almacenamiento secundario 2504, memoria de solamente lectura (ROM) 2506, memoria RAM 2508, dispositivos de entrada/salida (I/O) 2510 y dispositivos de conectividad de red 2512. El procesador 2502 se puede poner en práctica como uno o más circuitos integrados de CPU, o puede ser parte de uno o más circuitos integrados específicos de la aplicación (ASICs).

El almacenamiento secundario 2504 está compuesto, típicamente, por una o más unidades de disco, o unidades de cinta, y se utiliza para una memorización no volátil de datos y como un dispositivo de almacenamiento de datos de desbordamiento si la memoria RAM 2508 no es lo suficientemente grande como para contener todos los datos de trabajo. El almacenamiento secundario 2504 se puede utilizar para memorizar programas que se cargan en la RAM 2508 cuando dichos programas se seleccionan para su ejecución. La memoria ROM 2506 se utiliza para memorizar instrucciones y tal vez datos que son objeto de lectura durante la ejecución del programa. La memoria ROM 2506 es un dispositivo de memoria no volátil que generalmente tiene una capacidad de memoria pequeña en relación con la mayor capacidad de memoria del almacenamiento secundario 2504. La memoria RAM 2508 se utiliza para memorizar datos volátiles y tal vez para almacenar instrucciones. El acceso tanto a la ROM 2506 como a la RAM 2508 suele ser más rápido que al almacenamiento secundario 2504.

Se da a conocer al menos una forma de realización y las variaciones, combinaciones y/o modificaciones de las formas de realización y/o características de las formas de realización realizadas por un experto en la técnica están dentro del alcance de la idea inventiva. Las formas de realización alternativas que resultan de combinar, integrar y/u omitir características de las formas de realización también están dentro del alcance de la idea inventiva. Cuando los rangos o limitaciones numéricas se establecen expresamente, dichos rangos o limitaciones expresos deben entenderse que incluyen rangos iterativos o limitaciones de magnitud similar que caen dentro de los rangos o limitaciones expresamente establecidos (p.ej., desde aproximadamente 1 a aproximadamente 10 incluye, 2, 3, 4, etc.; mayor que 0.10 incluye 0.11, 0.12, 0.13, etc.). Por ejemplo, cada vez que se da a conocer un rango numérico con un límite inferior, R_1 y un límite superior, R_u, se divulga, específicamente, cualquier número que se encuentre dentro del rango. En particular, se dan a conocer, de forma específica, los siguientes números dentro del rango: $R = R_1 + k * (R_u - R_1)$, en donde k es una variable que varía de 1 por ciento a 100 por ciento con un incremento de 1 por ciento, es decir, k es 1 por ciento, 2 por ciento, 3 por ciento, 4 por ciento, 7 por ciento,..., 70 por ciento, 71 por ciento, 72 por ciento,..., 97 por ciento, 96 por ciento, 97 por ciento, 98 por ciento, 99 por ciento o 100 por ciento. Además, cualquier rango numérico definido por dos números R, tal como se define con anterioridad, son también dados a conocer de forma específica. El uso del término "opcionalmente" con respecto a cualquier elemento de una reivindicación significa que el elemento es requerido o, como alternativa, el elemento no es requerido, ambas

alternativas caen dentro del alcance de la reivindicación. El uso de términos más amplios, tales como comprende, incluye y tiene, debe entenderse que proporciona soporte para términos más limitados, tales como que consiste en, que consiste esencialmente en, y que comprende prácticamente. En consecuencia, el alcance de protección no está limitado por la descripción expuesta anteriormente, sino que se define por las siguientes reivindicaciones. Todas y cada una de las reivindicaciones se incorporan como idea inventiva adicional en la especificación y las reivindicaciones son formas de realización de la presente invención. La discusión de una referencia en la idea inventiva no es una admisión de que es una técnica anterior, especialmente cualquier referencia que tenga una fecha de publicación posterior a la fecha de prioridad de esta solicitud.

Los presentes ejemplos deben considerarse como ilustrativos y no restrictivos, y la intención no debe limitarse a los detalles aquí proporcionados. A modo de ejemplo, los diversos elementos o componentes se pueden combinar, o integrarse, en otro sistema, o ciertas características se pueden omitir o no ponerse en práctica.

Además, las técnicas, sistemas, subsistemas y métodos descritos e ilustrados en las diversas formas de realización como discretos o separados pueden combinarse o integrarse con otros sistemas, módulos, técnicas o métodos sin desviarse del alcance de la presente invención. Otros elementos ilustrados o descritos como acoplados o directamente acoplados o que se comunican entre sí, pueden estar indirectamente acoplados o comunicarse a través de alguna interfaz, dispositivo o componente intermedio, ya sea de forma eléctrica, mecánica o de otra forma.

REIVINDICACIONES

1. Un aparato que comprende:

una pasarela (ACG) de optimización de estratos cruzados de aplicación, CSO, (314) acoplada a un estrato de aplicación (110, 210, 310, 410) que gestiona una pluralidad de servidores (112, 212, 312);

una pasarela CSO de red, NCG, (324) acoplada a un estrato de red (120, 220, 320, 420) que gestiona una pluralidad de nodos de red (122, 222, 322) y está configurada para comunicarse con la ACG (314) utilizando un Protocolo de CSO, CSOP; y

una interfaz CSO establecida entre la ACG (314) y la NCG (324);

en donde la ACG (314) está configurada para comunicarse con la NCG (324) por intermedio de la interfaz CSO y para proporcionar información de recursos de aplicación y limitaciones de acceso a entidades externas en el estrato de la red (120, 220, 320, 420);

en donde la NCG (324) está configurada para comunicarse con la ACG (314) por intermedio de la interfaz CSO, y para proporcionar información de recursos de red y limitaciones de acceso a entidades del estrato de aplicación;

en donde se intercambian una pluralidad de mensajes de CSOP por intermedio de la interfaz CSO entre la ACG (314) y la NCG (324) para una asignación, un aprovisionamiento y una optimización comunes de recursos de red de aplicación.

2. El aparato según la reivindicación 1, en donde el CSOP proporciona medios para garantizar el intercambio de información necesaria para lograr la CSO al mismo tiempo que se evita el intercambio de información privada o segura que no está autorizada a otras entidades, redes o capas.

3. El aparato según la reivindicación 1, en donde los mensajes de CSOP comprenden un mensaje de Demanda que se utiliza desde la ACG (314) a la NCG (324) para solicitar una configuración de ruta, una estimación de ruta con o sin compromiso real de reserva/asignación, o una topología de red virtual.

4. El aparato según la reivindicación 3, en donde los mensajes de CSOP comprenden un mensaje de Respuesta que se utiliza desde la NCG (324) a la ACG (314) en respuesta al mensaje de Demanda.

5. El aparato según la reivindicación 1, en donde los mensajes de CSOP comprenden un mensaje de Liberación que se utiliza desde la ACG (314) a la NCG (324) para solicitar la liberación de una ruta existente.

6. El aparato según la reivindicación 5, en donde los mensajes de CSOP comprenden un mensaje de configuración de liberación, ReleaseConf, que se utiliza desde la NCG (324) a la ACG (314) en respuesta al mensaje de liberación para confirmar la liberación de la ruta existente.

7. El aparato según la reivindicación 1, en donde los mensajes de CSOP comprenden un mensaje de Notificación que se utiliza desde la ACG (314) a la NCG (324), o desde la NCG (324) a la ACG (314), para notificar un evento ocurrido; o

un mensaje de Notificación que se utiliza desde la NCG (324) a la ACG (314) para supervisar un servicio de transporte existente.

8. El aparato según la reivindicación 1, en donde los mensajes de CSOP comprenden un mensaje de error de CSOP, CSOPErr, que se utiliza para indicar una condición de error de protocolo que se asocia con CSOP; o

los mensajes de CSOP comprenden un mensaje de Inicialización que se utiliza para iniciar una sesión de CSOP con un procedimiento de autenticación entre la ACG (314) y la NCG (324); o

los mensajes de CSOP comprenden un mensaje de mantenimiento activo, KeepAlive, que se utiliza para mantener una sesión de CSOP; o

un mensaje de sesión de CSOP, CLOSE, que se utiliza para finalizar una sesión de CSOP.

9. El aparato según la reivindicación 1, que comprende, además, una pluralidad de ACGs (314) que corresponde, cada una, a un centro de datos respectivo, o un respectivo servicio informático en la nube; o

que comprende una pluralidad de NCGs (324) correspondiendo, cada una, a una respectiva portadora o dominio de red del proveedor de servicios.

10. Un componente de red que comprende:

un receptor configurado para recibir un primer mensaje de protocolo CSOP de optimización de estrato cruzado, CSO, por intermedio de una interfaz CSO establecida entre un estrato de aplicación (110, 210, 310, 410) y un estrato de red (120, 220, 320, 420); y

un controlador de plano configurado para habilitar una CSO entre el estrato de aplicación (110, 210, 310, 410) y el estrato de red (120, 220, 320, 420) procesando el primer mensaje de CSOP para asignar, aprovisionar u optimizar un recurso de red de aplicación común; y

un transmisor configurado para enviar un segundo mensaje de CSOP por intermedio de la interfaz CSO en respuesta al primer mensaje de CSOP, o para la finalidad de CSO;

en donde el primer mensaje de CSOP, y el segundo mensaje de CSOP, proporcionan mecanismos de abstracción y resumen para garantizar el intercambio de información necesaria para lograr una CSO mientras se evitar la utilización compartida de información privada o segura, que no está autorizada a otras entidades, redes y/o estratos.

11. El componente de red según la reivindicación 10, en donde el primer mensaje de CSOP y el segundo mensaje de CSOP comprenden una cabecera de mensaje de CSOP con uno o más objetos, y en donde la cabecera de mensaje de CSOP comprende un campo de versión, un campo de tipo de mensaje y un campo de longitud de mensaje.

12. El componente de red según la reivindicación 11, en donde el campo de tipo de mensaje se establece a 1 para indicar un tipo de mensaje de Inicialización, a 2 para indicar un tipo de mensaje de mantenimiento activo, KeepAlive, 3 para indicar un tipo de mensaje de Demanda, 4 para indicar un tipo de mensaje de Respuesta, 5 para indicar un tipo de mensaje de Liberación, 6 para indicar un mensaje de configuración de liberación, ReleaseConf, 7 para indicar un mensaje de Notificación, 8 para indicar un mensaje de error de CSOP, CSOPErr, o 9 para indicar un mensaje de sesión de CSOP, CLOSE.

13. El componente de red según la reivindicación 11, en donde los objetos comprenden un objeto de perfil de autenticación, en el final de los objetos en el primer o segundo mensaje de CSOP, y en donde el objeto de perfil de autenticación comprende un campo de clase de objeto de autenticación, un campo de longitud, un campo de sub-tipo, un campo de Índice de Parámetro de Seguridad, SPI, y un testigo informático denominado token.

14. El componente de red según la reivindicación 11, en donde los objetos comprenden un objeto de perfil de servicio que incluye un campo de tipo de servicio, S, una pluralidad de indicadores y un identificador, ID, de número de demanda de servicio, y en donde el campo S se establece a 0 para indicar una Reserva de ruta, 1 para indicar una Modificación de ruta, 2 para indicar una Estimación de ruta, o 3 para indicar una Demanda de topología de red virtual, VNT.

15. El componente de red según la reivindicación 11, en donde los objetos comprenden un objeto de perfil de rendimiento que comprende un campo de límite de retardo unidireccional máximo, un campo de límite de retardo de ida y vuelta máximo, un campo de límite de fluctuación de fase de retardo máximo y un campo de tasa de pérdida de paquetes; o

en donde los objetos comprenden un objeto de perfil de ancho de banda que comprende un campo de capa de transporte, una pluralidad de indicadores, un bit de indicador de ancho de banda asimétrico, A, un campo de flujo descendente de ancho de banda bidireccional, y un campo de ancho de banda de flujo ascendente; o

en donde los objetos comprenden un objeto de perfil de modo de conectividad que incluye un campo de conectividad, C, una pluralidad de indicadores, y un bit de direccionalidad, D, y en donde el campo C se establece a 0 para indicar una conectividad de punto a punto, P-P, 1 para indicar una conectividad de punto a multipunto, P-MP, 2 para indicar una conectividad de multipunto a multipunto, MP-MP, o 3 para indicar una conectividad ‘any-cast’ para múltiples destinos; o

en donde los objetos comprenden un objeto de perfil de localización que comprende un campo de perfil de localización, L, un campo de numero de orígenes, un campo de número de destinos, un campo de versión, V, del Protocolo Internet, IP, una pluralidad de indicadores, y uno o más Tipo/Longitud/Valores opcionales, TLVs, y en donde el campo L se establece a 0 para indicar una conectividad de punto a punto, P-P, 1 para indicar una conectividad de punto a multipunto, P-MP, 2 para indicar una conectividad de multipunto a punto, MP-P, 3 para indicar una conectividad de multipunto a multipunto, MP-MP, o 4 para indicar una conectividad ‘any-cast’ para múltiples destinos.

16. El componente de red según la reivindicación 11, en donde los objetos comprenden un objeto de perfil de protección que comprende un campo de nivel de protección, P, y una pluralidad de indicadores que incluyen un bit de diversidad S de grupo de enlaces de lista compartida, S, un grupo de enlace de lista compartida, SRLG, un bit de

diversidad de nodo, N, y un bit de diversidad de enlace, L, y uno o más Tipo/Longitud/Valores opcionales, TLVs, y en donde el campo P se establece a 0 para indicar Sin protección, 1 para indicar protección 1+1, o 2 para indicar Protección compartida.

17. El componente de red según la reivindicación 11, en donde los objetos comprenden un objeto de ruta que comprende un campo de tipo de servicio, S, una pluralidad de indicadores que incluyen un bit de protección, P, un número de identificador de demanda de servicio, ID, y al menos un Tipo/Longitud/Valor opcional, TLV, y en donde el campo S se establece a 0 para indicar una Reserva de ruta, 1 para indicar una Modificación de ruta, o 2 para indicar una Estimación de ruta.

18. El componente de red según la reivindicación 17, en donde un TLV opcional comprende un identificador de ruta, una versión 4 de Protocolo Internet de origen de aplicación, IP, dirección IPv4, una dirección IPv4 de origen de aplicación, una dirección IPv4 de origen de red, una dirección IPv4 de destino de aplicación, una dirección IPv4 de origen de red y un ancho de banda reservado; o

en donde un TLV opcional comprende un identificador de ruta, una dirección de versión 4, IPv4, de Protocolo Internet de origen de aplicación, IP, una dirección IPv4 de origen de aplicación, una dirección IPv4 de origen de red, una dirección IPv4 de destino de aplicación, una dirección IPv4 de origen de red y un ancho de banda modificado; o

en donde un TLV opcional comprende un identificador de ruta, una dirección de versión 4, IPv4, de Protocolo Internet de origen de aplicación, IP, una dirección IPv4 de origen de aplicación, una dirección IPv4 de origen de red, una dirección IPv4 de destino de aplicación, una dirección IPv4 de origen de red y un ancho de banda estimado.

19. El componente de red según la reivindicación 11, en donde los objetos comprenden un objeto de topología de red virtual, VNT, que comprende un campo de perfil de localización, L, un campo de número de orígenes, un campo de número destinos, una versión, V, de Protocolo Internet, IP, una pluralidad de indicadores, un número de identificador de demanda de servicio, ID, y uno de Tipo/Longitud/Valores opcionales, TLVs, y en donde el campo L se establece a 0 para indicar una conectividad de punto a punto, P-P, 1 para indicar una conectividad de punto a multipunto, P-MP, 2 para indicar una conectividad de multipunto a punto, MP-P, 3 para indicar una conectividad de multipunto a multipunto, MP-MP, o 4 para indicar una conectividad ‘any-cast’ para múltiples destinos.

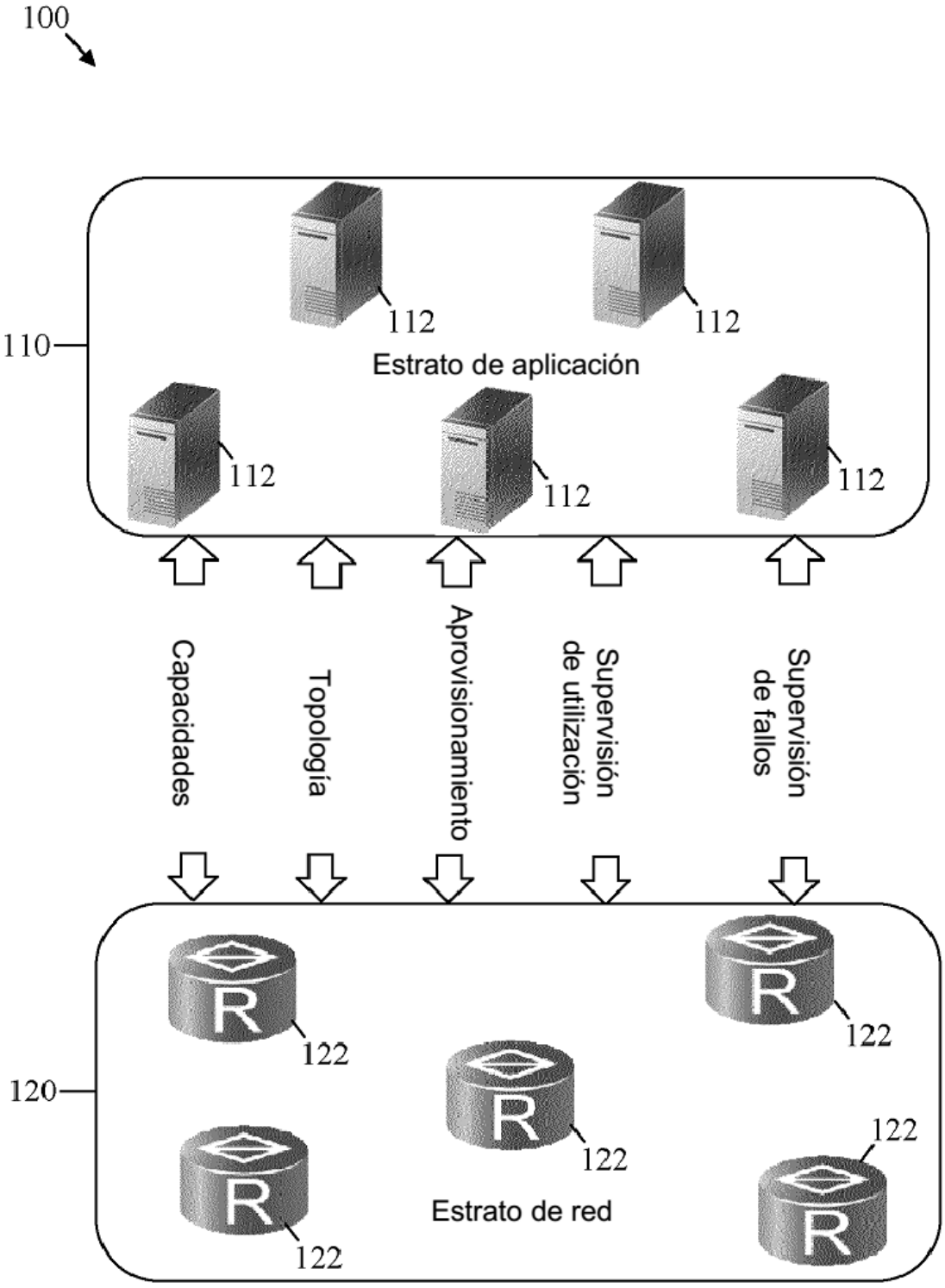

100
110
112
112
Estrato de aplicación
112
112
112
Capacidades
Topología
Aprovisionamiento
Supervisión de utilización
Supervisión de fallos
120
122
122
122
122
122
Estrato de red

FIG. 1

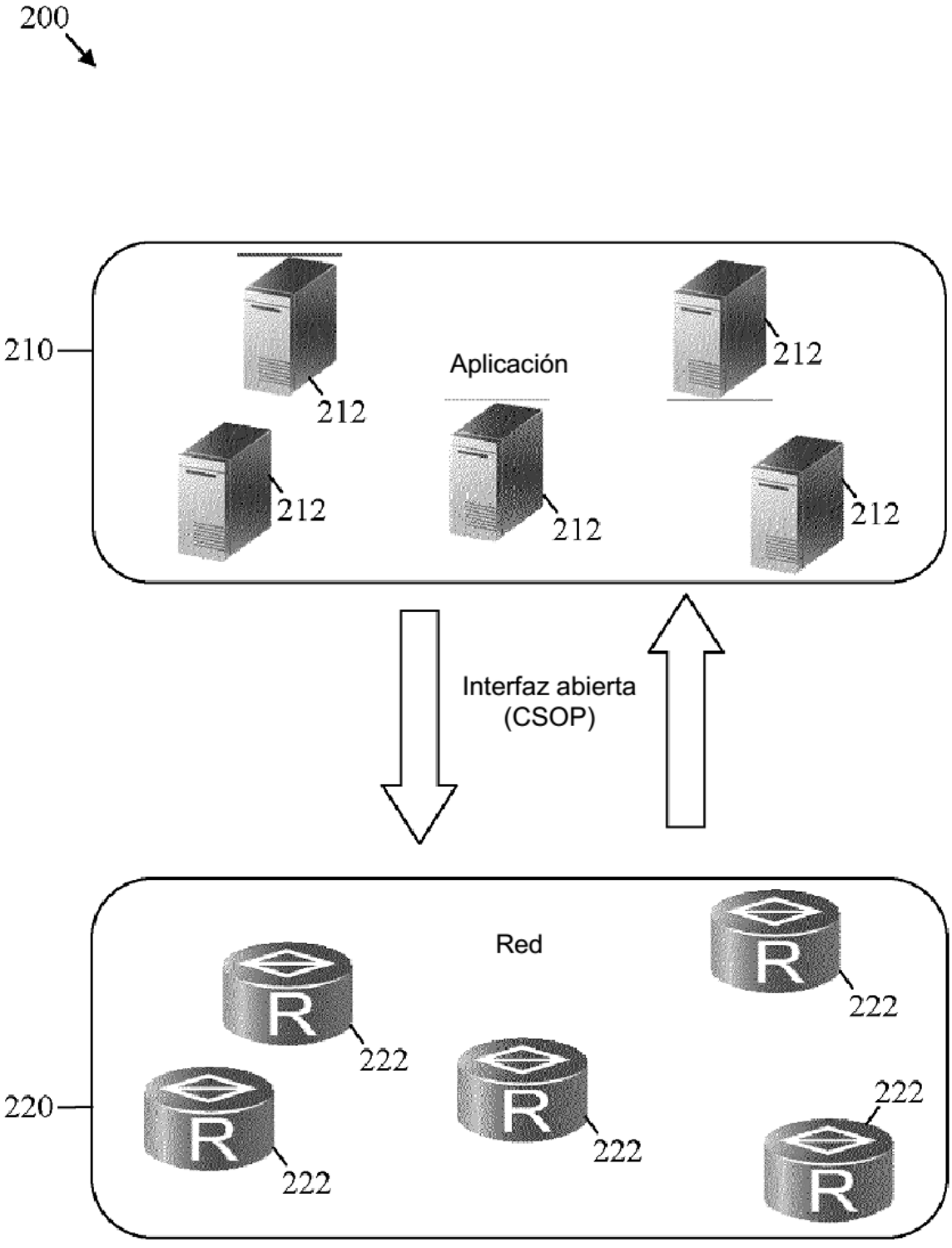

200
210
212
212
212
Aplicación
212
212
212
Interfaz abierta
(CSOP)
220
Red
222
222
222
222
222

FIG. 2

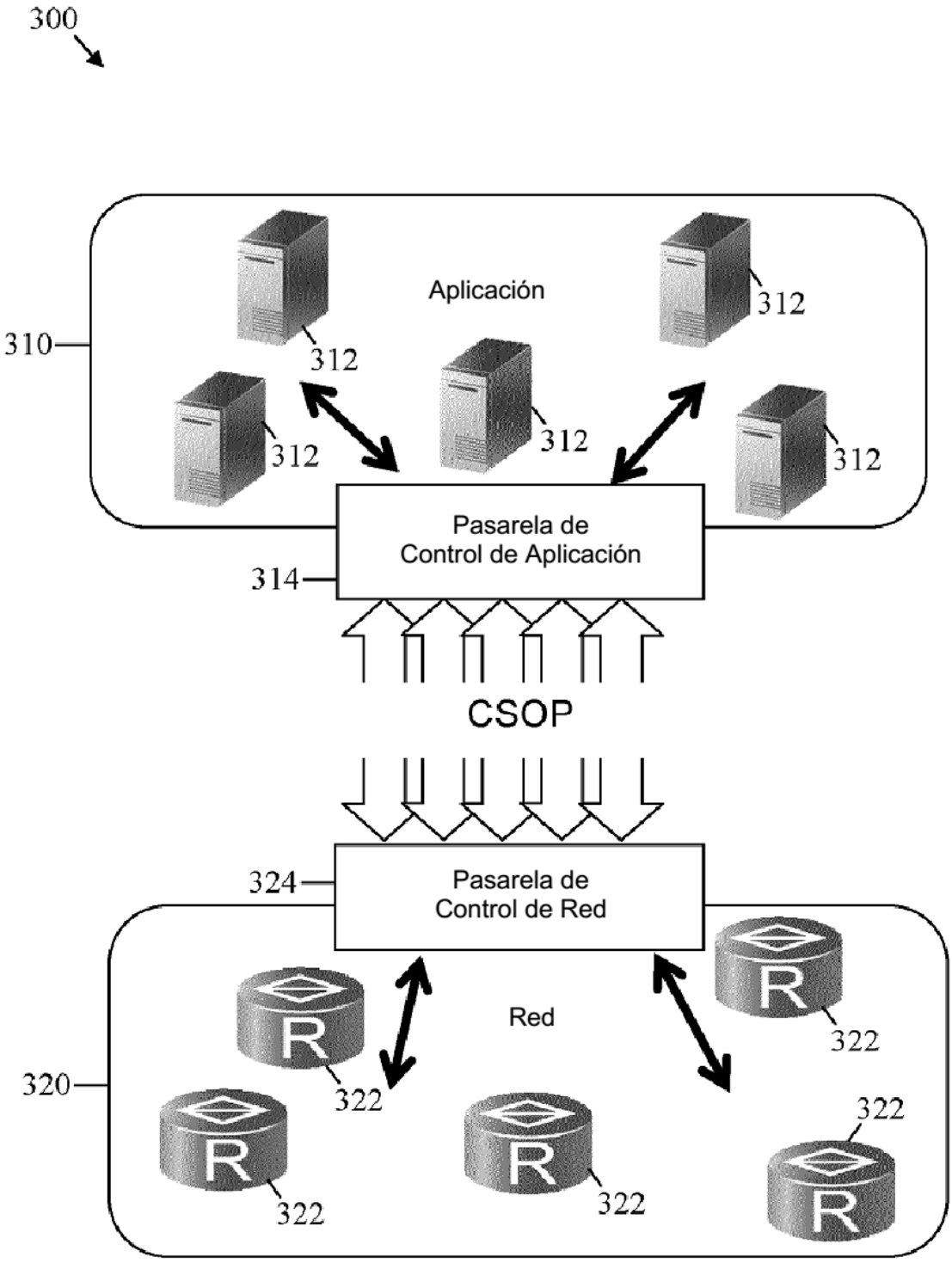

300
310
Aplicación
312
312
312
312
312
Pasarela de
Control de Aplicación
314
CSOP
324
Pasarela de
Control de Red
320
Red
R
322

FIG. 3

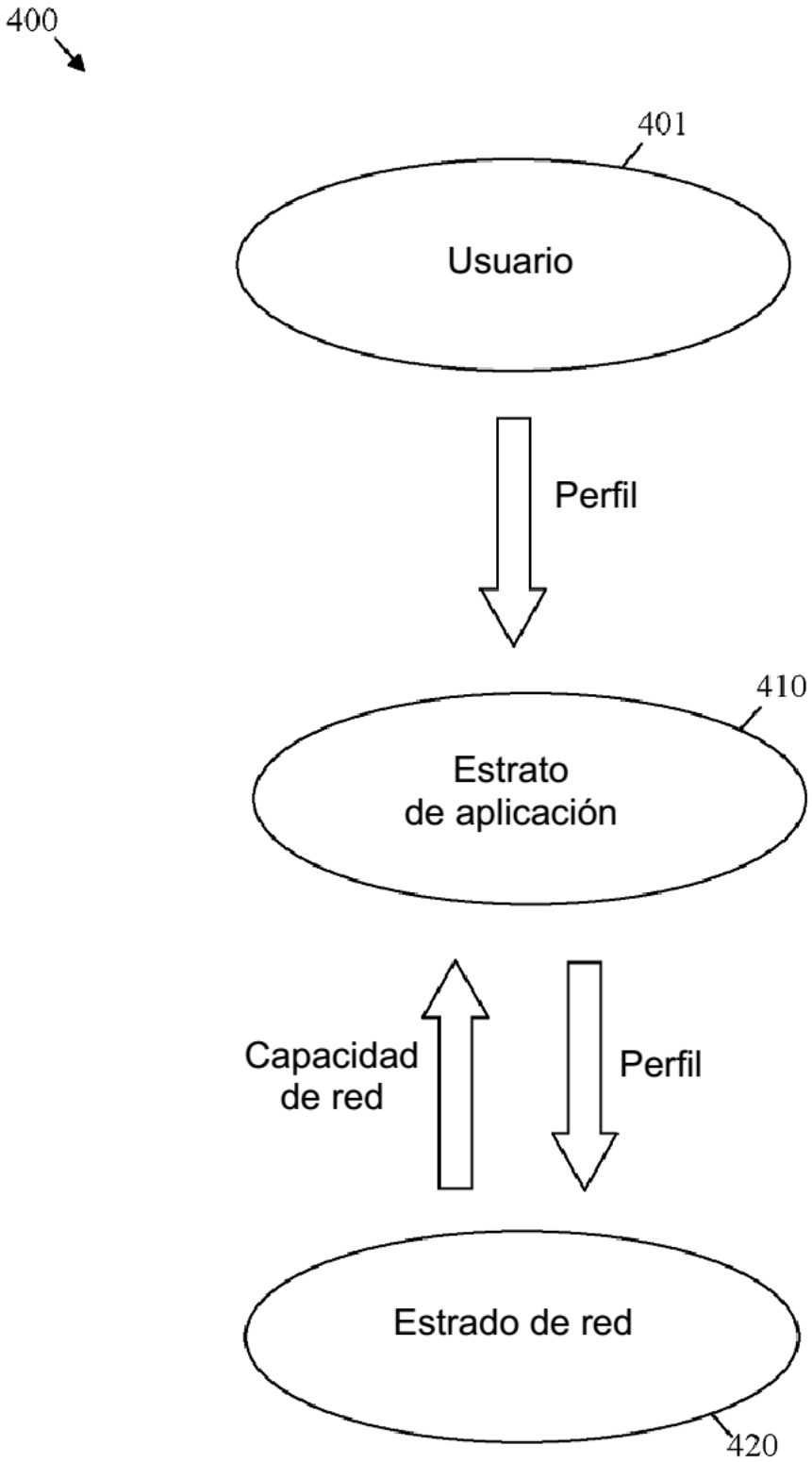

400
401
Usuario
Perfil
410
Estrato
de aplicación
Capacidad
de red
Perfil
Estrado de red
420

FIG. 4

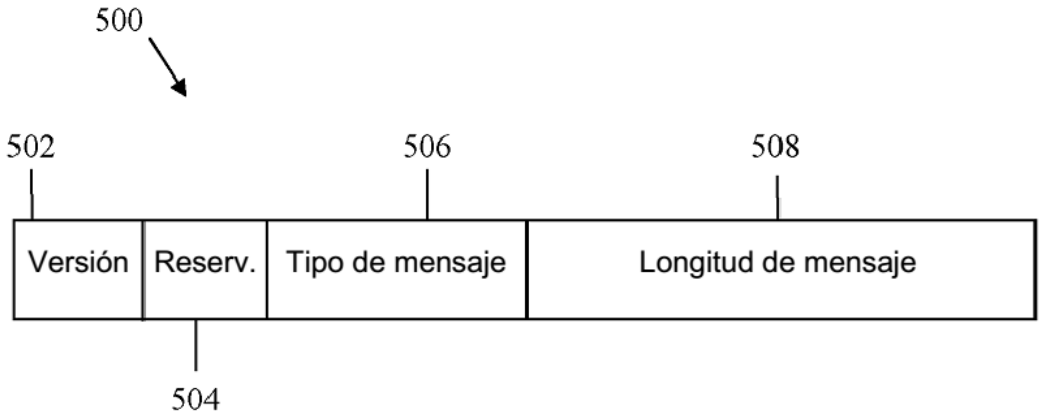

500
502
506
508
Versión
Reserv.
Tipo de mensaje
Longitud de mensaje
504

FIG. 5

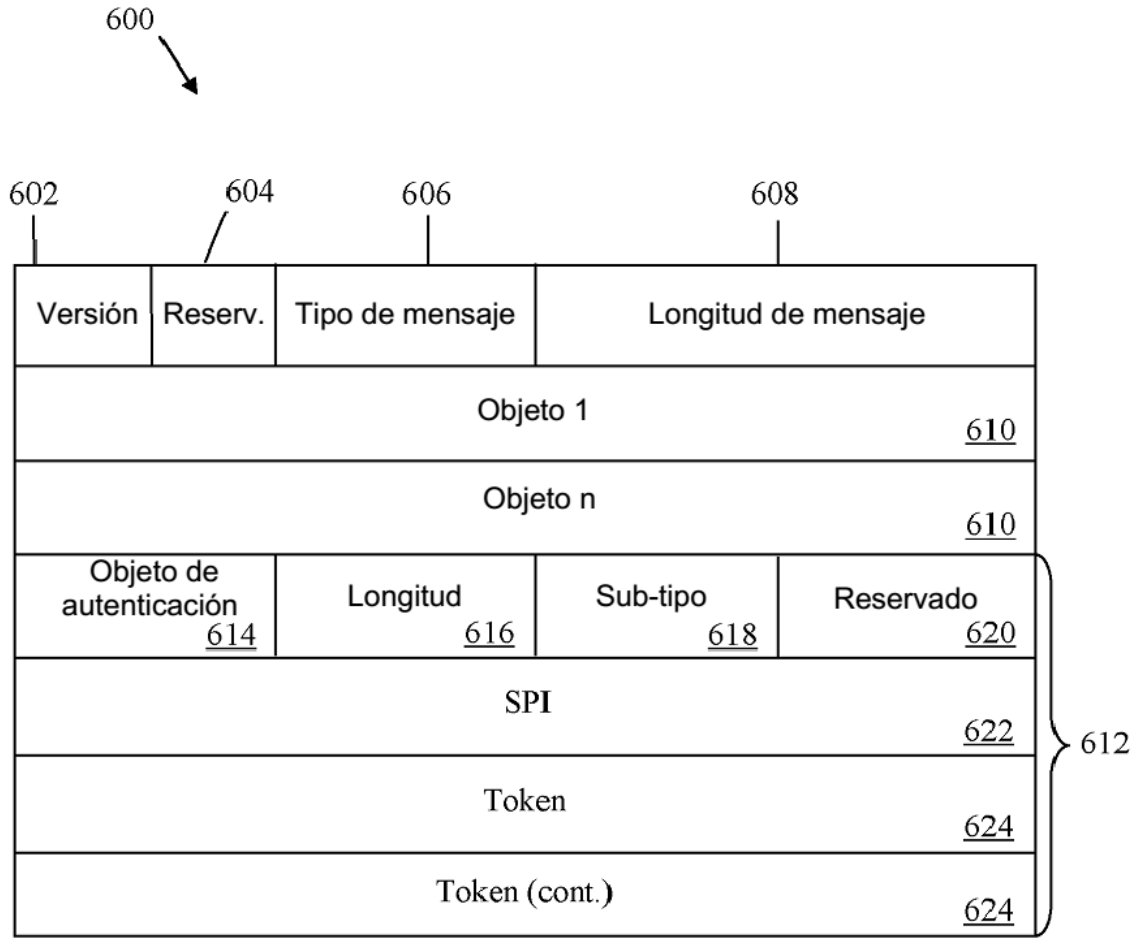

600
602
604
606
608
Versión
Reserv.
Tipo de mensaje
Longitud de mensaje
Objeto 1
610
Objeto n
610
Objeto de autenticación
614
Longitud
616
Sub-tipo
618
Reservado
620
SPI
622
Token
624
Token (cont.)
624
612

FIG. 6

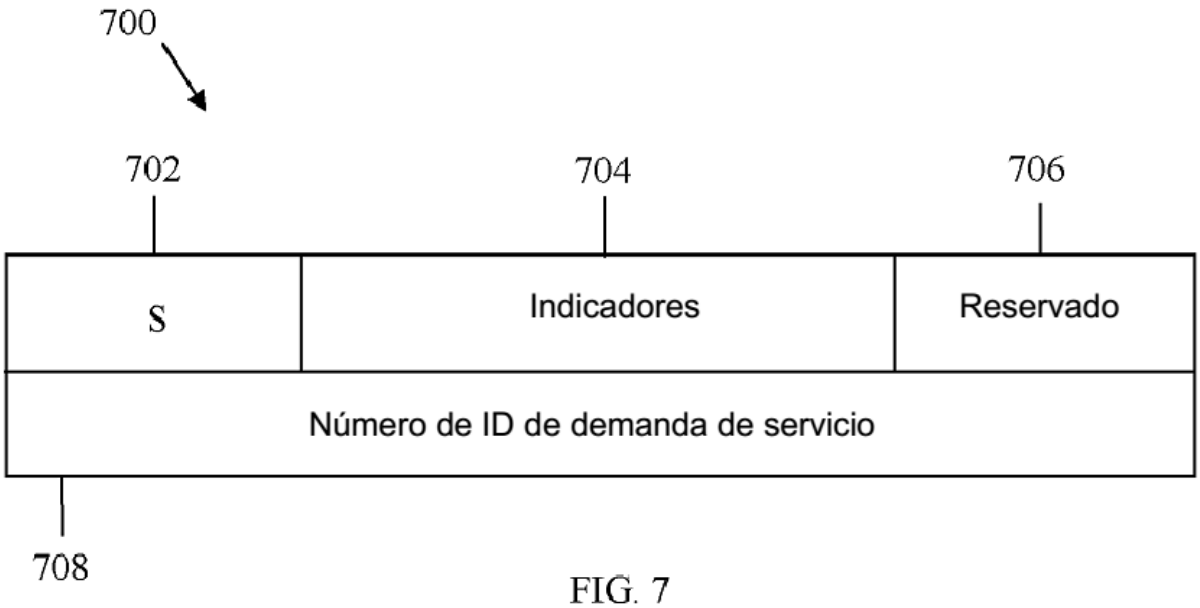

700
702
704
706
S
Indicadores
Reservado
Número de ID de demanda de servicio
708

FIG. 7

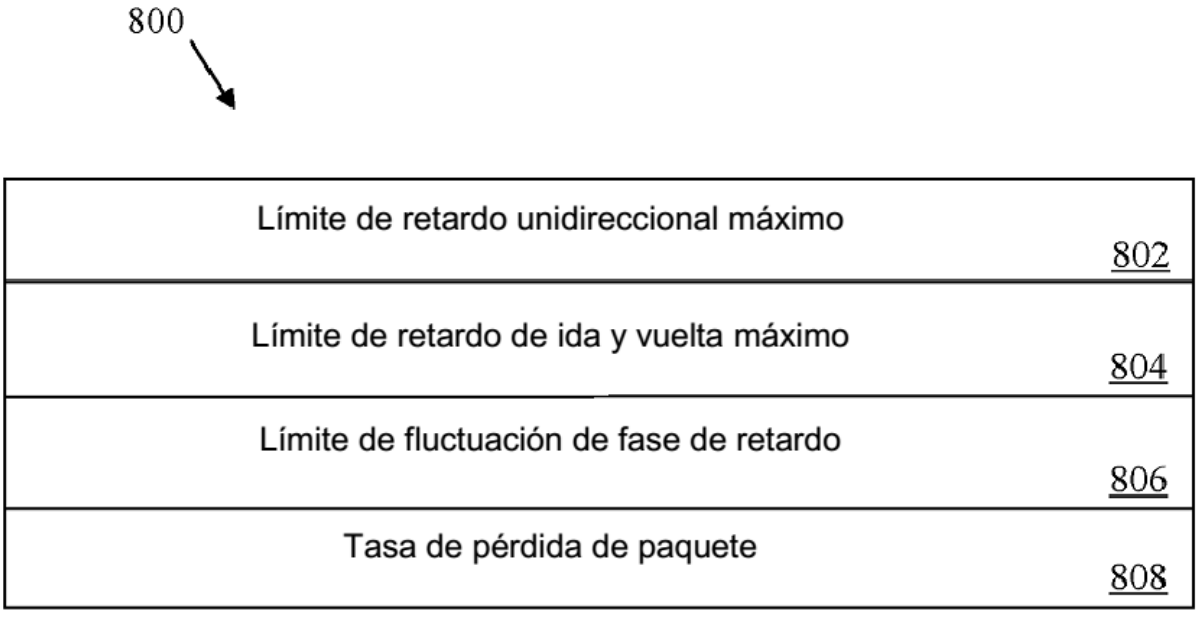

800
Límite de retardo unidireccional máximo
802
Límite de retardo de ida y vuelta máximo
804
Límite de fluctuación de fase de retardo
806
Tasa de pérdida de paquete
808

FIG. 8

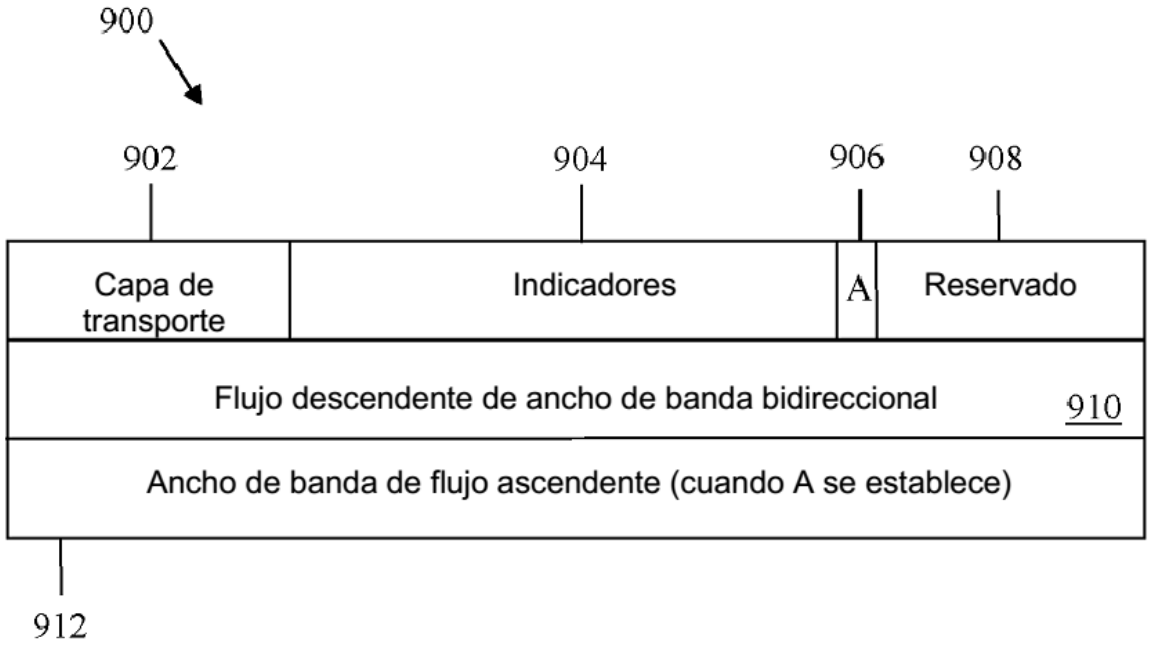

900
902
904
906
908
Capa de transporte
Indicadores
A
Reservado
Flujo descendente de ancho de banda bidireccional
910
Ancho de banda de flujo ascendente (cuando A se establece)
912

FIG. 9

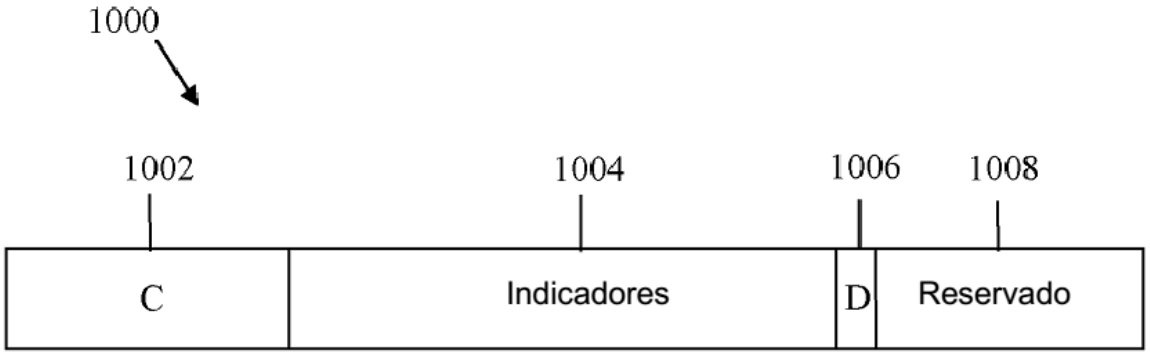

1000
1002
1004
1006
1008
C
Indicadores
D
Reservado

FIG. 10

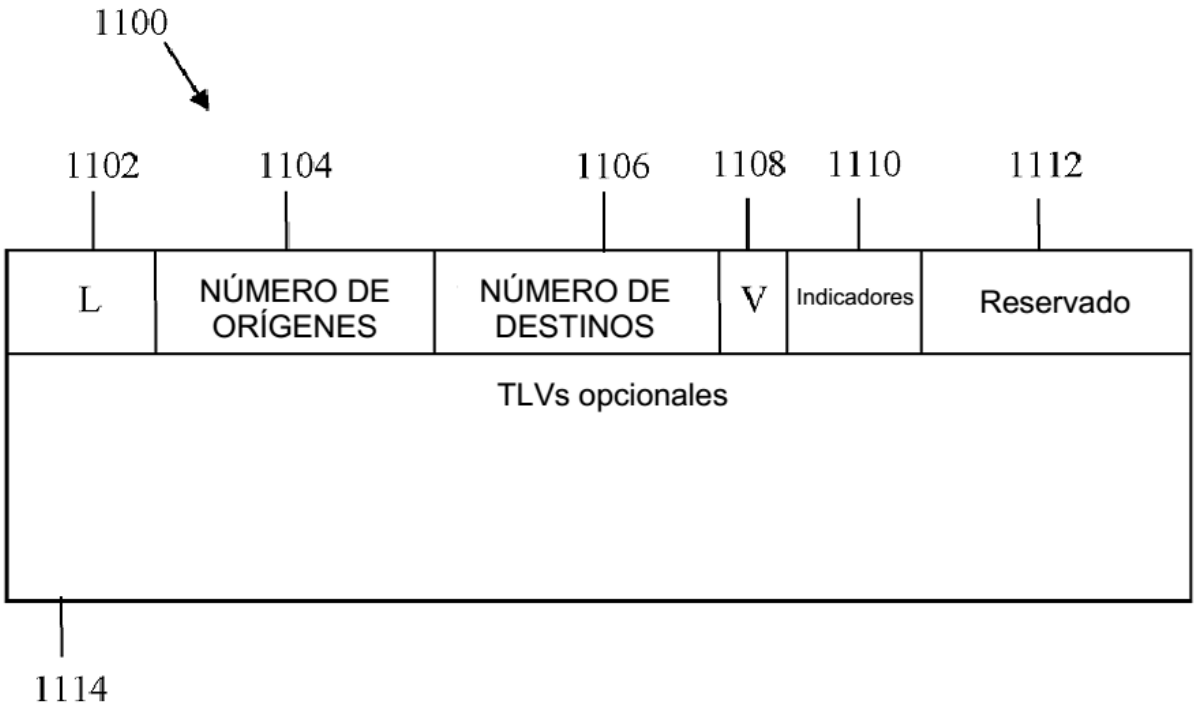

1100
1102
1104
1106
1108
1110
1112
L
NÚMERO DE ORÍGENES
NÚMERO DE DESTINOS
V
Indicadores
Reservado
TLVs opcionales
1114

FIG. 11

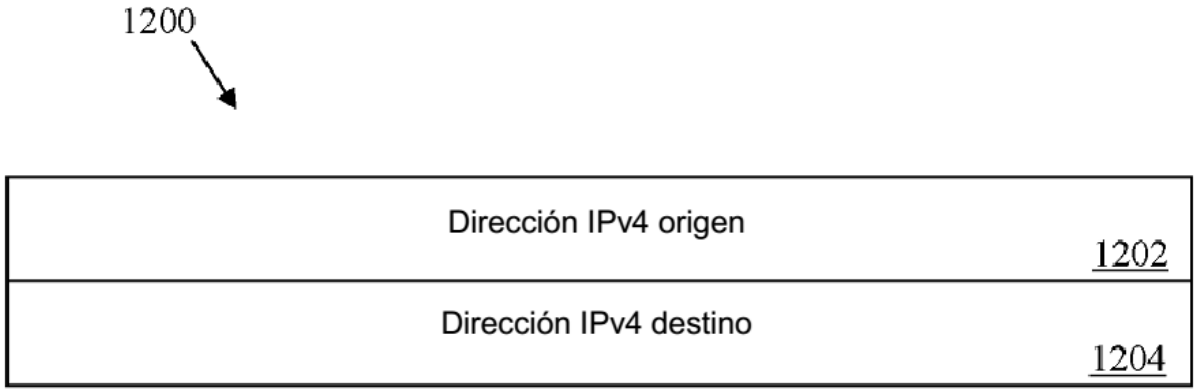

1200
Dirección IPv4 origen
1202
Dirección IPv4 destino
1204

FIG. 12

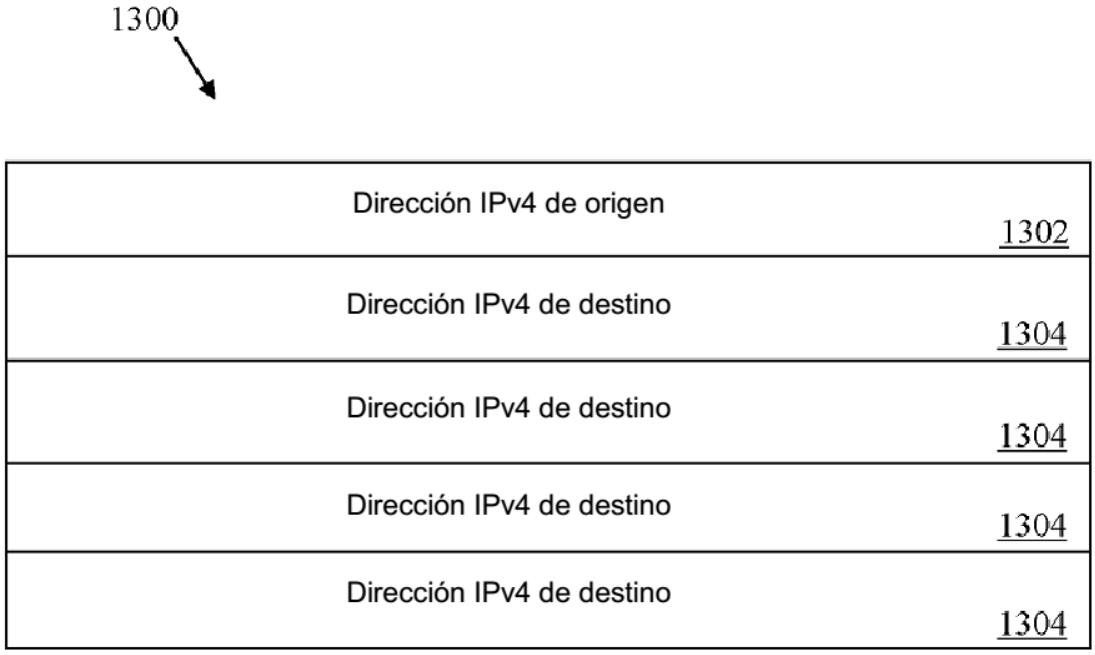

1300
Dirección IPv4 de origen
1302
Dirección IPv4 de destino
1304
Dirección IPv4 de destino
1304
Dirección IPv4 de destino
1304
Dirección IPv4 de destino
1304

FIG. 13

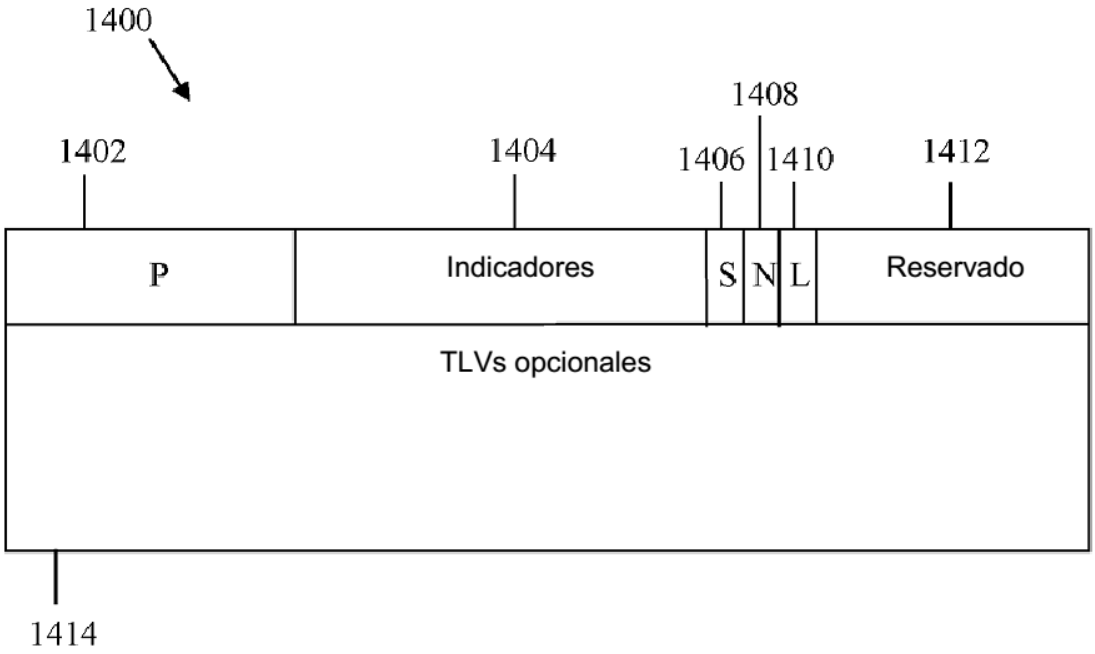

1400
1408
1402
1404
1406
1410
1412
P
Indicadores
S
N
L
Reservado
TLVs opcionales
1414

FIG. 14

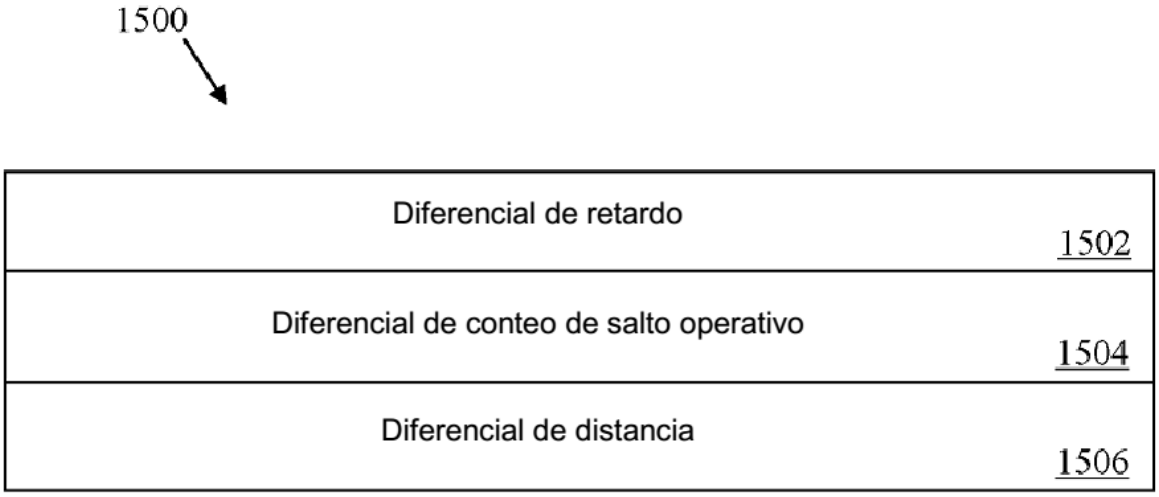

1500
Diferencial de retardo
1502
Diferencial de conteo de salto operativo
1504
Diferencial de distancia
1506

FIG. 15

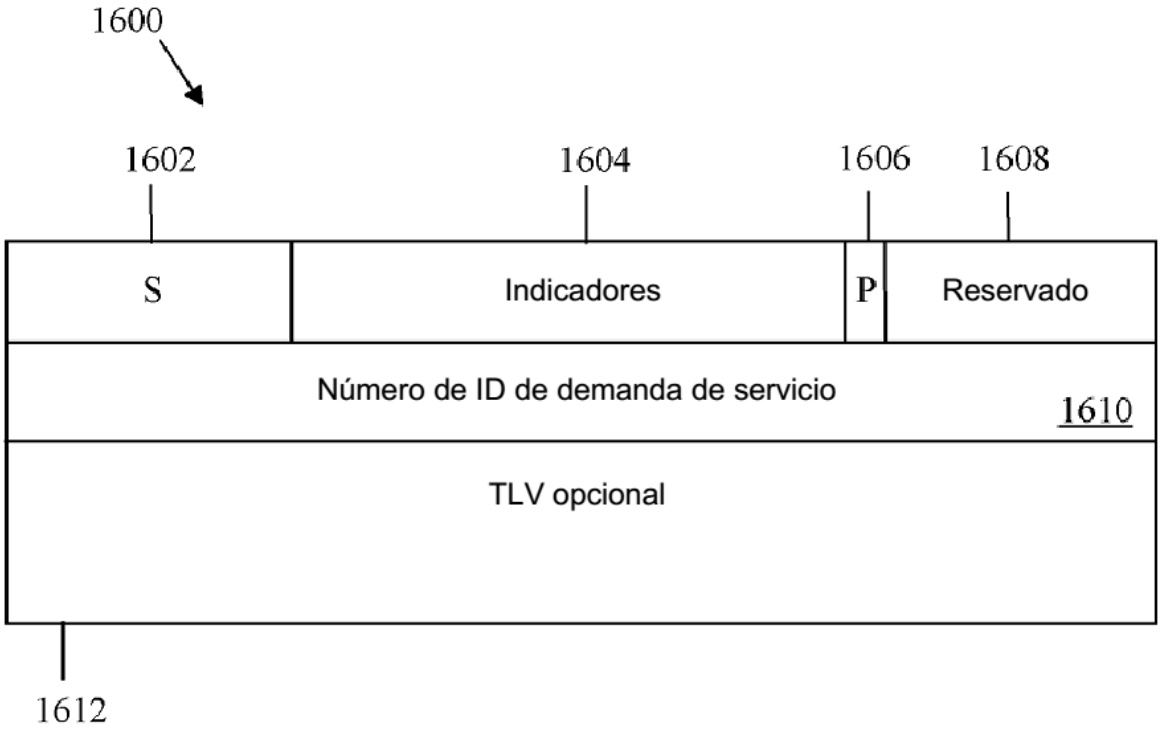

1600
1602
1604
1606
1608
S
Indicadores
P
Reservado
Número de ID de demanda de servicio
1610
TLV opcional
1612

FIG. 16

Identificador de ruta	1702
Dirección IPv4 de origen de aplicación	1704
Dirección IPv4 de origen de red	1706
Dirección IPv4 de destino de aplicación	1708
Dirección IPv4 de origen de red	1710
Ancho de banda reservado	1712

FIG. 17

Identificador de ruta	1802
Dirección IPv4 de origen de aplicación	1804
Dirección IPv4 de origen de red	1806
Dirección IPv4 de destino de aplicación	1808
Dirección IPv4 de origen de red	1810
Ancho de banda modificado	1812

FIG. 18

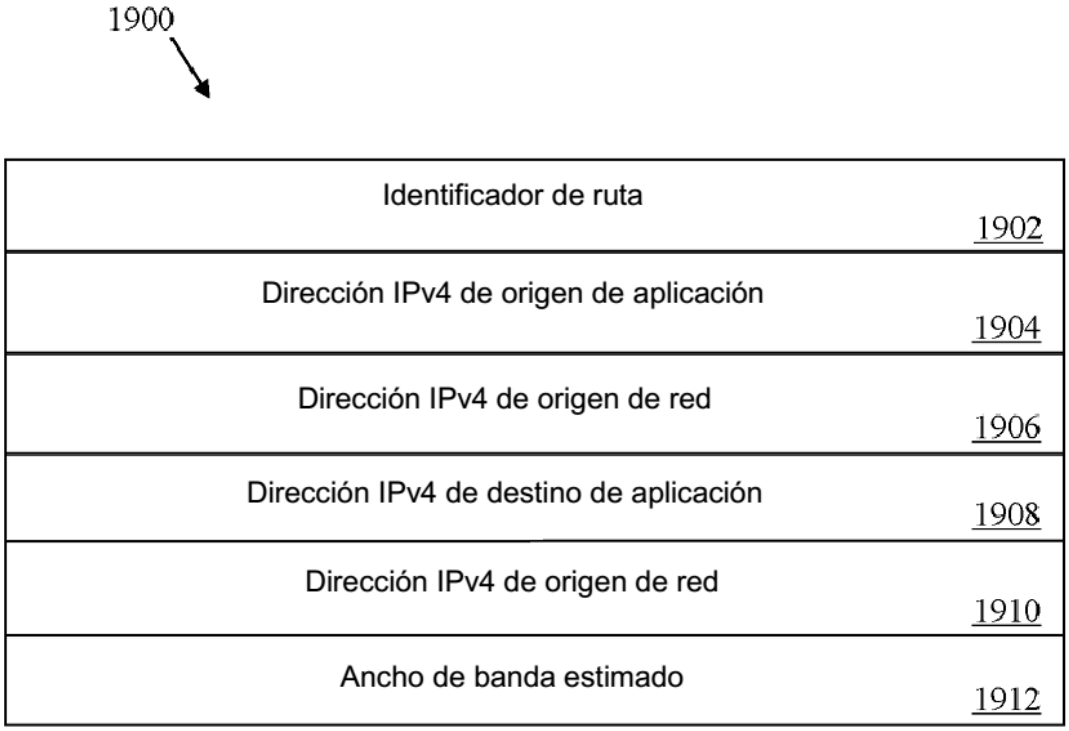

1900
Identificador de ruta
1902
Dirección IPv4 de origen de aplicación
1904
Dirección IPv4 de origen de red
1906
Dirección IPv4 de destino de aplicación
1908
Dirección IPv4 de origen de red
1910
Ancho de banda estimado
1912

FIG. 19

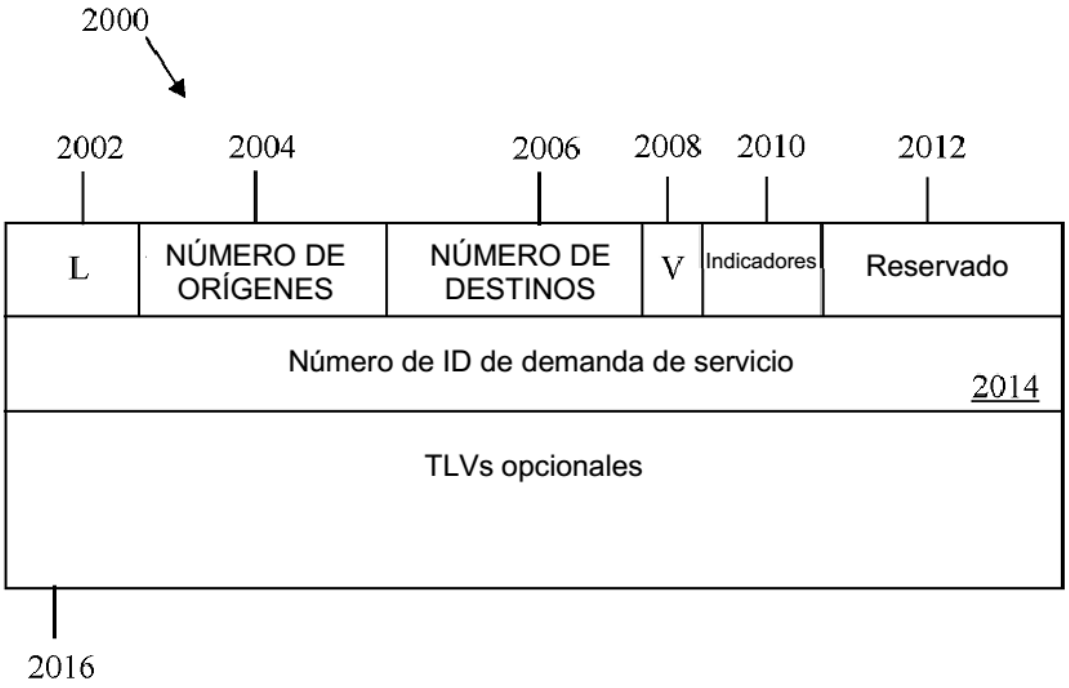
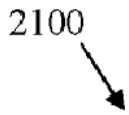
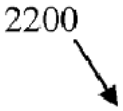

2000
2002
2004
2006
2008
2010
2012
L
NÚMERO DE ORÍGENES
NÚMERO DE DESTINOS
V
Indicadores
Reservado
Número de ID de demanda de servicio
2014
TLVs opcionales
2016

FIG. 20



Dirección IPv4 de origen de aplicación	2102
Dirección IPv4 de origen de red	2104
Dirección IPv4 de destino de aplicación	2106
Dirección IPv4 de origen de red	2108
Ancho de banda disponible	2110

FIG. 21



Dirección IPv4 de origen de aplicación nº 1	2202
Dirección IPv4 de origen de red nº 1	2204
Dirección IPv4 de destino de aplicación nº 1	2206
Dirección IPv4 de origen de red nº 1	2208
Ancho de banda disponible	2210
Dirección IPv4 de origen de aplicación nº 2	2212
Dirección IPv4 de origen de red nº 2	2214
Dirección IPv4 de destino de aplicación nº 2	2216
Dirección IPv4 de origen de red nº 2	2218
Segundo ancho de banda disponible	2220

FIG. 22

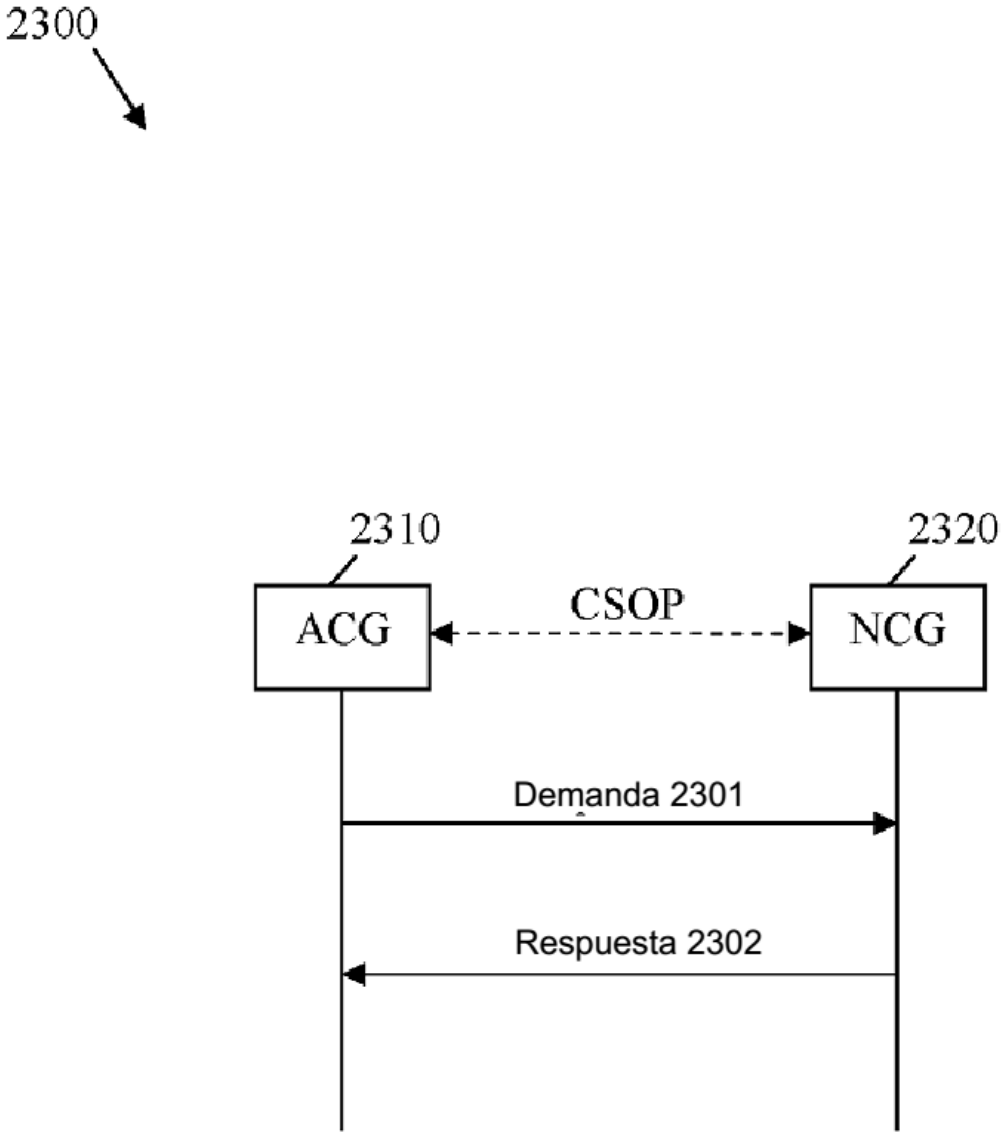


FIG. 23

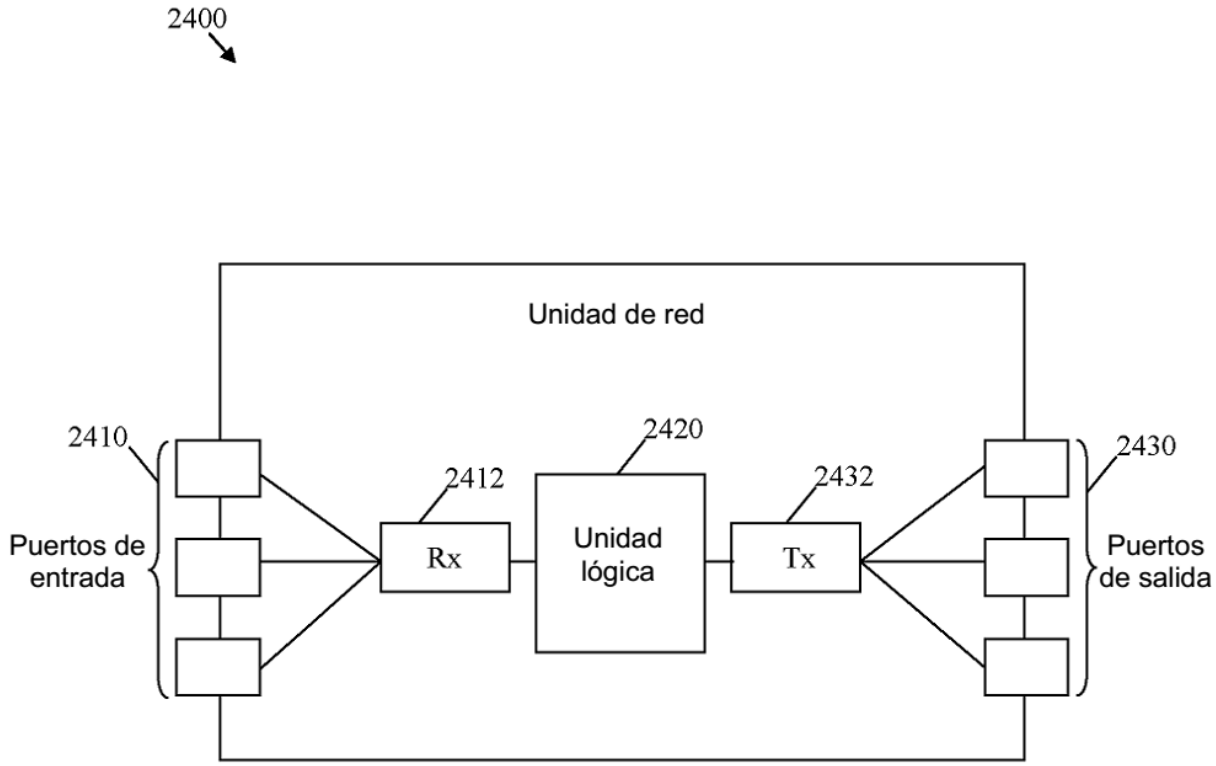

2400
Unidad de red
2410
Puertos de entrada
2412
Rx
2420
Unidad lógica
2432
Tx
2430
Puertos de salida

FIG. 24

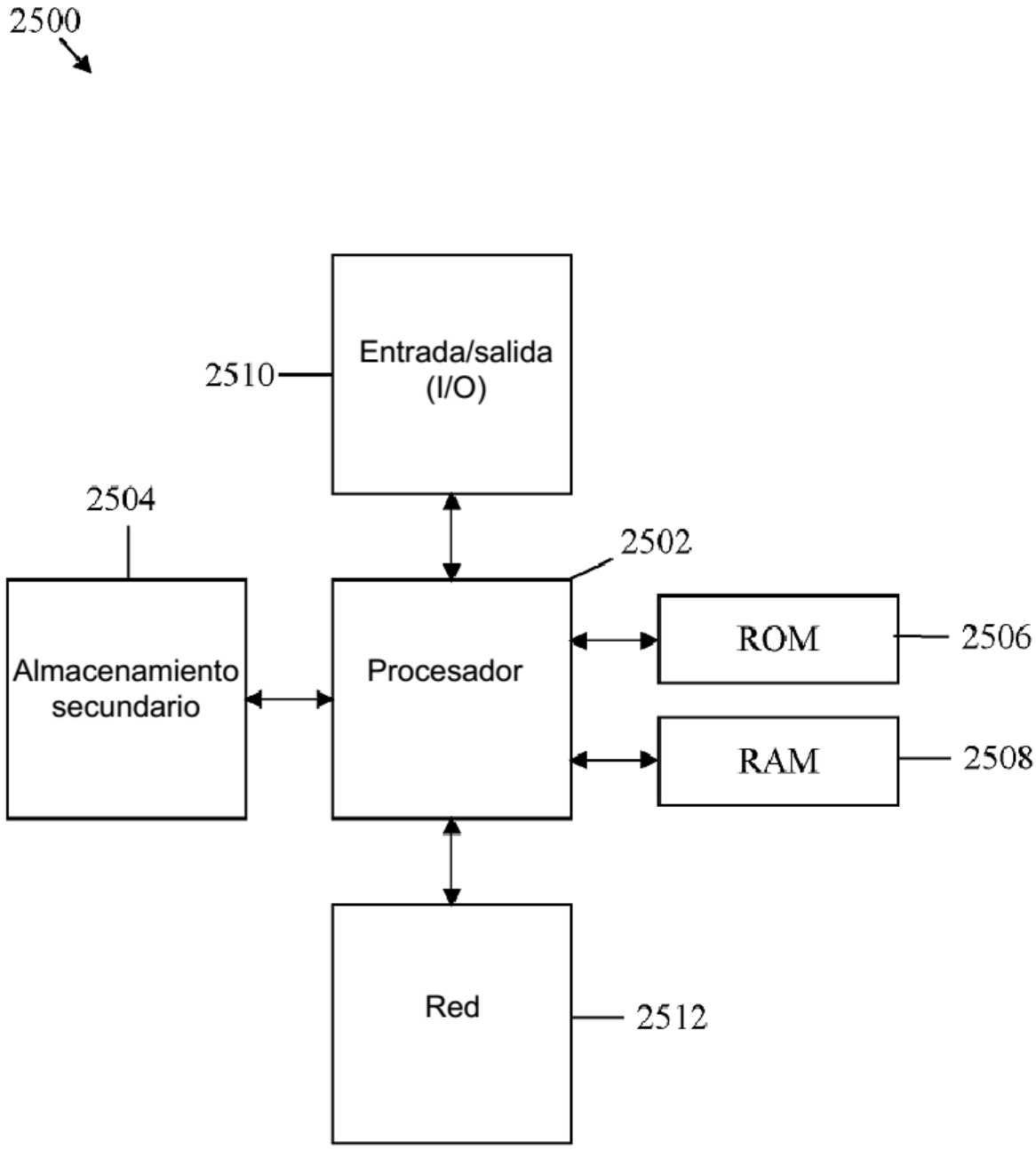

2500
2510
Entrada/salida (I/O)
2504
2502
Almacenamiento secundario
Procesador
ROM
2506
RAM
2508
Red
2512

FIG. 25